The Rationalization of Geographic Information Management Practices with Fair Information Practices

by

Christopher St. Elmo Michell-Viret
B.Sc., (General), University of Alberta, 1983
B..Sc., (Geography), University of Alberta, 1984
M.Sc., (Geography), University of Alberta, 1989

A Thesis Submitted in Partial Fulfilment of the
Requirements for the Degree of
MASTER OF ARTS

In the Department of Geography

We accept this thesis as conforming
to the required standard

[redacted]

Dr. P. Keller, Supervisor (Department of Geography)

[redacted]

Dr. H. Foster, Departmental Member (Department of Geography)

[redacted]

Dr. C. Wood, Departmental Member (Department of Geography)

[redacted]

Dr. C. Bennett, Outside Member (Department of Political Science)

[redacted]

Dr. T. Huston, External Examiner (Faculty of Business)

Supervisor: Dr. P. Keller

ABSTRACT

This thesis undertakes to rationalize Geographic Information Management practices with Fair Information Practices. The thesis describes alternate ways in which to balance geographic information management technologies and geographic information management requirements of public and private organizations with the right to privacy. The dissertation addresses three primary issues. Firstly, the dissertation provides an analysis of the effectiveness and efficiency of the application of information management practices on geographic information management and analysis. Secondly, the thesis includes the identification of innovative geographic information management practices that permit the most diverse and intensive forms of geographic information analysis without compromising fair information management practices. Thirdly, the dissertation addresses the development of potential geographic information management remedies where geographic information is underutilized or where geographic information analysis practices contravene fair information management practices.

Examiners:

[redacted]

Dr. P. Keller, Supervisor (Department of Geography)

[redacted]

Dr. H. Foster, Departmental Member (Department of Geography)

[redacted]

Dr. C. Wood, Departmental Member (Department of Geography)

[redacted]

Dr. C. Bennett, Outside Member (Department of Political Science)

[redacted]

Dr. T. Huston, External Examiner (Faculty of Business)

TABLE OF CONTENTS

Section		Page
	TITLE	**i**
	ABSTRACT	**ii**
	TABLE OF CONTENTS	**iii**
	LIST OF FIGURES	**viii**
	DEDICATION	**ix**
1.0	**INTRODUCTION**	**1**
2.0	**GEOGRAPHIC INFORMATION ANALYSIS**	**4**
2.1	**Context for Geographic Information Analysis**	**5**
2.1.1	Geographic Information Technology Development	6
2.1.2	Information Management Practices in Disparate Disciplines	9
2.1.3	User Pay Management Philosophy	10
2.1.4	Managing Property Rights in Information	10
2.1.5	Management of Uncertainty in Data	11
2.1.6	Management of Data Security and Liability for Information	13
2.1.7	Summary of Contributory Factors in GIA	14
3.0	**INFORMATION ACCESS AND PRIVACY PROTECTION**	**15**
3.1	**Trends in Information Access and Privacy Protection**	**15**
3.2	**Freedom of Information and Protection of Privacy Legislation**	**16**
3.3	**Fair Information Practices: Setting the International Context**	**24**
3.3.1	Model with Licensing Scheme (Sweden)	26

3.3.2	Model with Registration Scheme (United Kingdom)	29
3.3.3	Models with Partial Registration Schemes	31
3.3.3.1	Switzerland	32
3.3.3.2	Quebec	33
3.3.4	Models with Sectoral Codes of Practice (New Zealand)	34
3.3.5	Hybrid Models with Partial Registration/Sectoral Codes of Practice	36
3.3.5.1	Netherlands	36
3.3.5.2	Ireland	37
3.4	**Fair Information Practices: Setting the Canadian Context**	**38**
3.4.1	Model Based on Voluntary Self-Regulation (Canada)	38
3.4.2	Model Based on Mandatory Regulation	40
3.4.3	Private Sector Legislation in Quebec	45
3.5	**Privacy Protection Model for the Private Sector**	**46**
3.5.1	Proposed Model Based on Marketing Principles	46
3.5.2	Government/Private Sector Partnerships	48
3.5.3	Public Support for Stronger Privacy Protection	49
3.5.4	Voluntary Codes	52
3.5.5	Potential Implications of Extending Privacy Protection to the Private Sector	59
3.5.6.	Trends in the application of Fair Information Practices	65
4.0	**DATA COLLECTION AND ANALYSIS**	**69**
4.1	**Identification of Stakeholders**	**69**

4.2	**Research Methodology**	**70**
4.3	**Survey Administration**	**71**
4.4	**Data Analysis**	**72**
4.4.1	**Jurisdictional Summaries**	**75**
4.4.1.1	Introduction	75
4.4.1.1.1	Compilation of Jurisdictional Summaries	78
4.4.2	**Cross Jurisdictional Summary**	**78**
4.4.2.1	Jurisdictional Setting	79
4.4.2.2	Modes of Geographic Information Management	81
4.4.2.3	Modes of Geographic Information Analysis	85
4.4.2.4	Application of Fair Information Practices	87
4.4.2.5	Impact on Geographic Information Management and Analysis	91
4.4.2.6	Innovations in Geographic Information Management	94
4.4.2.7	Innovations in Geographic Information Analysis	98
4.4.2.8	Contravention of Fair Information Practices	101
5.0	**DISCUSSION AND CONCLUSIONS**	**104**
5.1	**Jurisdictional Setting**	**105**
5.1.1	**Access to Information and Protection of Privacy Legislation**	**106**
5.1.2	**Office of the Information and Privacy Commissioners**	**107**
5.2	**Modes of Geographic Information Management**	**110**
5.2.1	**Access to Information and Protection of Privacy Offices**	**110**
5.2.2	**Geographic Information Management Frameworks**	**112**

5.2.3	Information Brokerages	113
5.2.4	Legislative, Regulatory or Voluntary Authority for Geographic Information Management Frameworks	114
5.3	Modes of Geographic Information Analysis	117
5.3.1	Strategic Information Systems Planning	117
5.3.2	Function Creep	118
5.4	Application of Fair Information Practices	120
5.4.1	Privacy Impact Assessments	121
5.5	Impact on Geographic Information Management and Analysis	124
5.5.1	Leveling the Playing Field	125
5.6	Innovations in Geographic Information Management	126
5.7	Innovations in Geographic Information Analysis	129
5.8	Contravention of Fair Information Practices	131
5.9	Recommendations to enhance compliance with Fair Information Practices in Geographic Information Management and Geographic Information Analysis	135
5.9.1	Geographic Information Management Framework	136
5.9.2	Access to Information Considerations	140
5.9.2.1	Access to Information GIS Management Principles	140
5.9.3	Protection of Privacy Considerations	142
5.9.3.1	Protection of Privacy GIS Management Principles	143
6.0	FINAL ANALYSIS	146
	ENDNOTES	148

APPENDICES

1.0	**Definitions**	**175**
2.0	**Questionnaire**	**177**

LIST OF FIGURES

Figure 1 **Geographic Information Management Framework Hierarchy 137**

DEDICATION

This thesis is dedicated to the loving memory,

of my late partner,

Craig Ashley Yuzel

1.0 INTRODUCTION

Geographic Information Analysis (GIA) touches many aspects of our public and personal lives in the Information Age. Most information collected about our person or possessions is linked to an address or physical location at any one point in time. Techniques in GIA such as exploratory spatial data analysis, geostatistics, data matching, profiling and enabling technologies such as Geographic Information Systems (GIS) allow users of geographic information to create profiles about the data subject. These profiles often extend beyond the person to include possessions and associations over extended periods of time. With the availability of each additional theme of data, the information analyst has the capacity to generate increasingly detailed profiles of data subjects that range from the pre-cradle to the post-grave. Thematic information layers may range from such information sets as the genetics information captured before our birth to the traditional archives files that continue to hold details of our lives long after our death. As the sophistication of the techniques of GIA have increased, the right to privacy of data subjects has continued to erode.

The purpose of this research programme was to determine whether geographic information is managed in Canada in a manner that permits its use in geographic information analysis without compromising fair information practices and to describe alternate ways in which to balance geographic information management technologies and geographic information management requirements of public and private organizations with the right to privacy.

The research has involved conducting a survey of Canadian geographic information management practices. The survey was focused on the information management practices that are followed in the Canadian public sector and the manner in which fair information practices have been incorporated into procedures for geographic information analysis.

The intent of the survey was threefold. Firstly, the survey was designed to identify the conceptual models for geographic information management in the Canadian public sector. Secondly, the survey was intended to allow the researcher to identify the parameters for geographic information analysis in the Canadian public sector. The final intention of the survey was the identification of the legislative, regulatory and voluntary codes of fair information practices that are presently being used to regulate geographic information management and analysis in the Canadian public sector.

Following from the survey, the researcher anticipated being able to draw conclusions in three areas of inquiry. The first area of inquiry was the analysis of the effectiveness and efficiency of the application of fair information practices on the geographic information management and analysis. The second area of inquiry was the set of innovative geographic information management practices that permits the most diverse and intensive forms of geographic information analysis without compromising fair information practices. The third area of inquiry was the development of potential geographic information management remedies where geographic information is under-utilized or where geographic information analysis practices contravene fair information practices.

The structure of the remainder of the dissertation is as follows. Chapter two contains a discussion of the concepts involved in geographic information analysis and includes a discussion the factors that contribute to the context within which geographic information analysis is conducted. A discussion of concepts in access to information and privacy protection is provided in chapter three. This discussion includes a review of several models for the application of fair information practices in both the public and private sectors. Data collection and analysis is addressed in chapter four. This chapter contains a statement of methodology and includes the jurisdictional summaries following from the administration of the survey of Canadian federal, provincial and territorial jurisdictions. The discussion and conclusions drawn from the administration of the survey of Canadian federal, provincial and territorial jurisdictions is contained in chapter five. Concluding observations following from a final analysis of the research are contained in chapter six.

2.0 GEOGRAPHIC INFORMATION ANALYSIS

Integrated resources management is a resources management philosophy that is being applied more intensively to both physical and non physical resources. Geographic Information Analysis (GIA), through the application of such technologies as Geographic Information Systems (GIS), provides the means to assess alternative futures in the process of generating integrated resources management solutions. GIS applications are applied in an ever increasing range of disciplines but are commonly applied in land management; conservation; resource management; emergency services; disaster response; medical and health research, services and planning; transportation; law enforcement; military operations; municipal and local government; and many commercial and private sector applications.

By definition, a GIS is a database management system that facilitates the storage, retrieval, manipulation and analysis of spatial and temporal data and its display in the form of maps, tables and figures. The information in a GIS describes entities that have a physical location and extent in some spatial region of interest, while queries involve identifying these entities based on their spatial and temporal attributes and relationships between entities. Geographic data refers to spatial data in terms of their position with respect to a known co-ordinate system, their attributes (which are unrelated to their position) and their spatial inter-relationships with one another.[290]

Conducting GIA, with the use of GIS, involves the intensive integration of diverse information sets and results in integrated information resources products that describe these integrated resources management solutions.

Bodies of access to information and protection of privacy legislation exist in most jurisdictions in Canada and embody sets of information management practices that are designed to protect corporate and individual privacy. Techniques in GIA and GIS applications tend to employ sophisticated techniques in information analysis and data aggregation that tease out the trends and relationships that access to information and protection of privacy legislation generally attempts to protect.

2.1 CONTEXT FOR GEOGRAPHIC INFORMATION ANALYSIS

Many authors have discussed the broader aspects of alternative ways in which legislative, regulatory and voluntary codes of information management practices have been introduced in different jurisdictions to address the issue of setting parameters for geographic information analysis to balance the right of access to geographic information with the data subject's right to privacy. [24,78,98,99,115,126,143,165,189,194,234,261,358,359]

Techniques in GIA such as exploratory spatial data analysis, geostatistics, data matching, profiling [75,113,114,195,211,319,320] and enabling technologies such as Geographic Information Systems (GIS) [7,9,47,80,217,242,312,368] allow users of geographic information to create profiles about the data subject [28,144,205,246]. Several factors contribute both positively and

negatively to establishing the environment for GIA in society. Information technology development, information management practices, user pay philosophy, property rights in information [10,11,13,14,103,104,201,218,239,316], information brokerage [12,253,354], and the management of data uncertainty, information security and integrity [48,96,158,168], and, liability for information all contribute significantly to establishing the environment for conducting GIA. Increasingly intrusive techniques in information management and information technology development add impetus to the demand for legislative, regulatory and voluntary codes of practice for information management in order to balance the right of access to geographic information with the data subject's right to privacy.

2.1.1 Geographic Information Technology Development

Even over the past fifteen years, GIA has undergone considerable metamorphosis. Relatively speaking, information technology has been revolutionized since the late 1970's and in many areas has forged ahead of the organizational evolution and the development of geographical concepts in GIA.

For the period from the late 1970's into the early to 1980's, enabling technologies such as GIS were generally centralized, single-purpose, single-means applications. Jurisdictional barriers, computer literacy and the transferability of data were primary obstacles in implementing broader GIS applications as we perceive them today. For the most part, the data resided within the organization that operated the specific GIA application.

With the introduction of the microcomputer in the early 1980's, computer literacy levels soared, distributed information processing evolved and the development of applications, tools and technology within the vendor community flourished in response to public and private sector's quest to implement integrated GIS initiatives. Multi-purpose, multi-jurisdictional GIS initiatives had emerged in the early 1980's and were facilitated by the technical innovations in telecommunication links, interactive graphics, techniques in spatial analysis and relational database management and the development of concepts in decision support systems.[217]

As today, much of the data being used as an input to GIA originated from a diverse range of typically government databases.[244] The information was collected as per the mandate of the respective government agencies for the purposes of administering the programs under their jurisdiction. [23,89,100,102,112,140,155,157,184,188,231] Government has therefore served as a barometer of the organizational changes that have accompanied the GIS technological development and that have impacted the GIA practices.[175,213,217,226,227,228,245]

Application-oriented initiatives, focused at the local level of government, had given way to multidisciplinary GIS for programs at the regional level of government by the mid 1980's. As government programs have moved from centralized data processing toward decentralized information management, the 'technological priesthood' no longer holds governance over GIA. The focus of GIA initiatives has broadened from applications in local government to regional, national and international programs and focuses on GIS

development that would provide interdisciplinary management tools. Through ongoing technical and institutional innovations, the traditional single-purpose GIS application has broadened into multi-purpose, multi-jurisdictional platforms. [226] In most cases, the data required as an input to these multi-purpose, multi-jurisdictional techniques in GIA is no longer housed within a single agency or jurisdiction. The rate of evolution of the GIA techniques and GIS technology has surpassed the rate of the organizational evolution of the agencies and jurisdictions that would permit access to the multiple data sources required for these forms of integrated GIA.

Since the early 1990's, GIA programs in government have included the emergence of organizational models for multi-jurisdictional GIS programs. System migration strategies have also appeared in response to market conditions where heterogeneous multi-vendor systems are becoming commonplace. Techniques in GIA management are tending to become more centralized in government as the computing power increases and the GIS techniques for data processing become more distributed. Apart from the technological viability of these formulae there appears to be a cultural aspect of this status in GIA programs development. In many instances the fundamental issues in GIA in government have not changed since the late 1970's even though the fundamental structure of GIS technology has changed radically over the past fifteen years. The complexity involved in resolving these obstacles, however, appears to have increased exponentially over the past fifteen years as the sophistication of the technology has increased, the scale of GIA initiatives has broadened, the organizational structure of GIA initiatives has evolved, and the relative 'size of the world' of GIS applications has decreased. [217,226,242]

2.1.2 Information Management Practices in Disparate Disciplines

GIA and the process of its evolution has provided a forum for unparalleled communication between professionals from previously disparate disciplines. The use of GIS technology by a wide variety of disciplines has maintained the momentum for the continued expansion of applications and evolution of GIA through the application of GIS technology. Applications such as exploratory spatial data analysis, virtual reality and visualization provide us with examples of current applications of GIS technology which have been applied in wide variety of disciplines. While this multidisciplinary cross-fertilization of ideas has contributed significantly to the development of techniques in GIA and GIS technology and its application within an increasing number of disciplines, considerably less attention has been devoted to developing the philosophy and practice of the interdisciplinary information resources management. The philosophy of integrated interdisciplinary information resources management appears to have been left without a sponsor in the multidisciplinary forum for the development of GIS technology and GIA applications. Little appears to have been accomplished in establishing a forum for interdisciplinary users of the information. The lack of controls over the access, aggregation and use of information, with the exception of a limited number of disciplines, has created an increasingly uncertain environment for information users. [218]

2.1.3 User Pay Management Philosophy

As governments have continued to attempt to scale down in size in recent years in response to decreasing budgets, user pay principles have continued to gain profile in government programs. In many agencies, data are viewed as an untapped commodity of value to a society that is increasingly oriented to integrated information resources management.

It is not surprising therefore that the focus of the issues in accessing data appears to revolve about potential financial and societal costs associated with converging trends in which governments are downsizing and society is becoming increasingly reliant on access to a wide variety of data sources for the operation of geographic information systems. [217]

2.1.4 Managing Property Rights in Information

Under Canadian law, no property rights in information appear to exist. Without property rights associated with the information, the agency issuing the information would have considerable difficulty restricting the use of the information once it has been released. In future decisions, the Canadian courts could conceivably grant property rights for such categories of information as confidential information. In addition to confidentiality, limited proprietary rights may be granted to those who gather information as they may be entitled to "reap what they have sewn".

Provisions under Copyright Law generally do not protect the information itself but do protect the manner in which one is permitted to express the information. [11,98,201,218]

2.1.5 Management of Uncertainty in Data

The capacity to assess uncertainty in data significantly impacts our ability to broker data and subsequently process and apply the data in integrated information products for decision-making purposes in an integrated resources management environment.

In order to effectively manage the uncertainty in using data, we have to consider three contributing areas of uncertainty. These three areas include the uncertainty incurred in the capture of the data, the uncertainty incurred in processing of the data and the uncertainty incurred in the subsequent application of the processed data in decision-making.

Conceivably, in an integrated information resources management environment, the decision-making process could employ the use of integrated information products formulated from multiple data sources. Each data sources has the potential of contributing to the degree of uncertainty in the integrated information product and ultimately in the decision taken in integrated resources management.

As implied above, different applications place different levels of importance on the quality of data. As a result, taxonomies of data usage have typically been developed to

aid in the recognition of critical data quality components such as attribute accuracy, currency, completeness, consistency and positional accuracy. To aid in the selection of data that are appropriate to decisions being undertaken, techniques in error visualization also have been developed. [48,96,158,168]

As the degree of use of the data increases in the decision-making process, so does the importance of accurately assessing the degree of uncertainty in the data. The uncertainty of data which is barely referred to in the decision-making process is of relatively less importance to the preservation of the integrity of the decision. Conversely, the data may not be an integral component of the decision-making process because there exists a lack of confidence in assessing the degree of uncertainty associated with this data. Furthermore the tolerable degree of uncertainty is likely to vary with each distinct application of the data. [168]

An additional consideration is the degree of user knowledge about the use of the data and the subsequent use of meta-uncertainty. Three levels of users have been identified with the use of data and meta-uncertainty. These three levels are associated with the use of data meta-uncertainty by novice, partially-informed and knowledgeable users.

The research asserts that, while the novice user of the data places little emphasis on the importance of meta-uncertainty, the partially-informed and somewhat skeptical user maximizes the use of the available meta-uncertainty. In contrast, the knowledgeable user

requires less meta-uncertainty as this user is sufficiently experienced to assess and account for error or uncertainty in the data.

As the broker or user of information, the management of uncertainty in the data and the reliability of the resulting integrated information products is non-trivial in securing the integrity of decisions and decision-making in integrated resources management.

2.1.6 Management of Data Security and the Liability for Information

As part of the context for the sound management of information resources, the management of data security and liability for information must form some of the base considerations. Legislation in the form of the British Data Protection Act provides an example where limited civil remedies are available when information, distributed by an institution, is incorrect or is of a confidential nature. There are no statutory provisions in Canada which offer this type of remedy. It is apparent, however, that there is a common law duty imposed on those who initiate and collect data to ensure the validity of the data before they are released. The institution in the best position to have prevented the error is the one upon whom this burden is placed.

Canadian courts have left the question of civil remedies for the unauthorized distribution of confidential information open for debate. It is submitted that one would have to show the court specific damages in order to be provided with any sort of relief. Punitive

damages would be negligible unless the plaintiff could show that substantial harm was sustained as the result of the institution's negligence. [218]

2.1.7 SUMMARY OF CONTRIBUTORY FACTORS IN GIA

GIA, through the application of such technologies as GIS, provides the means to assess alternative futures in the process of generating integrated resources management solutions. Techniques in GIA such as exploratory spatial data analysis, geostatistics, data matching, profiling and enabling technologies such as GIS allow users of geographic information to create profiles about the data subject. Several factors contribute both positively and negatively to establishing the environment for GIA in society. Information technology development, information management practices, user pay philosophy, property rights in information, information brokerage, and the management of data uncertainty, information security and integrity, and, liability for information all contribute significantly to establishing the environment for conducting GIA. Increasingly intrusive techniques in information management and information technology development add impetus to the demand for legislative, regulatory and voluntary codes of practice for information management in order to balance the right of access to geographic information with the data subject's right to privacy. These contributory factors will be revisited in chapter five, in the context of the discussion and conclusions arising from the administration of the survey of Canadian federal, provincial and territorial jurisdictions.

3.0 INFORMATION ACCESS AND PRIVACY PROTECTION

Principles in information access and privacy protection are included in a variety of forms that direct the manner in which information is managed. These forms include legislation, regulation, policy, procedure and a variety of codes of practice.

The discussion in this chapter focuses upon the variety of models that have been adopted across several jurisdictions in an attempt to manage access to information and privacy protection, and includes both the Canadian and international context.

3.1 Trends in Information Access and Privacy Protection

Improvements in information storage and processing techniques are increasing the capacity for governments and businesses to gather and manipulate large amounts of personal information. Adding to this capacity is the proposed development of an advanced information and communication infrastructure which promises to link Canadian homes, businesses and governments into large interactive networks. This "information highway" will allow both public and private sector organizations to collect, combine, store and share personal and transactional data to an extent never before possible.

The changing technological environment, in conjunction with the establishment of international trade agreements, has already begun to break down national boundaries to the free flow of information and to reshape the global economy. Success in the new

international marketplace is becoming increasingly dependent upon the ability to transport data freely across borders.

The evolution of information technology and the reshaping of the global economy present enormous opportunities and efficiencies for the public and private sectors. However, the free flow of personal information across international boundaries also increases concerns about the potential loss of personal privacy and the need to protect data on a worldwide basis. The implementation of international standards for data protection is becoming increasingly important to those who are concerned about the potential loss of privacy associated with the transfer of personal information into jurisdictions lacking adequate protection, as well as to those data users who are currently required to contend with the multiplicity of regulatory systems across jurisdictions.

3.2 Access to Information and Protection of Privacy Legislation

Legislation governing access to information and protection of privacy has a significant impact on GIA practices in realizing integrated information resources management with the use of such enabling technologies as GIS. From a Canadian perspective, the goal of access to information and protection of privacy legislation is to provide the public with greater access to government information. It is an attempt to balance the "right to know" with the "right to privacy". The underlying purpose of access to information and protection of privacy legislation is to facilitate the release of government information to anyone who makes a request, subject to a limited and specific set of exceptions.

Basically, the legislation in most Canadian jurisdictions requires that all information, subject to this list of exemptions, is available to the public. If the information is not specifically excluded, it must be released.

The legislation provides a significant deviation from the traditional system that relies on ministerial discretion for the release of information. Access to information and protection of privacy legislation generally compels government agencies to release information which they may have traditionally retained. In many ways, the legislation makes government agencies more accountable for their action or inaction within set time constraints. The legislation would appear to formalize enhanced access to government-held information. However, further conditions are applied before any information is released for such multi-purpose applications as GIS.

Most pieces of Canadian access to information and protection of privacy legislation restrict the collection, compilation and distribution of personal and non-personal information to that information that is necessary for an operating program or activity of the public body. This information therefore could subsequently not be distributed within or beyond the ministry for any purposes other than those for which it was collected, or for a consistent purpose. This information is therefore not to be available for any of the multi-means, multi-purpose GIA whether within, between or beyond the ministries. GIS applications would therefore also be restricted to single-means, single-purpose applications within the specific operating program. The full capacity of GIA and the full

analytical functionality of GIS could therefore be restricted by the conditions of these provisions. [4,51,151,152,208, 236,237,241, 254,281,321]

Further provisions require that the purpose for the intended use of the information be communicated to the data subject at the time of information collection. Once again, the multi-purpose use of information, typical of many multi-layered GIA and GIS analytical techniques would not necessarily be consistent with the conditions of this provision. Unless the multi-layered GIA and GIS-type of application was envisaged at the time at which the information was collected, only limited GIS functionality could be applied in analyzing this information. From an administrative perspective, the costs of gaining the informed consent of the data subject after data collection are generally prohibitive within present information management practices. Innovations in information management practices may alleviate the administrative burden and facilitate gaining the informed consent of the data subject after the information collection period.

In most Canadian jurisdictions where access to information and protection of privacy legislation is in place, the legislation may thus restrict some aspects of the traditional practices of government agencies involved in the management, analysis and sharing of information. It is apparent that these legislative provisions may also extend to restrict mergers of separate data bases, and the formulation of integrated information products that are commonly the product of most GIA and GIS applications.

The access to information and protection of privacy legislation represents a significant improvement over the pre- access to information and protection of privacy environment in which applicants for information relied heavily on the discretionary power of the head of the respective public bodies for access to the requested information. The requirement under most current Canadian access to information and protection of privacy legislation requires that the respective government ministries or departments account for the granting or denial of access to requested information. This establishes a dynamic mechanism for accountability for access to information. This dynamic mechanism could prove to be a valuable tool in arguing for access to information for the purposes of integrated information analysis or GIA using GIS.

Most Canadian access to information and protection of privacy legislation also precludes the head of an institution from relying on a discretionary exemption to refuse to disclose information which would have been available prior to the access to information and protection of privacy legislation being enacted. If the head wishes to continue to distribute information containing personal data, this individual must show that the previous practice was warranted and that the personal information should continue to be distributed. This provision could be used to lobby for access to integrable information, recognizing the benefits of GIA and fully functional GIS capability and the merits in integrated information resources management.

The preservation of trade secrets or confidential information of economic value is found in most Canadian access to information and protection of privacy legislation and has the

potential to conflict with the analytical nature of GIA and the capability of GIS. This provision generally relates to third party requests for information. Regulating the scope of GIA and GIS activities with respect to this provision of access to information and protection of privacy legislation would appear to be an ongoing challenge.

Subject to receiving the consent of the third party, the agent issuing the information would be required to monitor the intended uses of the third party information being requested in order to assess the impact of releasing information as it relates to the business of the third party. The intent is to ensure that the released information would not reveal the trade secrets of a third party or the commercial, financial, labour relations, scientific or technical information pertaining to the third party. These types of provisions pose the core of the challenge to GIA and the deployment of fully functional GIS. GIA and the fully functional capability of GIS applications are designed to tease out the underlying relationships in such areas as the social, spatial, economic and temporal relations. It is precisely the confidentiality of these relations that these provisions seek to protect.

Responsibility for the intended use of the information lies with the agency releasing the information. The broker of the information could reasonably be expected to ensure compliance with any such provisions of access to information and protection of privacy legislation. These provisions would restrict the available applications of information products and would set a precedent for the addition of further restrictions to the applications for information products. Successfully managing the process of ensuring

compliance with these provisions would be essential to establishing an environment in which the merging of information databases and the use of integrated information products would facilitate the use of GIS types of analytical applications. Notably, the short-term political solution to unsuccessfully managing this process would likely be to simply curtail access to the information.

Further provisions of the access to information and protection of privacy legislation generally place a statutory duty on those who collect information to insure that there is adequate security in place for the protection of data once they have been collected. Clearly, those persons operating GIS systems and conducting GIA must remain cognizant of the potential conflict with the intent of this legislation when developing integrated information products.

Access to information and protection of privacy legislation has provided the framework for a set of fair information practices to be applied to information resources held largely by government. At the time that the research survey was administered, Quebec was the only provincial jurisdiction in Canada to have extended privacy protection to the private sector. In mid September, 1996, the Government of Canada committed to extend privacy protection to the private sector by the year 2000. The Personal Information Protection and Electronic Document Act was proclaimed by the Government of Canada in January 2001. The Act will apply initially to the federally-regulated sector and will apply fully to the private sector by the year 2004.

The introduction of privacy protection for the private sector has the potential to result in significant alteration to the legislative or regulatory environment, the business environment and the information management practices that could be applied to information with the implementation and operation of GIS. Initiatives such as the Model Code for the Protection of Personal Information, as prepared by the Canadian Standards Association, provide further momentum to the probability that the remainder of Canadian jurisdictions will extend privacy protection to the private sector in the near future. [70]

Extending privacy protection to the private sector would likely result in all Canadian information holdings being subject to the following set of fair information practices. [70]

1. An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organizations compliance with the following principles.
2. The purposes for which the personal information is collected shall be identified by the organization at or before the information is collected.
3. The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the of the individual.

Personal information shall only be retained as long as necessary for the fulfillment of those purposes.

6. Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

7. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information

9. Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. An individual shall be able to address a challenge concerning compliance with the above principles to the designated individuals accountable for the organization's compliance

Although these fair information practices have been included in most Canadian access to information and protection of privacy legislation, extending these principles to the regulation of information management practices in the private sector would represent a significant shift in culture for many areas of the Canadian private sector.

Most European jurisdictions have had fair information practices incorporated into their business system designs for some time. Recent landmark decisions taken in the USA banking sector suggest that adequacy of protection measures required by the European Union member countries for the transfer of personal information are likely to have far reaching affects in the USA and Canadian public and private sectors. The European Union directive became effective in October of 1998 and the implications on information management practices are being felt in the USA banking sector. The landmark case, involving the development of the German RailwayCard by the USA-based Citibank, has resulted in Citibank complying with adequacy of protection measures for personal information as set within the German jurisdiction. [115] We appear to have reached a new threshold in the global village with regard to the regulation of the flow of personal information.

New thresholds in privacy protection result in striking new balances with access to information and privacy protection. The new balance redefines the environment for the application of GIA and enabling technologies such as GIS and reshapes the wave of information that is available to information users.

3.3 FAIR INFORMATION PRACTICES: SETTING THE INTERNATIONAL CONTEXT

While the North American approach has typically been to leave data protection in the private sector to market forces, the European approach has been to implement legislation that requires both public and private sector organizations to abide by the same data

protection requirements. This dichotomy in attitudes toward data protection has generally been attributed to historical factors that have sensitized Europeans to the potential abuses of unrestricted compilations of personal information. The differing approaches to data protection in the private sector present an ongoing challenge to the free flow of personal information across national borders. Of primary concern is the fact that data users seeking to avoid data protection requirements can move their operations into jurisdictions with less stringent requirements. This concern has provided the impetus for a number of initiatives geared at harmonizing data protection standards around the world.

The first attempt at harmonization was the Organization for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) developed in 1980. Since the United States dominated the computer and information technology sector at the time, the North American preference for an open economic system was the principle upon which the guidelines were based. The guidelines are voluntary and carry no force of law and, as a result, have been applied differently across nations. Although the OECD Guidelines have served as the basis for the vast majority of privacy protection schemes throughout the world, they are generally perceived as not having achieved harmonization in approaches to data protection across member states. [261]

Following the OECD Guidelines, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the

Council of Europe Convention 108). [90] Unlike the OECD Guidelines, the Council of Europe Convention 108 was legally binding on members and called for data protection legislation that covered the private sector in addition to government organizations. However, a number of European nations did not yet ratified the agreement.

In response to the perceived inadequacies of the OECD Guidelines and the Council of Europe Convention 108, in 1990 the European Union drafted a Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data. After extensive revisions to the initial proposal, the European Union on July 25, 1995 formally adopted a Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of such Data (EU Directive). The EU Directive prohibits the transborder flow of personal information to countries without adequate protection. The impact of the EU Directive on North American organizations has been the subject of much debate since the initial draft was circulated and has increased pressure to strengthen private sector data protection throughout North America. [251]

3.3.1 Model With Licensing Scheme (Sweden)

The trend among European nations has been to enact proactive data protection legislation which applies to both the public and private sectors.

As the first national data protection system, the Swedish Data Act of 1973 has had considerable influence over the development of other statutes in Western European countries such as the United Kingdom and France. The Swedish law prohibits the creation and maintenance of a database of personal information in machine-readable form without a license from the Data Inspection Board (DIB), and, this applies to both the public and private sectors. In certain sensitive cases, permission of the DIB is required for the creation of a database, unless it is created by the Cabinet or Legislature.

The DIB is an independent authority with a Board of Directors who are appointed for fixed terms and represent a variety of political parties and interest groups. It exercises considerable control over the collection, use and disclosure of personal information, and enforces a system of responsible keepers for computerized personal data banks. Although the DIB is provided with ombudsman or supervisory functions, in actual practice these functions are subordinate to the licensing function. [30]

Since it would not be possible for the DIB to oversee and enforce all of the requirements of the legislation, the effectiveness of the Swedish model depends on the voluntary compliance of the responsible keepers of the personal information. Responsible keepers are anyone who has a personal file at his or her disposal and for whose purpose the file is kept. The responsible keepers of personal information are accountable for ensuring that the provisions of the legislation and their license are implemented. Non-compliance with the requirements of the statute is subject to various civil and criminal penalties. Although

the decisions of the DIB can be appealed to government, this is said to occur infrequently.

The licensing approach adopted by Sweden has been characterized as "highly regulatory and bureaucratic". [137] Critics of strict licensing note that such systems tend to be too intrusive, grant too much power to the licensing agency, and require a very large staff to handle the paperwork and ensure compliance with the requirements of the licensing agreement. However, on the positive side, licensing ensures openness and guarantees some level of regulation and investigation. Another advantage to this approach is that the provisions of the license may be tailored to the specific information system.

The Swedish approach of appointing a Board of Directors rather than a Data Protection Commissioner also has its pros and cons. On the positive side, having a Board of Directors which includes representatives of various political parties may help to sensitize politicians to privacy issues and ensures that the decisions of the Board reflect a wide range of interests. On the negative side, since the Board of Directors represents conflicting points of view, its decisions may be diluted and reflect political compromises. [238] However, it should be noted that, although there is no Data Protection Commissioner, there is a Director General who acts as both chair of the Board and administrative head of the DIB. This position is not a political appointment and the person occupying it may exercise considerable influence over matters affecting personal privacy.

3.3.2 Model With Registration Scheme (United Kingdom)

The United Kingdom's Data Protection Act of 1984 is based on a model emphasizing registration rather than licensing of personal data users and computer bureaus in the public and private sectors. All users of data systems which automatically process personal data are required to register with the Data Protection Registrar. Failure to register is an offence subject to fine.

In addition to maintaining the register of personal data users, the Data Protection Registrar is charged with ensuring compliance with a set of eight data protection principles. The principles are not directly enforceable. Instead, the Registrar is required to promote the observance of the principles. Therefore, voluntary compliance is critical to the effectiveness of this scheme.

Nevertheless, the Registrar has been provided with a number of powers to promote compliance with the data protection principles. The Registrar may refuse to register an entry, may conduct an inspection and seize material, and may serve three different types of notices - enforcement, de-registration, and transfer prohibition.

If the Registrar finds that a registered person is not complying with the data protection principles, that individual may be served with an "enforcement notice." A data user or computer bureau which fails to comply with the provisions of an enforcement notice is guilty of an offence and liable to a fine or subject to the seizure of the offending data.

Under extreme circumstances, the Registrar may serve a "deregistration notice." Decisions of the Registrar may be appealed to a special Data Protection Tribunal. The decisions of the tribunal are final and can only be appealed to the courts on a point of law.

Proceedings for a criminal offence under the legislation can only be started by the Registrar or the Director of Public Prosecutions or with the consent of the Director of Public Prosecutions. Data subjects that seek redress of a monetary nature are required to commence civil proceedings in court.

Although the legislation does not make provisions for industry specific statutory codes of practice, the Registrar is required to encourage trade associations and other bodies representing data users to prepare and disseminate codes of practice. In addition, the Registrar is expected to fulfill certain ombudsman or supervisory functions such as receiving complaints and conducting investigations. However, in practice, the registration function tends to dominate over these other roles.

As was the case with the DIB in Sweden, the Data Protection Agency in the United Kingdom was intended to be self-supporting through the collection of registration fees. In fact, the Data Protection Agency returned more than five million pounds to consolidated revenues in 1990. However, the registration scheme has been criticized as being over-regulatory and excessively tough on data users. [214] Data users argue that registration costs them time and money, adding to the burdens of data processing departments without

yielding substantial benefits. Small-scale data users believe that they should be exempt because their activities pose little or no threat to privacy.

Another limitation of the data protection legislation in the United Kingdom is the exclusion of manual records. This is also a problem with the Swedish model which was developed in response to the threat to privacy imposed by computerized technology.

Privacy advocates also have criticized the legislation for striking the balance in favour of information processors. They feel that the Registrar may lack adequate powers and resources to be an effective data protection ombudsman. Since the Registrar has no authority to supervise or inspect the activities of data users after registration, the effectiveness of the registration system as an indirect form of privacy protection has been questioned. It also has been noted that, in comparison to the Swedish licensing model, the registration scheme of the United Kingdom is more remedial than anticipatory, as the Registrar has no authority to block the creation of an information system. On the other hand, it has been suggested that the educative effects of the legislation may be more important than the scope or limitations of its legal provisions.

3.3.3 Models With Partial Registration Schemes

Since the Swedish data protection model was first implemented in 1973, the trend among European countries has been to move away from the comprehensive licensing approach

in favour of notification/registration schemes and partial notification/registration schemes based on classifications of perceived sensitivity of data and/or sectoral classifications.

3.3.3.1 Switzerland

The federal Data Protection Act of Switzerland applies to both private and federal public sectors and sets up a limited registration system in both sectors. Although all federal agencies are required to register the personal files which they hold, private sector organizations are only required to register files if the organization regularly processes sensitive personal information or personality profiles, or transfers personal information to third parties without statutory obligation or the knowledge of the persons concerned. [258]

The register of files is maintained by the Federal Data Protection Commissioner who independently enforces compliance with the law. The Commissioner has the power to conduct investigations that are either self-initiated or requested by the a third party. If the data protection rules set out in the legislation have been breached, the Commissioner may recommend that processing be modified or stopped. If the recommendations are not followed, the Commissioner may bring the case before the Commission to make a decision or inform the individual who requested action to pursue the case through the court. Those who breach the requirements of the legislation are subject to a fine or imprisonment. Enforcement measures are regulated by the Federal Council.

3.3.3.2 Quebec

The legislative frameworks in some jurisdictions distinguish between public and private sector organizations. This dichotomy is often made for administrative purposes and does not necessarily imply a different level of protection for personal data between the two sectors.

The Quebec Act Respecting the Protection of Personal Information in the Private Sector is somewhat unique in that a separate piece of legislation was enacted for the implementation of fair information practices in the private sector. However, one administrative body, the Commission d'acces a l'information, oversees the legislation pertaining to both the private and public sectors.

The private sector legislation applies to all enterprises operating within the province of Quebec which, directly or indirectly, collect, hold, use or disclose personal information. In addition to setting out the basic fair information practices to which all organizations must adhere, the legislation establishes specific rules in respect of personal information agents who maintain files on individuals on a commercial basis and prepare and communicate credit reports to third persons. Such agents (mainly credit bureaus) are required to register with the Commission and to make their activities known to the public by means of periodic notices in the press.

The Commission, at its own initiative or following a complaint from a third party, may conduct an inquiry. Following an inquiry the Commission may recommend or order remedial action to ensure the protection of personal information. Offences under the statute are subject to various fines. Decisions of the Commission are final, however, an order may be appealed to the Court of Quebec on any question of law or jurisdiction. [251]

3.3.4 Model With Sectoral Codes of Practice (New Zealand)

In contrast to the European approach of licensing or registration, legislation adopted in non-European countries tends to rely more on self-regulation and the powers of the data protection authority to conduct investigations and audits to ensure compliance with the legislation.

The New Zealand Privacy of Information Act of 1993 is based on the OECD guidelines and has adopted much of its structure from the Australian Privacy Act. However, unlike the Australian Privacy Act which has only recently been amended to cover the consumer credit industry, the New Zealand statute regulates both the private and public sectors.

The scheme of regulation requires the observance of 12 information privacy principles and is overseen by a Privacy Commissioner who may receive complaints, carry out investigations on his or her own initiative or otherwise, and act as a mediator of disputes where they arise. If the dispute cannot be resolved through mediation, then the matter is

heard by a tribunal. Under the legislation, the tribunal may issue orders and award damages and compensation for breaches of the legislation.

Although the legislation does not provide any sector-specific regulation, provisions are made for codes of practice to be approved by the Commissioner to cover specified activities or agencies, or certain professional groups. These codes of practice can impose standards that are stricter or more lenient than the privacy principles set out in the legislation, and can be developed at the initiative of an industry body or the Privacy Commissioner. If the code of practice diverges from the privacy principles set out in the legislation, it takes precedence over the legislation while it is in force. In urgent cases, the Commissioner may issue a temporary code which remains in force for up to one year.

One disadvantage to a self-regulatory approach of this nature is the enormous time and resources that are required to conduct consultations in developing industry-specific codes of practice. On the positive side, however, the process provides for flexibility in the development of the code of practice, and this may result in greater commitment to adhering to its requirements on the part of the industry.

3.3.5 Hybrid Models with Partial Registration/Sectoral Codes of Practice

3.3.5.1 Netherlands

The Netherlands Data Protection Act of 1989 is based on a general registration scheme which distinguishes between private and public sector personal data files. Particulars about personal data files held in either sector must be registered with the Registration Chamber unless the files come within certain defined categories (e.g., pay-roll systems, subscription lists). Although the basic data protection principles set out in the legislation apply equally to the public and private sectors, the registration procedure differs between the two sectors.

The Registrar has the authority under the legislation to conduct investigations that are self-initiated or at the request of a third party. On the basis of an investigation, the Registrar can make a recommendation to the data controller. Decisions of the data controller can be appealed to the courts. Breaches of the act are offences that are subject to fines and compensation for damages. Decisions, statements, announcements or recommendations of the Registration Chamber are not subject to administrative appeal.

The data protection legislation also contains provisions for some measure of self-regulation through sectoral Codes of Conduct. Codes may be formally approved by the Registration Chamber but, unlike the codes of practice developed in Ireland and New Zealand, they are not legally binding. [238] The codes must conform to the minimum data

protection standards set out in the legislation and be developed by a body that is representative of the industry or sector. Once a code is approved, it can stay in effect for three to five years.

The Registration Chamber has reported that although the self-regulatory aspect of the data protection scheme began slowly, it is now gaining momentum. [258] About 10 codes have been established to date. Although it can take years to get all members of a particular sector or group in line, once agreed upon, the code applies to all members of the sector. The development of a code is generally perceived as desirable by organizations because, although a code is not legally binding, it provides organizations with a better assessment of the risks involved in certain data practices.

3.3.5.2 Ireland

The Irish Data Protection Act sets out eight basic data protection principles with which public and private sector data controllers must comply. Certain data controllers, particularly those that collect sensitive information, are required to register certain particulars about their data holdings. The restricted registration scheme applies to three major groups - public sector organizations, financial organizations and other individuals and organizations holding sensitive data. However, other provisions of the statute also apply to other forms of personal data which do not require registration. Some difficulty has been encountered by the Commissioner in correcting a general misunderstanding that the legislation only applies to personal data which require registration. [258]

The Data Protection Commissioner is responsible for enforcing the legislation. The Commissioner may conduct investigations on his own initiative or at the request of a third party. Following an investigation the Commissioner may serve an enforcement notice. Failure to comply with the notice is an offence, which is subject to a fine.

There also are provisions for trade associations and other bodies representing categories of data controllers to develop their own Codes of Practice. These codes may be formally approved by the Data Protection Commissioner (this is desirable rather than essential) and then be tabled in Parliament. If Parliament approves a code, it is then deemed to be a statutory instrument. [238]

3.4 FAIR INFORMATION PRACTICES: SETTING THE CANADIAN CONTEXT

3.4.1 Model Based on Voluntary Self-Regulation (Canada)

In 1984, Canada formally agreed to adhere to the OECD Guidelines. The privacy protection principles set out in these guidelines are reflected in the federal Privacy Act [152] and in most provincial data protection legislation. These data protection laws put limitations on the collection, use and disclosure of personal information by government bodies. The independent offices of the federal Privacy Commissioner and provincial data

protection authorities, oversee the administration of the legislation pertaining to their respective jurisdictions.

With the exception of Quebec, there is no provincial legislation encompassing privacy protection principles for the private sector. There is a patchwork of federal and provincial laws which contain sections that provide some protection for personal information held by organizations in specific sectors.

This typically North American approach of enacting legislation to deal with industry specific problems has been characterized as "remedial", "retroactive" and "ad hoc". [260] Although sector-specific legislation may provide some protection, it generally fails to fully embrace fair information principles, such as those set out in the OECD Guidelines. In addition, there is usually no oversight mechanism, such as a supervisory body to oversee compliance with the legislation. In the absence of an oversight body, enforcement of sector-specific legislation will depend on the courts.

However, it has been noted that privacy is a complicated and specialized business, too important to be left to the courts. [130] Not only are the courts not equipped to handle privacy issues on an ongoing and systematic basis, but under a court-enforced data protection system, all but the most determined litigants may be deterred by the high cost of private litigation and the difficulties of recovering legal costs.

3.4.2 Model Based on Mandatory Regulation

In September of 1996, the Government of Canada committed to extend privacy protection to the private sector by the year 2000. In October of 1998, the Canadian federal government introduced the Personal Information Protection and Electronic Documents Act. The Act received Royal Assent on 13th April, 2000 and is intended to introduce measures to protect personal information in the private sector, create an electronic alternative for doing business with the federal government and clarify how the courts assess the reliability of electronic records that are used as evidence. Having legislation that establishes a set of common rules for the protection of personal information will assist in building consumer confidence and create a level playing field for the public and private sectors, with clear and predictable rules for business. The provisions of the Act are based on the CSA Model Code for the Protection of Personal Information. The Act will initially apply to the federally-regulated private sector. Three years after coming into force, the provisions will apply more broadly to all personal information, collected, used or disclosed in the course of commercial activities.

The purpose of the Personal Information Protection and Electronic Documents Act is to establish rules to govern the collection, use and disclosure of personal information in a manner that balances the right of privacy of all individuals with the need of organizations to collect, use or disclose personal information for a reasonable purpose. This is necessary in an era in which technology increasingly facilitates the circulation and exchange of information.

The Act will apply to all organizations that collect, use or disclose personal information in the course of commercial activities. It will apply in two phases. For the first three years after coming into force, it will apply only to organizations in the federally-regulated private sector, including employee information in those organizations, and to international and inter-provincial trade in personal information where the information itself is the subject of the trade. After these three years, the provisions will apply more broadly to all organizations that collect, use, or disclose personal information in the course of commercial activities and to all interprovincial and international flows of personal information. Where and whenever a province adopts legislation that is substantially similar, the organizations, classes of organizations or activities covered will be exempted from the application of the federal law for intra-provincial transactions. There is one exception to this timetable. The Act will start applying to organizations collecting, using or disclosing personal health information one year after coming into force, so as to give the health sector more time to prepare to comply with the new legislation.

The privacy provisions do not apply to individuals collecting, using or disclosing personal information for domestic or personal purposes nor does it apply to collection, use, or disclosure for journalistic, artistic or literary purposes.

The privacy provisions are based on CSA International's Model Code for the Protection of Personal Information, recognized as a national standard in 1996. The Standard

addresses the ways in which organizations collect, use and disclose personal information. It also addresses the rights of individuals to have access to their personal information and to have it corrected if necessary.

Some groups, such as law enforcement agencies, have a lawful or investigative need to collect, use and disclose personal information without having to obtain the consent of the concerned individuals. For these reasons, certain exceptions to the consent requirement are included, for example:

- if the action clearly benefits the individual or if obtaining permission could compromise the information's accuracy;
- where such data can contribute to a legal investigation or aid in an emergency where people's lives and safety could be at stake; and
- if disclosure aids matters of legal investigation or facilitates the conservation of historically important records.

Individuals will have the right to complain about any aspect of an organization's compliance with the provisions relating to the protection of personal information to the federal Privacy Commissioner. The Commissioner will have general powers to receive and investigate complaints, and to attempt dispute resolution. Unresolved disputes relating to certain matters can be taken before the Federal Court. In addition to its normal powers, the Court may order an organization to correct its practices and award damages to the complainant. The Privacy Commissioner will have a mandate to develop and conduct information programs to foster public understanding of the privacy provisions of

the Act. The Privacy Commissioner will report annually on the application of the provisions on personal information and on the investigation of complaints. The privacy provisions of the Act will be reviewed every five years after the coming into force of the legislation by a Committee of the House of Commons, or of both Houses of Parliament.

The only jurisdiction in Canada that is exempt from the Personal Information Protection and Electronic Documents Act is the province of Quebec, which was the first jurisdiction in North America to enact comprehensive data protection legislation for the private sector. The Act Respecting the Protection of Personal Information in the Private Sector sets out fair information practices for businesses operating in Quebec. This legislation, in conjunction with several sections of the Civil Code which proclaim a broadly worded right to privacy, forms a comprehensive approach to data protection. As Quebec's existing privacy law is substantially similar to the proposed Personal Information Protection and Electronic Documents Act, Quebec will be exempt from it's application.

The second part of the Personal Information Protection and Electronic Documents Act address the adjustment of the legal framework for electronic commerce. Existing federal statutes and regulations often specify that information must be given "in writing", "certified" or "signed". These types of references can be interpreted as restricting transactions only to paper and preclude the possibility of transmitting information electronically.

The Department of Justice reviewed over 600 federal statutes and found that 300 of these made references to obtaining or sending information in a way that appeared limited to paper. However, as communication becomes increasingly paperless, the dependence on paper becomes outdated and cumbersome. The legislation provides a way to adapt existing federal statutes and regulations so that they are compatible with an electronic environment. In other words, it provides a way to adjust or apply current laws so that there is an electronic alternative to transmitting information. The legislation gives federal departments, agencies and boards the authority to decide how requirements in existing statutes and regulations can be satisfied by electronic means in place of paper. A key component of the legislation is the concept of "secure electronic signature" which may be used in electronic transmissions to ensure their integrity and reliability. The concept of a secure electronic signature will also provide the base requirement for being able to apply informed consent processes within the electronic environment.

Another element of the Personal Information Protection and Electronic Documents Act concerns electronic documents that are introduced as evidence in court proceedings. Although electronic documents presented as evidence is not new, electronic technology has affected how lawyers and judges interpret the rules of evidence. The Act clarifies how the courts assess the reliability of an electronic document that is introduced as evidence, and, assists courts in recognizing secure electronic signatures and how they are used in relation to electronic documents.

Federal departments, agencies and boards will need to adjust their existing statutes and regulations before they are in a position to deliver their services on-line. The intent of the legislation is to provide consumers with an understanding of what happens to their personal information in the global information society, and to allow consumers to make informed decisions about which organizations to trust. In turn, this legislation is intended to enhance the reputation of Canadian businesses, both nationally and internationally, as being trustworthy.

3.4.3 Private Sector Legislation in Quebec

The province of Quebec was the first jurisdiction in North America to enact comprehensive data protection legislation for the private sector. The Act Respecting the Protection of Personal Information in the Private Sector sets out fair information practices for businesses operating in Quebec. This legislation, in conjunction with several sections of the Civil Code which proclaim a broadly worded right to privacy, form a comprehensive approach to data protection.

The chairman of the Commission d'acces a l'information which oversees both the public and private sector legislation . The legislation is perceived as practical and has been widely accepted by private sector organizations.

All private sector organizations operating in Quebec have been required to revise their policies and procedures to conform to the fair information practices set out in the new

legislation. Since it is not efficient for corporations to implement different policies for each jurisdiction, some businesses, both commercial and financial, have decided to extend the new information handling procedures based on the data protection standards of Quebec to all their Canadian customers. As a result of their experiences in adapting to the requirements of the Quebec legislation, some organization have expressed their preference for national data protection standards to ensure the policies and procedures they develop will not be made obsolete by the enactment of more stringent legislation in other parts of Canada. [248]

3.5 PRIVACY PROTECTION MODELS FOR THE PRIVATE SECTOR

3.5.1 Proposed Model Based on Marketing Principles

The preceding models are similar in that they are all based on a consistent set of fair information principles, specifically those set out in the OECD Guidelines. However, it has been suggested that new technological developments have rendered the conceptual basis for these models out of date, and that additional concepts and methods of privacy protection are needed to address the issues arising in the evolving technological environment.

One suggestion has been to strengthen the existing data protection framework in North America by moving towards the use of marketbased mechanisms of privacy protection in

which individuals own their personal information and trade this information on information markets. [194] This proposal is based on the assumption that privacy will continue to deteriorate as long as the cost of invading privacy is far lower than the true social cost. In an unregulated system, the costs to private sector organizations in terms of customer complaints and loss of business are outweighed by the commercial value of the personal information. However, there are additional costs to the individual, and to society as a whole, in terms of a loss of privacy that are rarely taken into consideration.

Under the proposed market-based model, individuals and organizations would not be able to use personal information for reasons other than supporting a current transaction without the permission of the persons involved, and the payment of compensation for this use. The market-based system would only apply to secondary and tertiary uses of personal information for purposes other than those for which it was gathered.

The rationale for a system involving royalties to compensate individuals for the commercial use of their personal information is that privacy will increase because the cost of invading privacy would go up. Individuals would have a better understanding of the flow of their personal information, more control over its uses, and could choose to withdraw from the market altogether. Since the principal enforcement mechanism would be the marketplace rather than a regulation agency, the new system is seen as being much more powerful and less wasteful. Once the infrastructure has been established, the cost of administering the system would be trivial. The market would essentially be self-supporting based on fees charged to participants.

Advocates of a market-based model of data protection argue that there is too much financial and political gain involved in the selling of personal information for the regulatory approach to work by itself. They propose that perhaps the least expensive and most effective way to protect privacy rests in markets and taxes on those organizations that are most likely to invade privacy rather than regulation funded through general tax revenues. However, while the market-based approach may help to minimize secondary and tertiary uses of consumer information with a commercial value, it is not clear how such a model would operate at an international level or be useful for addressing other privacy issues such as those that arise in the workplace or with respect to health care information.

3.5.2 Government/Private Sector Partnerships

As governments attempt to downsize and improve the efficiency of their operations, processes such as privatization and the contracting out of government functions are eroding the distinction between the public and private sectors. By example, the federal government has committed to establishing alliances with private sector enterprises in their strategies to "renew" government through the application of information and telecommunication technology. In a discussion paper issued by Treasury Board of Canada entitled "Blueprint for Renewing Government Services Using Information Technology", one of the proposed business principles involves the development of partnerships with the private sector.

Private sector organizations are increasingly performing what were once strictly government functions. To carry out these functions, particularly those involving applications of information and telecommunications technology, private organizations often require access to public data. However, since private sector organizations are not generally required to adhere to the same data protection standards as public sector organizations, the free movement of information between these two sectors poses a threat to privacy.

Contractual agreements established on a case-by-case basis are one mechanism which might be used to help ensure that personal information is handled in accordance with fair information practices. However, perhaps a more efficient alternative would be to require private sector organizations to adhere to the same data protection rules as government organizations through the enactment of private sector legislation. This would not only minimize barriers to the free flow of information between public and private sector organizations involved in these partnerships, but offer the maximum benefits in terms of data protection.

3.5.3 Public Support for Stronger Privacy Protection

While there is no direct evidence that the North American approach, characterized by a patchwork of sectoral legislation and voluntary codes of practice, is a less effective means of protecting privacy than the legislative approach adopted by European nations, a

number of public opinion surveys conducted in Canada clearly indicate that our current framework is perceived as being inadequate, particularly as it relates to the private sector.

The "Equifax Canada Report on Consumers and Privacy in the Information Age" (1994) indicated that a significant majority of Canadians feel that consumers have lost control over the circulation and use of their personal information by companies. Similarly, "Privacy Revealed: The Canadian Privacy Survey" (1992) conducted by Ekos Research Associates indicated a high degree of concern about privacy and a widespread belief that there is less privacy today than there was a decade ago. The study concluded that Canadians want to feel comfortable that someone is looking after their interests and prefer government regulation to voluntary self-regulation by businesses. A Gallup Canada survey for Andersen Consulting, "The Information Highway: What Canadians think about the Information Highway" (1994), revealed a very high degree of concern about privacy in relation to the information highway of the future. A 1995 survey conducted by the Public Interest Advocacy Centre and the Federation nationale des associations de consommateurs du Quebec, "Surveying Boundaries: Canadians and their Personal Information", found that Canadians generally lack confidence in private sector self-regulation and view legislation as an important part of the solution to the problem.

Support for tougher data protection regulation of private sector organizations has also been expressed by federal and provincial data protection authorities who currently oversee legislation pertaining to government organizations. In the 1993 Annual Report, the Information and Privacy Commissioner/Ontario called for legislation covering the

collection, use and disclosure of personal information for the private sector in the province of Ontario. The federal Privacy Commissioner, in his 1994-95 Annual Report, called upon the federal government to extend the Privacy Act to those areas of the private sector which fall within its jurisdiction and to convene a federal/provincial working group to seek harmonization of privacy laws in the private sector under provincial jurisdiction. The Information and Privacy Commissioner for British Columbia, in his 1993-1994 Annual Report, called upon the government and the private sector in that province to consider the implications of the EU Directive.

The Information Highway Advisory Council recognized the need for a national standard as to what constitutes effective privacy protection in an electronic environment. In its final report, "Connection Community Content: The Challenge of the Information Highway", it recommended that the federal government take a leadership role in creating a legislative privacy framework for both public and private sectors. The recommended legislation would require sectors or organizations to meet the standards set out in the Canadian Standards Association model privacy code.

Support for data protection legislation covering the private sector has also been expressed by the business community. The Canadian Direct Marketing Association (CDMA) was the first industry group in Canada to call on the federal government to enact a set of privacy principles as framework legislation for each industry sector to use in developing a code. The CDMA subsequently plans to ask each province, except Quebec which

already has private sector legislation, to enact identical laws to govern the private sector within its jurisdiction. [251]

3.5.4 Voluntary Codes

In the absence of legislated privacy protection standards for private sector organizations, a number of industry groups and individual organizations have attempted to implement fair information practices by adopting voluntary guidelines. In this context, the term "voluntary code of practice" is used to refer to a variety of codes that do not have statutory status. The term is not meant to imply that there are no factors compelling compliance with the code. Compliance may be a prerequisite for membership in a particular association and, therefore, some organizations/associations may not view these codes as being "voluntary."

For example, codes of practice have been adopted by the Canadian Direct Marketing Association. Canadian Bankers Association, Canadian Life and Health Insurance Association, and the Insurance Bureau of Canada.

Voluntary codes of practice appear to be the preferred approach of the business community. Businesses argue that this self-regulatory approach works because consumers demand privacy and businesses recognize that good privacy practices are good for business. [248]

The major advantage to self-regulation is its flexibility. Advocates of self-regulation argue that a more rigid regulatory approach cannot take into account the many ways in which advances in technology and innovative uses of personal information might have an impact on privacy. Regulation would become quickly outdated and require the lengthy process of enacting new laws or regulations. With self-regulation, the business community can rapidly develop and implement appropriate policies and codes of conduct in response to emerging issues. Furthermore, this more flexible approach avoids the establishment of procedures that may be justified in relation to one business sector, but inappropriate in relation to another.[346]

Voluntary codes also allow businesses to balance privacy with other competing interests and the everyday practicalities of data processing and use. [138] For example, voluntary codes can be developed to reflect operational realities such as the need to control costs while maintaining excellent customer service. Consequently, private sector organizations may be more likely to abide by a code of practice which they create than one which is imposed on them by government.

From the consumer's perspective, there are also a number of potential advantages to the voluntary approach. For example, since voluntary codes are often industry and issue specific, they tend to be more focused, detailed and relevant in comparison to government legislation. Also because they tend to be administered at a level where disputes between consumers and industry are likely to occur, consumers may have better access to redress than that which is provided through legislation. [126]

Another potential benefit of voluntary self-regulation is that it can create a moral obligation without establishing bureaucratic structures. [73] As a result, voluntary codes require little outlay of public funds and tend to be the preferred approach of governments operating under tight fiscal restraints.

On the other hand, the limitations of voluntary codes have been noted by both consumer and privacy advocates. The lack of meaningful enforcement measures and/or an appeal mechanism to an independent third party has been identified as one of the most serious limitations of voluntary codes. Even where there is some form of review or complaint handling mechanism, sanctions for non-compliance are often ineffective or non-existent. Consumer pressure and moral suasion are usually the only mechanisms available for inducing compliance with a voluntary code of practice. Remedies for breaches of the code, such as the correction of inaccurate information, may also be inadequate. Furthermore, although self-regulatory agencies may provide useful services for consumers, these bodies may not fulfill all of the functions of an independent mediator such as a data protection authority.

Another limitation is that voluntary codes do not cover all private sector organizations. Voluntary codes are just that - voluntary. This means that industries/organizations may choose not to have a code of practice, and even where a code exists, organizations may choose not to abide by it.

Another objection to industry/organization codes of practice is that they sometimes fail to incorporate objectively fair standards for data protection. This may be attributable to a lack of consultation with data subjects throughout the development of a code. Unless they are required by law to do so, industries/organizations may only do the minimum necessary to deflect further action by the public and government authorities. As a result, a privacy code may not cover all types of personal information maintained by the organization, it may not provide protection for both consumers and employees of the organization, or it may permit broad disclosures of personal information where it is in the interest of the organization to do so.

Research has pointed to a number of weaknesses in the codes of practice adopted by Canadian organizations. For example, one study of 16 codes of practice adopted by Canadian associations or corporations in response to the requirements of the OECD guidelines found that all codes were strictly voluntary, with no enforceable rights. [260] There was a widespread practice within large corporations of obtaining blanket consent for any eventual request or exchange of data. Consent forms rarely specified the rights of notice of transfer, access to, or correction of data. The study also noted that there were weaknesses in the notification of disclosure of personal information to third parties in the codes of practice and that existing remedies to deal with invasions of privacy were inadequate.

Another study of 12 national voluntary codes, found similar results. [126] The study concluded that, from the perspective of consumers, the codes were not an adequate means of protecting privacy. Common problems included the following:

1. low consumer involvement in code development;
2. consumer exclusion from code administration;
3. administration at either the firm or industry level;
4. low use of publicity as a compliance tool;
5. inadequate code coverage;
6. inadequate monitoring;
7. low levels of compliance;
8. weak sanctions; and
9. no ultimate means of consumer recourse.

The limitations of voluntary self-regulation led the Australian Law Reform Commission to conclude that "where large vested private financial interests are involved, voluntary agreements and self regulation simply do not work as a protection of consumer interests". [15] Similarly, the Canadian Department of Communication/Department of Justice Task Force on Computer Privacy concluded that the potential appeal of voluntary self-regulation is "too limited to be relied on as the principle means of protecting privacy." [73] The United Kingdom Committee on Data Protection also noted that "a wholly voluntary approach would not suffice" and that compliance with codes of practice should be compulsory rather than voluntary.

In spite of their limitations, voluntary codes of practice are expected to play a growing role in Canada. Both their number and effectiveness are expected to increase as industry groups attempt to forestall government legislation by adopting self-regulatory measures. Even if private sector data protection legislation is implemented throughout Canada by 2004, voluntary codes are seen as an important first step in this process and can help form the basis for the legislative framework. In recognition of the increasing importance of their role for protecting privacy in the private sector, there have been a number of recommendations for strengthening voluntary codes of practice.

The Public Interest Advocacy Centre, following a study of voluntary codes in Canada, recommended that improvements are needed in the following areas:

1. consumer inclusion;
2. independence of administration;
3. availability of resources;
4. public accountability;
5. sanctions and consumer recourse; and
6. government support.

One proposed mechanism for strengthening consumer recourse would be to declare codes of practice as contracts between consumers and those organizations that adopt them. In addition, each business that endorses a particular code of practice could refer to it in its

contracts with customers. By including such provisions within the code of practice and/or within customer service contracts, companies create legal rights for their customers and expand the range of redress mechanisms available.

Transforming voluntary codes into contractual agreements governing the use and disclosure of personal information would help to address the criticism that voluntary privacy codes are meaningless in the absence of certain legislated rights. However, while the threat of legal action may be a strong incentive to comply with a code of practice, such mechanisms should not be viewed as a replacement for other more readily accessible means of recourse, such as complaint resolution through an independent oversight body.

It should also be recognized that the contractual approach to data protection may have limited application in the broader contest of personal information held by private sector organizations. The competitive advantage that may be gained by establishing contractual agreements to adhere to fair information practices with respect to customer information may not exist with respect to other types of personal information that private sector organizations collect, retain, use and disclose. For example, there may be little incentive for private sector data users to establish legal rights for data subjects through contractual agreements in the context of employee records or health care information.

3.5.5 Potential Implications of Extending Privacy Protection to the Private Sector

Currently privacy protection in the private sector depends on a patchwork of federal and provincial legislation, in combination with voluntary codes of practice. However, in light of recent national and international developments in information technology and data protection, the adequacy of this framework has been questioned.

One strategy for addressing the concerns that have been raised would be to strengthen the existing framework. For example, more sector-specific legislation and regulations could be implemented to address industry-specific issues. Along with the staged implementation of the Personal Information Protection and Electronic Documents Act, voluntary self-regulation could be elevated to a new level via the development of codes of practice that incorporate national data protection standards and meaningful enforcement and/or appeal mechanisms. Enhancements such as these are an important first step in implementing effective data protection on the part of private sector organizations. However, in the long run these solutions alone may not be sufficient to address all of the concerns, particularly those that have been raised internationally. Eventually, a legislative framework may be required.

The models provided by data protection legislation enacted in other jurisdictions will be instructive in deriving a framework best-suited to the cultural context and legal traditions of Canada. These models range from the restrictive licensing model of Sweden, at one

extreme, to the more flexible self-regulatory model of New Zealand, at the other. Between these two models lie a variety of other models, some involving partial registration schemes, and others combining partial registration schemes with self-regulation through sectoral codes of practice.

Although strict licensing and registration schemes may enhance the openness of information handling practices and can potentially permit a data protection authority to be self-funding, it has been suggested that this type of approach may be too restrictive for the private sector in North America, which prefers a minimal amount of government intervention. Furthermore, even among European nations, there has been a trend away from licensing schemes because they require considerable resources to administer and, in and of themselves, do little to enhance privacy. The trend may reverse as a result of the EU Directive which requires data controllers to notify a supervisory authority before starting an automated data processing operation. Nevertheless, a limited registration scheme, such as that which exists in the province of Quebec, may be useful for increasing the transparency of information practices of specific sectors, such as the credit reporting industry.

A legislative framework that incorporates some degree of self-regulation may be more palatable to private sector organizations within the North American context. Self-regulation can be achieved through the inclusion of provisions for developing industry-specific codes of practice, such as those of New Zealand or the Netherlands. Although the development of these codes would require intensive consultations with stakeholders, the

end-product may be a more flexible and relevant code that industry would be more inclined to comply with in comparison to government imposed regulations. The voluntary codes of practice that have already been developed and implemented by some Canadian industries could provide a starting point for this process. Alternatively, the legislative framework could incorporate sector-specific regulations derived through consultations with industry representatives during the drafting stages. For example, the Quebec statute contains specific rules with respect to personal information agents who establish files of personal information on a commercial basis and prepare and communicate credit reports to third parties.

If the legislative framework contains provisions for establishing sector-specific codes of practice, there are various options for how such codes can be implemented. Once established, codes of practice can be legally binding on all members of the sector, or merely provide more detailed guidance on how to implement the fair information practices set out in the legislative framework. In addition, regardless of whether the codes of practice are legally enforceable, the approval of a data protection authority may or may not be required.

To the extent that codes of practice are legally binding on all members, careful consideration must be given to clearly specifying the parties to which the code should apply. This task is becoming increasingly complex in the Canadian context as the distinctions between the various sectors are obscured through processes such as deregulation in the financial services and telecommunications services industries.

Moreover, codes that are legally binding may involve a lengthier and more bureaucratic process of development in comparison to codes that are intended only to provide more specific guidance. On the other hand, a code of practice that lacks the force of law may be more likely to fail to meet the minimum requirements set out in legislation, and thus be open to challenges. For example, a case arose in the United Kingdom where the Registrar does not endorse but encourages the development of codes of practice. A code of practice for direct marketing was found to be inconsistent with one of the fair information principles in the legislation rendering the function and meaning of the code ambiguous. This could be the case even if a code of practice was endorsed by a data protection authority.

Many data protection models incorporate an independent authority for implementing and enforcing data protection principles. The data protection authority may take on a variety of roles. For example, the data protection authority may be responsible for licensing and registration, receiving and mediating complaints, advising data users and data subjects, making recommendations, issuing binding orders, and imposing civil and criminal sanctions.

It has been suggested that to the extent that a data protection authority has the legal power to make decisions, issue orders, and impose civil and/or criminal sanctions for non-compliance, that authority may be less effective as a privacy advocate or advisor. The rationale for keeping these roles separate is that such powers may force the supervisor body into adversarial rather than cooperative relationships with data users. This may

constrain the supervisory body in offering advice and opinions as a privacy advocate and advisor. Therefore, in many legislative models which incorporate an independent authority, arbitration and enforcement of privacy protection principles are left to the courts.

However, since court-enforced remedies may not be accessible to the average citizen, it has also been argued that it is preferable to provide the data protection authority with sufficient powers to resolve issues and enforce compliance with the legislation. To the extent that they are used with discretion, such powers need not diminish the capacity of the data protection authority to establish cooperative relationships with data users or to fulfill its functions as a privacy advocate.

Regardless of whether they are imposed by a data protection authority or a court, it has also been noted that strong criminal and/or civil sanctions for violations may not be an appropriate means of ensuring compliance with fair information practices. Many data protection schemes set up a system of responsible keepers or data custodians. Ultimately, the effectiveness of such systems rests in the voluntary compliance of the responsible keepers. When the practices of the responsible keeper are brought into question, the power of persuasion is often sufficient to ensure compliance with fair information practices. Arguably, the inclusion of strong measures to enforce compliance may be counterproductive, since such measures may be perceived as an inappropriate mechanism for encouraging information keepers to respect the trust obligations attached to their roles. This led the Privacy Committee of New South Wales, Australia to conclude that the

primary strategy of data protection legislation should be education rather than punishment. On the other hand, it has also been recognized that the potential to impose such sanctions and remedies may serve a useful function in relation to the most willful and extreme violations of fair information practices.

In Canada, the issue of private sector data protection legislation is complicated by questions about jurisdiction. While the protection of privacy may generally fall under provincial jurisdiction, quite often the context in which data are collected, used and disclosed extends beyond provincial borders. For example, the federal government has jurisdiction over extra-provincial works and personal information concerning telecommunications, national statistics, transportation, finance, and criminal law. Therefore, privacy issues arise that concern both levels of government.

In Quebec, the jurisdictional issue has arisen with respect to the banking sector. Although the federally-regulated banks have agreed to abide by the spirit of the legislation, they do not believe that they are statutorily obliged to do so. However, others have argued that in the absence of federal legislation on the subject matter, provincial laws, validly enacted, apply to both federal and provincial undertakings unless the legislation interferes with the federal operation. Therefore, to clarify any jurisdictional issues and to ensure that all private sector organizations are covered, both federal and provincial legislation may be required.

Uniformity in a national data protection system is often perceived as a desirable end in itself. However, it has been argued that such a requirement can result in rigidity, "lowest common denominator" standards, and limit the scope for innovation. With respect to public sector legislation in Canada, since various pieces of legislation were enacted at different points in time, refinements in drafting style have led to an improving standard of privacy protection over time. Although, it would be beneficial to harmonize private sector data protection standards across Canada through the development of a uniform model statute and/or a federal statute that could serve as a model for provincial legislation, this need not inhibit the individual provinces from undertaking an initiative to independently enact its own private sector privacy legislation. [251]

3.5.6 Trends in the application of Fair Information Practices

Although the staged implementation of the Personal Information Protection and Electronic Documents Act will extend privacy protection to the private sector by the year 2004, the present application of fair information practices within GIA and the application of GIS technology is governed by the patchwork of federal, provincial and territorial legislation on access to information and protection of privacy.

GIA and the use of GIS provides a spatial and possibly temporal base upon which to conduct extensive exploratory data analysis. The information highway has opened avenues to access and analyse a diverse range of information sources. Gatekeepers on the information highway have begun to assess the market value of providing access to these

information sources and charging mechanisms are rapidly being filtered into the processes for accessing information. Arguments around property rights in information, privacy rights for data subjects and the ethical use of these information resources are somewhat less tangible, yet equally critical to ensuring equitable access to information.

On a parallel course, as governments have continued to attempt to scale down in size in recent years in response to decreasing budgets, user pay principles have continued to gain profile in government programs. In many agencies, data are viewed as an untapped commodity of value to a society that is increasingly oriented to integrated information resources management. As the broker or user of information, the security of data, the management of uncertainty in the data and the reliability of the resulting integrated information products is non-trivial in securing the integrity of decisions and decision-making in government.

Access to information and protection of privacy legislation has provided the framework for a set of fair information practices to be applied to information resources held largely by government. The introduction of privacy protection for the private sector has the potential to result in significant alteration to the legislative or regulatory environment, the business environment and the information management practices that could be applied to information with the implementation and operation of GIS. Extending privacy protection to the private sector would likely result in all Canadian information holdings being subject to fair information practices.

GIA and the process of it's evolution has provided a forum for unparalleled communication between professionals from previously disparate disciplines. The use of GIA by this wide variety of disciplines has maintained the momentum for the continued expansion of applications and evolution of the GIS technology. The lack of controls over the access, aggregation and use of information, with the exception of a limited number of disciplines, has created an increasingly uncertain future for geographic information analysts in the private sector.

As the sophistication of the techniques of GIA have increased, the right to privacy of data subjects has continued to erode. There is a general perception that the current data protection framework, consisting of some sectoral legislation and voluntary codes of practice, does not provide sufficient safeguards against the inappropriate collection, retention, use and disclosure of personal information by private sector organizations. There also is concern that this framework may become increasingly inadequate over time, as a result of future developments in information technology and data processing techniques.

Although the development of more effective voluntary codes of practice is encouraged as a first step toward data protection in the private sector, the limitations of the strictly voluntary approach make it an inadequate long-term solution to privacy issues. Comprehensive data protection legislation will provide the most effective means of protecting privacy. Alternatives range from adopting a licensing or registration scheme such as those of some European nations, to the more flexible private sector models that

provide some degree of self-regulation through sectoral codes of practice and which have been successfully implemented in other jurisdictions. A combination of a legislative model based on self-regulation through sectoral codes of practice in conjunction with an independent oversight agency would also be a viable model to consider.

Despite fair information practices having been included in most Canadian access to information and protection of privacy legislation, extending these principles to the regulation of information management practices in the private sector would represent a significant shift in culture for the typical Canadian geographic information analyst. We appear to have reached a new threshold with regard to the regulation of the flow of personal information. New thresholds in privacy protection result in striking new balances with access to information, which redefines the environment for the application on enabling technologies such as GIS and reshapes the wave of information available for GIA by the geographic information analyst.

4.0 DATA COLLECTION AND ANALYSIS

4.1 IDENTIFICATION OF STAKEHOLDERS

In order to conduct a systematic review of the infrastructure for geographic information management in the Canadian federal and provincial governments, several stakeholder groups will have to be identified in each jurisdiction.

For most federal and provincial jurisdictions these stakeholder groups may be identified as:

1. Office of the Chief Information Officer
2. Office of Policy on Information Management
3. Office of Policy on Access to Information and Protection of Privacy
4. Office of the Information and Privacy Commissioner
5. Office of Information Registries and/or Information Brokerage
6. Selected offices dedicated to Geographic Information Management and Analysis

The researcher recognized that apart from the policy and operational areas in information management and analysis listed above, business areas such as information technology, information systems, security, finance and risk management all exert considerable influence on the resulting geographic information management and analysis practices. In

addition, the researcher recognized that a comparable set of stakeholders may exist for the Quebec private sector.

4.2 RESEARCH METHODOLOGY

The methodology applied in this research involves a simple two-part qualitative survey of Canadian jurisdictions. The objective of the first part of the survey was to determine whether a structured approach to information management presently is applied in the area of geographic information management. The objective of the second part of the survey was to determine whether fair information management practices presently are followed in the geographic information analysis that is conducted within the geographic information management framework.

A survey of Canadian geographic information management practices was undertaken to determine the relationship between geographic information management frameworks and the nature of the GIA that is conducted within the bounds of these frameworks. The survey was comprised of a literature review, a mail-out survey and personal interviews. The literature review and survey were focused on Canadian public sector geographic information management practices and the manner in which information management practices have been incorporated into procedures for geographic information analysis.

The primary mode of inquiry was a two-part survey, which was composed of mail-out and personal interviews. The structure of the survey was designed to identify:

1. the conceptual models for geographic information management;
2. the parameters for geographic information analysis;
3. the legislative, regulatory and voluntary codes of information management practices that presently are being used to regulate geographic information management and analysis;
4. the effectiveness and efficiency of the application of information management practices on the geographic information management and analysis;
5. innovative geographic information management practices that permits the most diverse and intensive forms of geographic information analysis without compromising information management practices; and
6. business areas in need of potential geographic information management remedies where geographic information is under-utilized or where geographic information analysis practices contravene information management practices.

The primary tool for the data gathering was the questionnaire. See Appendix 2.0 for details of the questionnaire. Secondary data gathering has involved telephone interviews. The telephone interviews were used primarily to clarify information contained in the questionnaires.

4.3 SURVEY ADMINISTRATION

The structure of the survey was designed to identify:

1. the respondent's conceptual models for geographic information management;
2. the respondent's parameters for geographic information analysis;
3. the legislative, regulatory and voluntary codes of fair information practices that are presently being used to regulate geographic information management and analysis;
4. the effectiveness and efficiency of the application of fair information practices on the geographic information management and analysis;
5. innovative geographic information management practices that permits the most diverse and intensive forms of geographic information analysis without compromising fair information practices; and
6. business areas in need of potential geographic information management remedies where geographic information is under-utilized or where geographic information analysis practices contravene fair information practices.

4.4 DATA ANALYSIS

The results of the mail-out survey and personal interviews provided a snapshot of geographic information management practices across Canadian jurisdictions between 1 January, 1999 and 30 June, 1999. Following from the survey of each of the six primary stakeholder groups in each of the federal, provincial, and territorial jurisdictions, the researcher has identified the areas of variation between the policies, practices and applications of GIA, GIS and information management practices across Canada. As

expected, the results are primarily qualitative in nature. Survey responses range from broad concepts in information management and trends to specific sets of geographic information management practices that are applied to sets of information systems that have been designed for the purposes of conducting geographic information analysis.

In order to consistently analyze each survey response as part of a cross-jurisdictional comparison, a three stage analysis was applied as follows:

Stage 1. analysis of the definition of the range of business activities conducted in each business area or jurisdiction;

Stage 2. analysis of the business rules or regulations that govern the management and analysis of the geographic information in each business area or jurisdiction; and

Stage 3. analysis of the design of the technical configuration of the information system to meet the range of business activities while conforming to the business rules that are specified in each business area or jurisdiction.

This three stage analysis was intended to be sufficiently generic to accommodate most systems for geographic information management and analysis. Although not all systems for information management or information analysis are developed using these three stages, many information system development methodologies have similar component stages. The intent in applying this methodology for analysis was to facilitate the consistent critical analysis of each case across all jurisdictions, to assist in comparison

and the assessment of the relative effectiveness and efficiency of the application of information management practices on the geographic information management and analysis.

Stage 1 of the analysis provided an assessment of the linkages and diversity of uses of the geographic information in each jurisdiction, and in some cases allowed for the identification of the conceptual model for geographic information management. Stage 2 of the analysis provided an assessment of the degree to which prescribed information management practices have been incorporated into the business model for geographic information analysis. Stage 2 of the analysis has facilitated the identification or definition of parameters for geographic information analysis in terms of the legislative, regulatory and voluntary codes of information management practices that are to be applied to regulating geographic information management and analysis. Stage 3 of the analysis was used to assess the potential under-utilization of geographic information and/or the potential for violation of the prescribed information management practices.

Collectively, all three stages of the methodology provided a consistent framework for identifying the distribution of innovative geographic information management practices that has permitted the most diverse and intensive forms of geographic information analysis without compromising fair information practices. Business areas in need of potential geographic information management remedies have also be identified where geographic information is noted to be under-utilized or where geographic information analysis practices contravene information management practices.

The analysis of the mail-out survey and interviews has thus resulted in a cross jurisdictional breakdown of the conceptual models for geographic information management and geographic information analysis in relation to the respective application of fair information practices. The following cross jurisdictional summaries are qualitative in nature and reflect the currents practices in jurisdictions across Canada.

4.4.1 JURISDICTIONAL SUMMARIES

4.4.1.1 Introduction

In administering the questionnaire, all questions were framed within a specific context. The context was described in terms of six definitions. Definitions were provided for Fair Information Practices, Geographic Information, Geographic Information Analysis, Geographic Information Management, Geographic Information Management Framework and Information Management Lifecycle.

The definitions provided in the questionnaire were as follows:

Fair Information Practices:

1. Accountability: An organization is responsible for information under its control and shall designate an individual or individuals who are accountable for the organizations compliance with the following principles.

2. Identifying Purpose: The purposes for which the information is collected shall be identified by the organization at or before the information is collected.
3. Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of information, except where inappropriate.
4. Limiting Collection: The collection of information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Limiting Use, Disclosure and Retention: Information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual. Information shall only be retained as long as necessary to for the fulfillment of those purposes.
6. Accuracy: Information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
7. Safeguards: Information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. Openess: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of information.
9. Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of the individual's information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individuals accountable for the organization's compliance

Geographic Information:

All information types that describe spatial and temporal relationships between objects.

Geographic Information Analysis:

Techniques in information analysis that allow users to determine the relationship between geographic information types.

Geographic Information Management:

Techniques in information management that are applied to the management of geographic information.

Geographic Information Management Framework:

A policy and/or organizational structure that is designed to address all aspects of managing geographic information through a complete information management lifecycle, including the collection, use, disclosure, security and disposition of geographic information.

Information Management Lifecycle:

A structured process that is designed to address all aspects of managing the information, including the collection, use, disclosure, security and disposition of the information.

4.4.1.1.1 Compilation of Jurisdictional Summaries

Within the context of the abovestated definitions, the questionnaire was administered across Canadian federal and provincial jurisdictions between 1 January, 1999 and 30 June, 1999.

Following from the jurisdictional summaries, the following composite cross-jurisdictional summaries were compiled.

4.4.2 Cross Jurisdictional Summary

As noted in Section 4.1, six sites in each of the provinces, territories and the federal government to which the surveys were administered were identified

Several jurisdictions opted to provide a co-ordinated response. There is evidence of considerable collaboration in several of the co-ordinated responses and in these case all six sites are shown as having responded to the survey. The average nonresponse rate for the questionnaire was 21 percent.

The structure of the following cross-jurisdictional summary will reflect the structure of the questionnaire.

4.4.2.1 Jurisdictional Setting

The federal government has had access to information and protection of privacy legislation in place since the mid 1980's. At the provincial and territorial level, all but the jurisdiction of Prince Edward Island have legislation in place that addresses freedom of information and protection of privacy with respect to the public sector. In some instances freedom of information and protection of privacy legislation is in the process of being implemented. As in the case of New Brunswick, protection of personal information policy has been in place for five years, legislation has been enacted, and, at the time of the survey proclamation was expected within the year. At the time that the questionnaire was administered, Quebec was the only jurisdiction in Canada that had comparable legislation in place that extends to the private sector.

In most jurisdictions, the focus of programs responsible for access to information and protection of privacy legislation appears to be on mechanisms for providing access to records. Expertise in the delivery of programs in access to information and privacy protection appears to reflect the focus on records management rather than information management. The distinction between records management, data administration and information management appears to be blurred in most jurisdictions.

Where strategies in information management do exist, the focus of programs in most federal, provincial and territorial jurisdictions appears to be primarily on the protection of personal information. Although provisions of most statutes dealing with access to information and privacy protection do address the protection of proprietary information, trade secrets and information of economic or strategic value, these information types are dealt with as discrete information sets.

Most pieces of legislation dealing with access to information and privacy protection do not address the information management issues associated with the relational nature of many automated information systems. As a result, the functionality of relational databases that allow the creation of integrated information products using spatial geographic data as a base with overlays of personal and non-personal data are not addressed in most pieces legislation dealing with access to information and privacy protection.

None of the jurisdictions have mandatory or voluntary codes of practice that regulate the collection, use, disclosure and/or retention of geographic information. Several jurisdictions acknowledged that voluntary codes of practice such as the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information, Canadian Bankers Association (CBA) and Canadian Direct Marketing Association (CDMA) effectively regulate aspects of geographic information management and the application of techniques in geographic information analysis. These codes of practice comply with fair information practices.

Many of the voluntary codes of practice mentioned above have evolved in the private sector in recognition of the growing concern expressed by private citizens for the potential for invasion of privacy that arises with the application of relational information systems and the increasing ability to create personal and nonpersonal profiles with merging of previously disparate data sets.

A guiding principle drawn from the discussion on the jurisdictional setting from across Canada is that:

- Government organizations should recognize public access to government-held information as a central underlying tenet of any program or service involving GIS technology. Before introducing any GIS application, the impact on access should be identified and assessed. Appropriate and effective measures (technological, legislative and policy) should be developed and implemented.

4.4.2.2 Modes of Geographic Information Management

Six of the thirteen jurisdictions acknowledged the existence of a Geographic Information Management Framework (GIMF) that has been established for the management of geographic information.

Examples of multidisciplinary jurisdiction-wide GIMF initiatives include the :

1) Canadian Spatial Reference System and Geodetic Survey in the Government of Canada;
2) Geographic Data BC in British Columbia;
3) Land Information Alberta (LIA) and Information Management Framework, Office of the Chief Information Officer in Alberta;
4) Manitoba Land Related Information System (MLRIS) in Manitoba;
5) Province of Ontario Land Registration Information System (POLARIS) in Ontario; and,
6) Land Information Management System under development by the Department of Government Services, Yukon Territorial Government.

In several other jurisdictions, extensive committee structures are in place to address issues of interagency co-operation, provincial co-ordination and standards setting in the areas of geomatics and geographic information standards. Examples of such structures within the province of the Nova Scotia include the GeoNova Advisory Committee which serves as a provincial co-ordinating body, and the Nova Scotia Information Standards Committee which addresses issues of interagency co-operation with input to federal, provincial, municipal, academic and private sector initiatives. Together these committee structures constitute the complex organizational structure for Nova Scotia's virtual GIMF.

Although respondents from several jurisdictions anticipate ongoing progress in the development and application of GIMFs that address the full information management lifecycle, significant numbers of respondents clearly were frustrated in their efforts to gain secured long-term funding and commitment from executive levels of government to jurisdiction-wide application of GIMFs. By example, ministry respondents for the Province of British Columbia confirmed that a Geographic Information Management Framework (GIMF) had been established for the management of geographic information in the Province of British Columbia. Ownership of the Information Management Framework (IMF) is now shared amongst various organizations and is administered by the Information, Science and Technology Agency. Work continues on maintaining compliance with the IMF. The IMF does not include the management of geographic information through the full information management lifecyle. It focuses on the management and distribution or access aspects of the data lifecyle. No specific legislative, regulatory or voluntary authority exists for establishing and/or maintaining the IMF. The IMF was developed through an interagency group. It was intended to become part of the British Columbia Government Management Operating Procedures (GMOP). Because geographic data differs from most information materials, there has been difficulty finding an impartial, knowledgeable party to administer the IMF. As noted above, at the time of administering the questionnaire the IMF resided with the Information, Science and Technology Agency but was basically dormant.

With the exception of the privacy protection legislation governing the Quebec private sector, no respondents acknowledged legislative, regulatory or voluntary authority for establishing and/or maintaining the GIMF with respect to the private sector.

The lack of legislative, regulatory or voluntary authority for establishing and/or maintaining GIMF's speaks to the general lack of appreciation for the benefits and controls that would derived be from positively controlling the collection, use, disclosure, aggregation and disposition of personal and nonpersonal geographic information.

The rigour required to follow a set methodology in information management would involve organizations being required to articulate the reasons for information collection along with the intended primary and secondary uses of the information. Most information management frameworks also include consideration of information accuracy, completeness, security and brokerage, along with metadata standards that are designed to assist in making sound decisions in resource and information management.

Two guiding principles drawn from the discussion on the modes of geographic information management from across Canada are that:

- Government organizations should use GIS technology to enhance access to government-held information. They should look to the introduction of GIS technology as a way of increasing the amount of information that is routinely distributed or actively disseminated.

- Government organizations should collect, use, retain, and disclose data in an anonymized or aggregate format whenever possible in their GIS applications.

4.4.2.3 Modes of Geographic Information Analysis

From the perspective of the federal government, no authority has been established to regulate the application of techniques in geographic information analysis. Although no authority exists formally within the context of GIMF organizations such as the Geodetic Survey Division of Geomatics Canada, there is a voluntary acceptance of authority that varies from province to province depending on the issue at hand. Agreement is negotiated on the consistent application of techniques. Once the agreement is in place it becomes the standard mode of operation for that jurisdiction, subject to acceptance by other concerned agencies within the province.

From the provincial perspective, provincial agencies appear to face similar challenges in standardizing modes of geographic information analysis. No authority has been established within the provinces to regulate the application of techniques in geographic information analysis. As a result, no provincial mandatory or voluntary codes of practice that would regulate the application of techniques in geographic information analysis have been established. Neither have sets of parameters been established for conducting geographic information analysis.

When questioned whether the authority for the regulation of the application of techniques in geographic information analysis and the respective code of practice extend to both the public and private sectors, provincial ministry respondents indicated that the extension to the private sector was a relatively recent phenomenon. In most cases data are gathered to support specific applications requirements. The specifications determine the accuracy, content and format of the data. Access to this information from 'outside' organizations is a relatively recent phenomenon, and ministry respondents conceded that this will require different management techniques.

The notable exception is the Province of Quebec where geographic information management practices that impinge upon adequacy of protection for personal information would be regulated by provincial legislation.

Without formally constituted GIMFs in place at the federal, provincial or territorial levels of government, little structure exists around which to fashion mechanisms to assess and subsequently approve or decline applications in geographic information analysis. The failure of most program managers in the areas of access to information and privacy protection to recognize the pivotal role played by successfully deploying a jurisdiction-wide GIMF, is compounded when faced with assessing applications in geographic information analysis.

Two guiding principles drawn from the discussion on the modes of geographic information analysis from across Canada are that:

- Government organizations should ensure that all GIS applications are designed in such a way that the public can exercise their access rights in a meaningful and timely manner.
- Government organizations should only use GIS technology to enhance government programs and services, and not as an instrument of social control or surveillance.

4.4.2.4 Application of Fair Information Practices

Federal, provincial and territorial ministry respondents confirmed that the management of geographic information is based on the application of fair information practices. Practices must comply with the respective federal, provincial or territorial legislation that addresses access to information and privacy protection, and to some extent the respective IMF or GIMF.

Although the management of techniques in geographic information analysis is based on the application of fair information practices, provincial ministry respondents clarified that there are specific overriding policies on data analysis. The results of such analysis would still be subject to the respective jurisdiction's legislation on access to information and privacy protection.

At the time that the survey was undertaken, the authority for the application of fair information practices extended only to the public sectors, with the exception of Quebec.

Provincial ministry respondents indicated that the existing codes of practice apply equally to personal and nonpersonal information. Although presently the bulk of geographic data is viewed as nonpersonal data, ministry respondents acknowledged that as the ministries move more into demographic, statistical and 911 information, attention to comprehensive management of personal information will become more of an issue. Banking, real estate, crime, marketing, monitoring systems for criminals and medical patients were all cited as information sets requiring additional attention with respect to the aspect of managing personal information.

As noted in the preceding sections on modes of geographic information management and modes of geographic information analysis, many of the survey respondents demonstrated a general lack of understanding of the potential linkages between nonpersonal land-based geographic information and person-based geographic information. Respondents did not appear to appreciate the linkages that are afforded by the manner in which GIS technology allows land-based spatial information to be the overlain with thematic layers of information that often contain personal information. Additionally, respondents failed to grasp the importance of the integrated information products that result from this functionality of GIS technology, and the capacity conduct further queries on these integrated information products with the application of techniques in GIA. The functionality of the GIS technology and the application of GIA challenges the bounds of current fair information practices in adequately protecting personal privacy.

Most provincial ministry respondents did not anticipate that the Government of Canada Personal Information Protection and Electronic Documents Act, or, the European Union Directive on Personal Data Protection (95/46/EC) would require significant changes to their codes of practice.

From the perspective of the federal government, when questioned on whether the codes of practice apply equally to personal and nonpersonal information, the respondent for the Geodetic Survey Division noted that although the survey does not capture personal information, the technical/scientific data do not fall under a code of practice that is as restrictive as the one that applies to personal information. While rules regarding intellectual property and cost recovery serve as examples of restrictions, there is also an effort to improve access and reduce related barriers to access this technical/scientific data. The respondent also clarified that the reasons for collecting a specific type of data can sometimes be related to the potential for somewhat undefined benefits. Creative use of the data would be encouraged.

Akin to provincial ministry respondents, no significant changes were anticipated to arise from the Government of Canada Bill C-54, Personal Information Protection and Electronic Documents Act, or, the European Union Directive on Personal Data Protection (95/46/EC), in relation to federal government codes of practice.

Collectively, these responses once again speak to the particularly narrow focus of most federal, provincial and territorial ministry respondents in relation to the broader national

and international context for geographic information management and analysis. Effective internal and external communication by public bodies and orientations for program managers to broader concepts in jurisdiction-wide models in geographic information management and analysis could significantly improve consistency in strategies in geographic information management and analysis at the federal, provincial and territorial levels of government.

Four guiding principles drawn from the discussion on the application of fair information practices from across Canada are that:

- Government organizations should provide public education on their GIS applications to ensure that the public can exercise their access rights in a meaningful and timely manner.
- Government organizations should conduct in-house education about the access implications of GIS technology for all staff involved in the development of the application or the delivery of related programs and services.
- Government organizations should recognize that information associated with a specific location may be privacy-sensitive.
- Government organizations should ensure that their GIS applications are open and transparent to the data subjects, and that the data subjects are aware of the existence of any technology or record-keeping system impacting their personal information.

4.4.2.5 Impact on Geographic Information Management and Analysis

Responses received from federal government ministries indicated that the application of fair information practices had affected neither the effectiveness nor efficiency of techniques in geographic information management nor techniques in geographic information analysis. No discernable differences between the public and private sectors were observed as affecting the effectiveness or efficiency of the application of fair information management practices on geographic information management or geographic information analysis.

In a comparable fashion, the application of fair information practices is viewed by provincial ministry respondents as neither having affected the effectiveness nor efficiency of techniques in geographic information management or geographic information analysis.

The affects of the effectiveness and efficiency of the application of fair information management practices on geographic information management do not appear to differ between the public and private sectors. Provincial ministry respondents noted that the public sector is much more aware of the broad reaching application of the access to information and protection of privacy legislation, and that information management practices are established accordingly. In general, this does not extensively impact geographic data. Geographic data are viewed as accessible for purposes of conducting common place GIA. Several provincial ministry respondents recognized that the discord will arise from the expert conclusions that are drawn from the GIS analysis.

As publicly-held information sets become more widely known through applications in GIA, these information sets are likely to be more frequently merged with other information sets and result in more contraversial, market-based and privacy-sensitive integrated information products. Expert use of these integrated information products usually results identification of trends or in an administrative use of the information that ultimately impacts the data subject. Demands from the public for more stringent application of fair information practices to protect personal privacy are often the result.

It is informative that at the time of administering the questionnaire, most provincial ministry respondents indicated that the affects of the effectiveness and efficiency of the application of fair information management practices on geographic information analysis do not appear to differ between the public and private sectors. Ministry respondents cautioned that all parties involved in geographic information analysis need to be held accountable for the conclusions that are drawn from the analysis, based on the input data.

Although the survey responses indicated a measure of concern over the relative lack of accountability for the resulting use of the information products resulting from GIA, few jurisdictions were able to provide any concrete recommendations on improving accountability models for geographic information management or geographic information analysis.

As noted in previous sections, the inability to address issues of accountability in geographic information management and geographic information analysis appears to stem from deficiencies in jurisdiction-wide GIMFs in most federal, provincial and territorial jurisdictions in Canada. Without the conceptual, structural or virtual basis of a jurisdiction-wide GIMF upon which to base strategies in geographic information management and geographic information analysis, faint recognition and little success seems to be accorded to existing initiatives in co-ordinated geographic information management and geographic information analysis. As a result, most respondents from federal, provincial and territorial levels of government appear to have reported few affects on either the effectiveness or efficiency of techniques in geographic information management or geographic information analysis.

Although the Government of Canada Personal Information Protection and Electronic Document Act had not been enacted at the time of the survey, it had been anticipated by the private sector for some time. As this private sector, privacy protection legislation is implemented in stages between 2001 and 2004, the increasing regulation of the private sector with respect to privacy protection is likely to drive the private sector to negotiate more clearly articulated privacy protection models for accountability as revenues and profit margins are impacted by legislative mechanisms in privacy protection. This trend was clearly not identified by most respondents to the questionnaire. Most respondents from federal, provincial and territorial levels of government reported no discernable differences between the public and private sectors on the affects to either the

effectiveness or efficiency of techniques in geographic information management or geographic information analysis.

Two guiding principles drawn from the discussion on the impact of geographic information management and analysis from across Canada are that:

- Government organizations should recognize the data subject as the owner of their personal information, and as a key stakeholder to be consulted when contemplating the introduction of GIS technology or the development of policies or practices that could potentially impact their privacy.
- Government organizations should ensure that the complexity or cost of GIS technology, the commercial value of the data, fees, or copyright, do not become an unreasonable barrier to public access to government-held information.

4.4.2.6 Innovations in Geographic Information Management

No innovations in techniques in geographic information management were attributed to the application of fair information practices by respondents from the federal government. When questioned on whether there are discernable differences, between the public and private sectors in the trends in innovations in geographic information management, the respondent for the Geodetic Survey Division, Geomatics Canada, Natural Resources Canada noted that there are differences due to the differing roles of the public and private sector. The respondent noted that the private sector develops products to suit an existing

or potential market, with competition and profit as significant driving forces. The public sector has a primary focus on the 'public good', and 'client focus' includes *additional features such as a longer term view and multi-tiered levels of clients. In fact,* the public/private sector relationship takes advantage of these roles to their mutual benefit. Innovations were viewed as a major factor in the success of both sectors. By example, the respondent noted that the public sector is typically involved in ensuring the development and availability of a globally consistent national spatial reference system while the private sector is developing products and services with a spatially-referenced component. The public sector is therefore increasingly involved in participating and contributing to the development of international services, and, takes advantage of leading-edge technology to ensure that the national spatial reference system will contribute to the realization of future benefits for Canada. By comparison, the private sector is typically involved in developing new products based on leading-edge technology and taking advantage of the new modes of access to the spatial reference system.

The federal government respondent for the Geomatics Canada noted that the development of an 'enabling environment' should heighten concern about fair information practices, but the latter in turn have little influence on trends in innovation for these developments due to the perceived limited impact on personal privacy.

Provincial ministry respondents appear to have shared a similar experience and indicated that the application of fair information practices is not viewed as having resulted in

innovations in techniques in geographic information management. Access to information is driven by a need to meet client demands. Reduced budgets and staff lead to innovative ways to provide information access. In addition, new technologies, such as the Internet, continue to change the way ministries conduct business. Emerging solutions in electronic commerce are anticipated to generate the funds required to implement such new technologies.

Provincial ministry respondents indicated that with innovations in geographic information management, more diverse and intensive forms of geographic information analysis were possible without compromising fair information practices. Much of the innovation is focused on the greater ability to access and integrate data within Geographic Information Systems.

No discernable differences were identified, between the public and private sectors, in the trends in innovations in geographic information management. Generally, newer technology facilitates cheaper, more efficient business solutions and often forms the underpinning of major system re-engineering. As such, these factors must be rationalized in the broader context.

Responses from federal, provincial and territorial agencies on issues of innovations in geographic information management were particularly traditional in nature. Limited recognition was expressed of the potential for further innovation in geographic

information management as the trend to privitization in the public sector increases and public/private enterprise solutions continue to evolve.

Seven guiding principles drawn from the discussion on innovations in geographic information management from across Canada are that:

- Government organizations should ensure that private sector involvement in GIS applications does not reduce public access to government-held information.
- Government organizations should ensure that their GIS databases are as accurate, complete and up-to-date as is reasonably possible.
- Government organizations should recognize the data subject as the owner of their personal information, and as a key stakeholder to be consulted when contemplating the introduction of GIS technology or the development of policies or practices that could potentially impact their privacy.
- Government organizations should provide public education identifying any privacy issues associated with the use of GIS technology, prior to implementation. They should also communicate their privacy protection policies and practices to the public in a manner that enables the public to exercise its rights.
- Government organizations should govern their GIS practices related to identifying information by established fair information practices, regardless of whether that information is considered "public."
- Government organizations should conduct in-house education about the privacy implications of GIS technology for all staff involved in the development of the application or the delivery of related programs and services.

- Government organizations should communicate their privacy protection policies and practices regarding GIS applications to all staff, and make staff accountable for adherence to those policies and practices.

4.4.2.7 Innovations in Geographic Information Analysis

Following from the response to innovations in geographic information management, no innovations in techniques in geographic information analysis were attributed to the application of fair information practices by federal government respondents.

Provincial ministry respondents noted that the application of fair information practices has not resulted in innovations in techniques in geographic information analysis. As noted in earlier discussion, the majority of responses to the questionnaire did not appear to reflect the broader context for potential innovations in geographic information analysis.

By example, the provincial government respondent for British Columbia noted that technology is driven by need, not by something 'neat to do'. No correlation was made with the effect of function creep, whereby innovations in the functionality of GIS technology fuel further innovations in modes of geographic information analysis. The respondent's inference was that geographic data, for the most part, has always been available. With relatively few restrictions on the access and use of geographic data, little incentive exists to pursue further innovations in geographic information analysis with a

view to facilitating the development of more intensive forms of geographic information analysis, without compromising fair information practices.

Typically, access to the data has not been viewed by the majority of provincial ministry respondents as a critical issue. The critical consideration for the majority of respondents from provincial and territorial levels of government has been the cost of the data. As a result, provincial ministry respondents saw no discernable differences, between the public and private sectors, in the trends in innovations in geographic information analysis.

Responses from federal, provincial and territorial agencies on issues of innovations in geographic information analysis were particularly traditional in nature and typically reflected a single purpose/single means approach to geographic information analysis. Limited recognition was expressed of the potential for further innovation in geographic information analysis as the trend to privitization in the public sector increases and public/private enterprise solutions continue to evolve. Despite the identification of the cost of data as a critical factor in limiting innovations in geographic information analysis, few respondents explored the opportunities to be derived with public/private sector cost sharing, information brokerages or other privacy-sensitive, revenue-generating applications that would address the concerns over the cost of data and facilitate further innovations in more intensive forms of geographic information analysis.

The extremely cautious responses received from the majority of respondents for federal, provincial and territorial agencies provides a sense of the limiting environment for

exploring options and innovations in geographic information analysis in the majority of public sector agencies. The perceived disjoint relationship between applications in geographic information analysis and fair information practices appears to stem recognition of the potential threats to personal privacy that are posed with geographic information analysis. Without a clear understanding of the potential risks to personal privacy that are posed with the deployment of increasingly intensive forms of geographic information analysis, most program managers perceive little need to explore innovative solutions in optimizing the application of techniques in geographic information analysis with compliance in fair information practices.

Three guiding principles drawn from the discussion on innovations in geographic information analysis from across Canada are that:

- Government organizations should ensure that the use of GIS technology and applications in GIA do not adversely affect the records management, data management or information management systems.
- Government organizations should review their GIS-related access policies and practices on an on-going basis to ensure that they are appropriate and effective in addressing the range of issues that are likely to arise with more intensive forms of GIA.
- Government organizations should ensure that, if a proposed GIS or GIA application has the potential to modify information management practices in a way that might compromise existing levels of privacy, appropriate methods of

restoring any lost degree of privacy are provided, at no cost to the data subject, unless compelling reasons for not doing so exist and can be demonstrated.

4.4.2.8 Contravention of Fair Information Practices

No cases were identified by federal ministry respondents where the operational requirements in geographic information management or geographic information analysis involved contravening fair information practices. As a result, no discernable differences were identified, between the public and private sectors, in the trends in contravention of fair information management practices that arise from operational requirements in geographic information management or geographic information management analysis.

When requested to identify areas where operational requirements in geographic information management involved contravening fair information practices, several areas were identified by provincial and territorial ministry respondents. The nature of the examples highlighted the transformative nature of electronic records when applied in applications of geographic information analysis with the use of enabling GIS technologies. The translation of records from hardcopy to electronic medium essentially creates new types of records and enables analysis never before possible. Several respondents noted that as a result of this transfer in medium from hardcopy to electronic, information that traditionally has not been thought of as personal in nature, or that has been publicly available without adverse affect, can take on new and privacy-sensitive characteristics when digitized and combined with other data using GIS technology.

Although the transformative nature of information in an electronic medium was identified by program managers in the areas of both geographic information analysis and access to information and privacy protection, it is instructive that this distinction is not specifically addressed in the provisions of access to information or protection of privacy legislation in any federal, provincial or territorial jurisdiction.

Direction on addressing the transformative nature of electronic information is typically located in policy directives issued by oversight agencies such as the Offices of the Information and Privacy Commissioners or in codes of best practices related to such exercises, such as conducting Privacy Impact Assessments.

The reactionary model that applies in most systems of legislative review in Canada, perpetuates the system whereby proposed revisions to statutes arise from existing rather than potential exposures or violations to fair information practices. The inability to proactively address exposures to fair information practices that arise from such applications as geographic information analysis may in part be attributed to the rapid pace with which applications in geographic information analysis are developed and deployed.

The disjoint nature of the relationship between the provisions of access to information and protection of privacy legislation, and, the operational parameters for geographic information management and geographic information analysis, belies the inability of program managers to identify where the operational requirements in geographic

information management and geographic information analysis contravene fair information practices.

It is not surprising therefore that no discernable differences were identified, between the public and private sectors, in the trends in contravention of fair information management practices that arise from operational requirements in geographic information management or Geographic Information Analysis (GIA).

Three guiding principles drawn from the discussion on the contravention of fair information practices from across Canada are that:

- Government organizations should review their GIS and GIA related privacy policies and practices on an on-going basis to ensure that they are appropriate, effective and responsive to current privacy expectations, legislation, and technology.
- Government organizations should not withdraw access to essential services or products if the data subject refuses to permit the use of their personal information in a GIS for a purpose not identified at the time of collection, including the exchange or sale of personal information to a third party for marketing purposes.
- Government organizations should stipulate, in their contractual agreements, with private sector partners: (1) the privacy protection measures to be adopted when using their GIS data, (2) the purposes for which that information may be used and disclosed by their business partners, and (3) the penalties for misuse.

5.0 DISCUSSION AND CONCLUSIONS

The survey of Canadian federal, provincial and territorial jurisdictions provided a snapshot perspective of the status of geographic information management and geographic information analysis in relation to the application of fair information practices, for the period 1 January, 1999 to 30 June, 1999.

The range in the level of familiarity with fair information practices, geographic information management and geographic information analysis amongst experts and program managers in access, privacy, GIM and GIA in the public sector was considerable. The diversity of the perspectives of the survey respondents was as informative as the content of the survey responses.

Following from the survey of each of the six primary stakeholder groups in each of the federal, provincial and territorial jurisdictions, areas of variation between policies, practices and applications of GIM, GIS and GIA across Canada were identified. The results of the survey were primarily qualitative in nature. Survey responses ranged from broad concepts in information management to specific practices in GIM within discrete applications in GIA.

Perceptions held by managers of programs involved in geographic information management, geographic information analysis, access to information and privacy protection demonstrated relatively little understanding of the linkages between these four disciplines. Generally, linkages between the four disciplines were only made at the level

of specific applications in geographic information management or geographic information analysis, where issues in personal information management arose.

As a result, a fair portion of the analysis and discussion of the survey results focused upon the implication of this apparent disconnection between the disciplines of geographic information management and geographic information analysis with the disciplines of access to information and privacy protection.

Following from the analysis and discussion, a series of recommendations on access to information and privacy protection are provided and are intended to address select issues in geographic information management and geographic information analysis.

5.1 Jurisdictional Setting

Despite the fact that all but one of the jurisdictions in Canada has legislation that addresses access to information and privacy protection, most jurisdictions have not dealt directly with the potential violations of fair information practices that arise with the application of the techniques in GIS and more generally in geographic information analysis.

As noted above, one of the challenges in addressing this issue is being able to overcome the apparent disconnection between the worlds of the GIA practitioner and the program managers responsible for access to information and privacy protection. Without a forum in which to raise issues of access to information and privacy protection, there are limited

opportunities to educating GIA practitioners about fair information practices and fewer opportunities to address and resolve violations of fair information practices by GIA practitioners.

5.1.1 Access to Information and Protection of Privacy Legislation

With the exception of the Prince Edward Island, comparable access to information and protection of privacy legislation exists in federal, provincial and territorial jurisdictions across Canada.

During the period that the survey was undertaken, several jurisdictions introduced Health Information Acts which essentially calved off health information as a separate information set. Although most provisions of the respective pieces of health information legislation comply with fair information practices, health information continues to be an information set that remains of keen interest to researchers in socio, economic and demographic research. These information sets are particularly conducive to techniques in geographic information analysis with the application of geographic information systems.

The intensive use of sets of health information, in combination with spatial and temporal information, allows the generation of personal profiles with applications in GIA. The market value of personal profiles of health information to industries such as the insurance industry makes health information a particularly valuable commodity.

Most pieces of access to information and protection of privacy legislation are designed to protect the confidences that GIS technology and applications in GIA are designed to tease out. GIS technology continues to evolve rapidly in response to the increasing speed, efficiency and diminishing cost of computer hardware. Increasingly intensive applications in GIA continue to evolve in response to the evolution of the GIS technology.

Because of the rapid rate at which GIS technology and GIA applications continue to develop, the reactive model that is applied in most jurisdictions with regard to legislative amendments is particularly ineffective in proactively addressing exposures in access to information and protection of privacy that arise from new generations of GIS technology and GIA applications.

5.1.2 Offices of the Information and Privacy Commissioner

In most jurisdictions the Commissioners responsible for access to information and privacy protection have responsibility for overseeing the manner in which information is collected, used, disclosed, disposed and secured in their respective jurisdictions. Following from a review of the questionnaire responses, these offices tended to fall into four categories of respondents.

The first group of questionnaire respondents from the Offices of the Information and Privacy Commissioners perceived a conflict of interest with their oversight role, in

commenting on practices in geographic information management and geographic information analysis and the potential violation of fair information practices that arise with the application of GIS and GIA.

The second group of respondents from the Offices of the Information and Privacy Commissioners perceived little connection between geographic information management, geographic information analysis and fair information practices. In these responses, geographic information was simply characterized as physical geographic information with no recognition of the human, social, demographic or economic bases for geographic information. The respondents demonstrated very little understanding of the potential to integrate multiple information sets using techniques in geographic information analysis with the application of Geographic Information Systems (GIS) technology.

The third group of respondents from the Offices of the Information and Privacy Commissioners acknowledged that significant issues in access to information and protection of privacy have the potential to arise from the manner in which geographic information is managed and analyzed. This group also acknowledged a limited knowledge of practices in geographic information management and techniques in geographic information analysis. The reactive strategy adopted by this group of offices is to defer to the respective ministries where the information is being managed and analyzed, and to undertake investigations and to gain further experience in geographic information management and techniques in geographic information analysis as complaints arise.

The fourth group of respondents from the Offices of the Information and Privacy Commissioners proactively acknowledged that significant issues in access to information and protection of privacy have the potential to arise from the manner in which geographic information is managed and analyzed. The Office of the Information and Privacy Commissioner for Ontario exemplifies this group of offices. This office recognized that profound technological advances are continually transforming the basic nature of information management. As governments implement new information technology, conventional paper records are fast giving way to powerful electronic databases. One type of information management system that is increasingly being introduced by government organizations is Geographic Information System (GIS) technology. In proactively addressing these issues the office acknowledges that GIS technology has been developing steadily since the 1960s and that government organizations in Canada have played a pivotal role in that development. Although applications were initially confined to organizing and analyzing information about natural resources, as the technology has matured and become more user-friendly, costs have decreased and GIS applications have expanded into multiple disciplines.

As government organizations move with increasing speed toward the creation of a predominantly electronic environment, it is not always clear how to facilitate these purposes and rights. New questions and concerns inevitably arise about the protection of privacy, the nature of public access to information under the control of government organizations, and the applicability of access to information and protection of privacy

legislation. The access and privacy issues associated with today's electronic environment, of which GIS technology is a part, are complex and challenging.

As the watchdogs for access to information and privacy protection, the diversity of roles assumed by the Offices of the Information and Privacy Commissioners across Canada and the clear disparity in understanding the exposures were acknowledged as posing significant challenges in addressing the issues that arise from geographic information management and geographic information analysis in relation to fair information practices compliance across Canadian jurisdictions.

5.2 Modes of Geographic Information Management

Modes of geographic information management set the standards within the jurisdiction for information collection, use, disclosure, disposition and security.

5.2.1 Access to Information and Protection of Privacy Offices

Many of the same perceptions expressed by the Commissioners' offices about the limited exposures arising from geographic information management and geographic information analysis in relation to fair information practices compliance were expressed by several federal and provincial ministry respondents from the information and privacy offices. This apparent lack of familiarity with basic concepts in fields of the human, social, demographic and economic aspects of geography would appear to significantly limit the

role of these offices in monitoring information management practices as they relate to geographic information management and compliance with access to information and privacy protection legislation.

To compound this challenge, the focus of most programs responsible for access to information and protection of privacy legislation appears to be on mechanisms for providing access to records. Expertise in the delivery of programs in access to information and privacy protection appears to reflect the focus on records management rather than information management. The distinction between records management, data administration and information management appears to be blurred in most jurisdictions.

Where strategies in information management do exist, the focus of programs in most federal, provincial and territorial jurisdictions appears to be primarily on the protection of personal information. Although provisions of most statutes dealing with access to information and privacy protection do address the protection of proprietary information, trade secrets and information of economic or strategic value, these information types are dealt with as discrete information sets.

Most pieces of legislation dealing with access to information and privacy protection do not address the information management issues associated with the relational nature of many automated information systems. As a result, the functionality of relational databases that allow the creation of integrated information products using spatial geographic data as a base with overlays of personal and non-personal data are not

addressed in most pieces legislation dealing with access to information and privacy protection.

5.2.2 Geographic Information Management Frameworks

In the six jurisdictions where Geographic Information Management Frameworks (GIMF) are in place, GIMF administrators expressed considerable frustration in establishing a jurisdiction-wide adoption of the management principles that are essential to applying and maintaining the GIMF.

In several cases, the critical factor in establishing a jurisdiction-wide adoption of the GIMF appears to revolve around securing an impartial, knowledgeable administrator for the GIMF. In most jurisdictions, information continues to be viewed as a basis for power rather than as a common, shared resource within the respective ministries.

The reluctance to commit to a jurisdiction-wide GIMF thus appears to be based upon a lack of familiarity with concepts in information engineering methodologies, perceived loss of power in releasing direct control over information sets, and limited recognition of the exposures resulting from deficient geographic information management practices.

The lack of legislative, regulatory or voluntary authority for establishing and/or maintaining GIMF's speaks to the general lack of appreciation for the benefits and

controls that would be derived from positively controlling the collection, use, disclosure, aggregation and disposition of personal and nonpersonal geographic information.

The rigour required to follow a set methodology in information management would involve organizations being required to articulate the reasons for information collection along with the intended primary and secondary uses of the information. Most information management frameworks also include consideration of information accuracy, completeness, security and brokerage, along with metadata standards that are designed to assist in making sound decisions in resource and information management.

5.2.3 Information Brokerages

Significant portions of ministry budgets are spent annually on developing and maintaining existing information sets. Increasing fiscal constraint in the public sectors has resulted in the development of an increasing number of innovative revenue streams. As a part of this trend, several jurisdictions have established information brokerages. Although limited property rights in information have been established through the courts in Canada, most of the information brokerages sell the service of providing access to information held in public information repositories.

Traditional geographic information sets such as base maps have typically formed the base thematic layers for these information products. Composite integrated information

products using thematic or attribute data from a variety of other public and private sector information sets have been developed for sale through these information brokerages.

In most cases, the offices charged with responsibility for compliance with access to information and privacy protection have neither recognized the potential exposures resulting from this form of information brokerage, nor, conducted any form of Privacy Impact Assessment (PIA) as part of the planning or monitoring of the operation of these information brokerages.

5.2.4 Legislative, Regulatory or Voluntary Authority for Geographic Information Management Frameworks

Selected provisions of access to information and protection of privacy legislation from the federal, provincial and territorial jurisdictions address limited aspects of geographic information management.

Without the recognition of the potential exposures arising from geographic information management in relation to access to information and privacy protection amongst most Offices of the Information and Privacy Commissioners and most ministries responsible for access to information and privacy protection programs, it is not surprising that neither legislative, regulatory nor voluntary authorities exist for geographic information management frameworks.

At the time the questionnaire was administered, the Province of the Quebec was the only jurisdiction to have addressed legislation on access to information and privacy protection in relation to selected aspects of geographic information management within the private sector.

Despite the fact that compliance with fair information practices in geographic information management has not been addressed by most Offices of the Information and Privacy Commissioners or most ministries responsible for access to information and privacy protection programs, standards have been established with respect to other aspects of geographic information management. Most jurisdictions have extensive committee structures that address technical standards with respect to technology platforms, metadata, data interchange, systems migration and business continuity. The apparent challenge is to extend the mandate of the public sector technical standards committees to include consideration of compliance with fair information practices in setting standards for geographic information management.

Cost benefit analyses appear to have been undertaken by federal, provincial and territorial ministries on the financial, technical and business risks involved in geographic information management. The societal costs of current practices in geographic information management have yet to be addressed by most Offices of the Information and Privacy Commissioners and most ministries responsible for access to information and privacy protection programs.

In several instances, the private sector is providing a proactive lead in addressing the elementary issues in geographic information management with the development of the Canadian Standards Association (CSA), Canadian Bankers Association (CBA) and Canadian Direct Marketing Association (CDMA) and STENTOR codes of practice for privacy protection.

Many of the voluntary codes of practice mentioned above have evolved in the private sector in recognition of the growing concern expressed by private citizens for the potential for invasion of privacy that arises with the application of relational information systems and the increasing ability to create personal and nonpersonal profiles with the merging of previously disparate data sets.

Compliance with the European Union Directive on Adequacy of Protection for Personal Information and the Government of Canada Personal Information Protection and Electronic Documents Act are likely to provide further incentives for the development of sectoral codes of practice.

The extension of the Personal Information Protection and Electronic Document Act to the private sector by 2004 will, in certain sectors, likely require the private sector to comply with fair information practices in advance of certain programs in the provincial public sector being required to comply with a comparable standard in privacy protection. The requirement for the private sector to comply with fair information practices ahead of

compliance by a limited number of provincial public sector programs will undoubtedly be the source of much debate and lobbying. A positive side effect of this circumstance would be the incentive for public sector programs to comply with fair information practices in order to evade further scrutiny by private sector organizations that are bound to uphold the provisions of the Personal Information Protection and Electronic Documents Act.

5.3 Modes of Geographic Information Analysis

Modes of GIA pose the greatest exposure to noncompliance with fair information practices. GIS technology and applications in GIA allow the data drawn from diverse data sources to be aggregated and reconstituted in forms that create detailed profiles and reveal trends that provisions of access to information and protection of privacy legislation are typically designed to protection.

With few legislative, regulatory or voluntary codes of practices in place to govern geographic information management, GIA can be undertaken in the public and private sectors with relatively little oversight or restrictive control.

5.3.1 Strategic Information Systems Planning

Few ministries in the federal, provincial or territorial governments appear to undertake regular strategic information systems planning with respect to geographic information

systems planning and development. Business plans were in place for establishing initiatives such as British Columbia's Geographic Data BC, Alberta's Land Information Alberta (LIA), the Manitoba Land-Related Information Systems (MLRIS) and Ontario-based POLARIS system.

Of these initiatives, British Columbia's Geographic Data BC appears to be the most vigilant in reviewing the business area analysis, business systems design and technical system design. As part of these system reviews and business development exercises, privacy implications and compliance with fair information practices appear to be becoming an integral part of the business and technical feasibility assessments. Unfortunately, this Geographic Data BC represents an exceptional case rather than the standard mode of operation, at this time.

5.3.2 Function Creep

Increasingly, GIA and the trend to the more intensive use of geographic information is driven by the additional functionality of increasingly sophisticated information systems to process higher volumes of data from diverse data sources with greater speed and efficiency at lower costs. In part, many of the efficiencies gained in these areas may also be attributed to cross jurisdictional standardization of data and information standards that address issues of metadata, data transfer, referential integrity, data accuracy and data security in information systems.

New versions of relational database systems are available to consumers approximately ever twenty-two months. Added functionality that becomes available with each new version of GIS software becomes the base suite of tools for conducting GIA.

Legislative reviews generally are conducted at five years intervals in the most proactive of ministries. Policies regulating GIA are poorly documented and reviews appear to be conducted on an *ad hoc* basis. Policy and procedures that are designed to regulate applications in GIA are virtually nonexistant. GIS applications manuals provide the documentation of the functionality the GIS software and available applications in GIA. Little direction appears to be provided to GIS and GIA practitioners on considerations for compliance with fair information practices or parameters for regulating appropriate applications in GIA. Ministry-generated procedures relating to geographic information analysis appear limited to conventions that are adopted within ministries for their respective GIA applications.

Given the lack of legislative, regulatory, policy or procedural direction within ministries undertaking GIA, it is not surprising that the functionality of the GIS software with the most extensive set of GIA applications becomes the *de facto* base suite of tools for conducting GIA.

5.4 Application of Fair Information Practices

Given the relatively unstructured and unregulated geographic information management environment in which GIS technology is applied in conducting GIA, the means of assessing and enforcing compliance with fair information practices are relatively limited.

As noted in the preceding sections on modes of geographic information management and modes of geographic information analysis, many of the survey respondents demonstrated a general lack of understanding of the potential linkages between nonpersonal land-based geographic information and person-based geographic information. The linkages are afforded by the manner in which GIS technology allows land-based spatial information to be the overlain with thematic layers of information that often contain personal information. The integrated information products that result from this functionality of GIS technology, and the capacity to conduct further queries on these integrated information products with the application of techniques in GIA, challenge the bounds of current fair information practices in adequately protecting personal privacy.

Effective internal and external communication by public bodies and orientations for program managers to broader concepts in jurisdiction-wide models in geographic information management and analysis could significantly improve consistency in strategies in geographic information management and analysis at the federal, provincial and territorial levels of government.

5.4.1 Privacy Impact Assessments

Privacy Impact Assessments (PIA) provide a structured systematic approach to evaluating manual and automated information systems for the purposes of assessing compliance with fair information practices, usually as expressed in access to information and protection of privacy legislation.

PIA are particularly useful in assessing compliance with fair information practices within GIS or systems of GIA where information is drawn from diverse information sources. In GIA, information sets are often merged or manipulated outside of the structures within which the information was originally collected and often in circumstances that are out-of-context with the applications for which the information was intended to be used.

The PIA structure draws the attention of the information manager or GIA practitioner back to the ten basic fair information practices (see Appendix 1). Undertaking the PIA involves assessing whether the authority exists for the collection of the information; setting parameters for the information use, disclosure and security; and, setting parameters for the application of GIA.

Unfortunately, in practice PIA are rarely conducted by federal, provincial or territorial governments. The resistance to conducting PIA is reflective of the shift in culture that is required in the public and private sectors to readily adopt the spirit of the access to information and protection of privacy legislation. Information systems continue to be

developed in the public sector in relative secrecy. The watchdog role assigned to most Offices of the Information and Privacy Commissioner, in combination with the public sector's perceived need for secrecy in information systems development, precludes a frank discussion of intended developments in information systems by most ministries during the initial planning stages on integrated information systems design. This element of secrecy poses a fundamental challenge to undertaking a PIA as part of the initial business area analysis in the initial stages of the information systems planning and design. At this time, access to information and protection of privacy legislation in most jurisdictions does not require that PIAs be conducted on information systems.

GIS and GIA applications often involve information drawn from diverse sources and therefore represent the more complex cases in which to conduct a PIA. The diverse nature of GIA applications represent the cases in which fair information practices are more likely to be violated and therefore elevates the importance of the undertaking thorough PIA at the earliest stage in the information systems development.

Most often the experience of the ministries involves conducting a PIA after the information systems have been developed at considerable cost to the respective ministry. The PIA is often conducted at the request of the Office of the Information and Privacy Commissioner, in response to a complaint or investigation into noncompliance with fair information practices. At this point in the process, system retrofitting to comply with fair information practices is usually a far more costly proposition than incorporating fair information practices into the original design of the system. The systems refitting to

comply with fair information practices usually involves disabling elements of the more GIA-intensive functions of information systems, thereby reducing the functionality of the information system.

The reduced functionality, system regulation and costly retrofitting of ministry information systems has further limited the adoption of conducting PIA and enhanced the perceived need of many ministries to undertake information systems development in relative secrecy.

In several newer pieces of legislation across the country, PIA are now required as part of information systems development. Once the Alberta Health Information Act is proclaimed, ministries will be required to conduct PIAs on health information systems and provide copies to the Office of the Information and Privacy Commissioner. This legislative requirement may represent an incremental step in facilitating the shift in culture that is required in the public and private sectors to readily adopt the spirit of the fair information practices that are embodied in most access to information and protection of privacy legislation. Being required to undertake a PIA may also serve as an incentive to undertake the PIA earlier in the information systems design and development, thereby avoiding the additional costs associated with systems retrofitting. The requirement to conduct the PIA may also facilitate more extensive data modeling as part of the information systems design to ensure that compliance with fair information practices will not extensively restrict elements of the information systems functionality.

As the extensive functionality of GIS and GIA applications are often used as the basis for acquiring or enhancing these information systems, an assessment of modes of operation that comply with fair information practices, with the application of the PIA, would allow informed decisions about the GIS operation and permissible GIA applications.

Although few respondents to the questionnaire acknowledged that the Government of Canada Personal Information Protection and Electronic Documents Act (PIPED) and European Union Directive on Personal Data Protection would have any significant impact on their respective codes of practice, the impact of these pieces of legislation in the private sector will undoubtedly set new base levels for privacy protection that will have to be mirrored in the public sector.

5.5 Impact on Geographic Information Management and Analysis

Few of the questionnaire respondents for the federal, provincial or territorial jurisdictions acknowledged significant impacts on geographic information management or geographic information analysis, arising from the application of fair information practices. This may in part be attributed to the relatively low levels of compliance enforced by Offices of the Information and Privacy Commissioners and ministry offices charged with responsibility for access to information and privacy protection.

Reviews of the orders issued by Information and Privacy Commissioners across Canada are testimony to the continued effort that is required to bring the public and private sectors into compliance with fair information practices.

5.5.1 Leveling the Playing Field

As publicly-held information sets become more widely known through applications in GIA, these information sets are likely to be more frequently merged with other information sets and result in more contraversial, market-based and privacy-sensitive integrated information products. Expert use of these integrated information products usually results in the identification of trends or in an administrative use of the information that ultimately impacts the data subject. Demands from the public for more stringent application of fair information practices to protect personal privacy are often the result.

As privacy protection legislation is extended increasingly to the private sector through legislation such as Government of Canada Personal Information Protection and Electronic Documents Act, the private sector is likely to focus increasingly on the costs of privacy protection and compliance with fair information practices.

Many of the privacy-intrusive activities formerly undertaken in the public sector have migrated into the private sector during the past decade, to avoid public sector requirements for compliance with fair information practices. With the staged extension of

privacy protection legislation to the private sector, many of these privacy-intrusive lines of business will be subject to significant restructuring or be discontinued.

The private sector is therefore taking an increasingly critical view of the financial and opportunity costs associated with privacy protection and compliance with fair information practices. With the leveling of the playing field between the public and private sectors, it is reasonable to expect that the highly competitive private sector will move to hold the public sector as accountable for privacy protection and compliance with fair information practices as standards set for the private sector.

Although the Government of Canada Personal Information Protection and Electronic Document Act had not been enacted at the time of the survey, it had been anticipated by the private sector for some time. As this private sector, privacy protection legislation is implemented in stages between 2001 and 2004, the increasing regulation of the private sector with respect to privacy protection is likely to drive the private sector to negotiate more clearly articulated privacy protection models for accountability as revenues and profit margins are impacted by legislation mechanisms in privacy protection.

5.6 Innovations in Geographic Information Management

Neither the federal, provincial nor territorial jurisdiction respondents indicated that innovations in techniques in geographic information management could be attributed to the application of fair information practices. In the federal jurisdiction, pertinent factors

in driving innovations in geographic information management were identified in terms of 'public good' and 'client focus' rather than the notion of compliance with fair information practices. Further considerations were identified as the longer term perspective in serving multi-tiered levels of clients in both the public and private sectors.

The mutualistic relationship between the public and private sectors that arises within the client-focused environment allows both sectors to take advantage of the developments in the other sector. An example of this mutualistic relationship would be the ongoing activities in the federal jurisdiction to ensure the development and availability of a globally consistent national spatial reference system, while the private sector develops products and services with a spatially-referenced component. The focus therefore is on establishing an enabling environment for further development of GIS applications and techniques in GIA. This trend generally points to a more intensive and integrated use of geographic information, with a greater potential for violation of fair information practices. The responses to the questionnaire did not provide any specific indicators that particular attention was being paid to compliance with fair information practices, in relation to the management of geographic information management.

Without recognizing the potential risks of violating fair information practices that are associated with the relatively uncontrolled use of geographic information, few innovations in geographic information management are likely attributable to initiatives designed to comply with fair information practices.

At the provincial and territorial levels of government, efforts to comply with fair information practices were not viewed as having resulted in innovations in techniques in geographic information management. Forces driving innovations in geographic information management included client-focused initiatives and reduced budgets, rather than requirements to comply with fair information practices. Innovations in technology and the increased functionality of software applications were acknowledged as driving forces for innovation in geographic information management. Revenue streams that are likely to result from innovations in technology, user-pay business solutions and the proliferation of electronic commerce were also viewed as catalysts in innovations geographic information management.

No overarching and discernable differences were identified, between the public and private sectors, in the trends in innovations in geographic information management. Other than the synergy that arises from the mutualistic relationship between the public and private sector as described above, newer technology generally allows cheaper more efficient business and often forms the underpinning of major system re-engineering.

With continued education of program managers who are responsible for geographic information management, future methodologies for geographic information management will hopefully include modules on compliance with fair information practices as an increasingly standard component of the information engineering methodology.

5.7 Innovations in Geographic Information Analysis

Following from the responses that few innovations in geographic information management are attributable to requirements to comply with fair information practices, no innovations in techniques in geographic information analysis were attributed to the application of fair information practices by federal government respondents.

In a similar trend, provincial and territorial respondents noted that the application of fair information practices has not resulted in innovations in techniques in geographic information analysis. The observation was made by one respondent that the driving force in geographic information analysis may be expressed in terms of underlying GIS technology being driven by need, rather than by something 'neat to do'.

This observation provides a telling example of the priority with which compliance with fair information practices is viewed by GIS technology and GIA practitioners. The notion of function creep is entrenched in the culture of both the GIS technology and GIA practitioners. With the release of each new generation of GIS technology, the diversity of functionality of applications in GIA increases and the ingenuity of GIS technology and GIA practitioners is challenged to explore the full extent of most recent generation of products. Compliance with fair information practices is left to linger as a secondary consideration, once the functionality of the new generation of GIS technology and GIA applications have been fully exhausted.

Little impetus for innovation in GIA appears to arise from the availability of geographic data, as data has traditionally been viewed as always having been available. Therefore, there appears to have been little incentive in the past for further innovations in geographic information analysis in order to facilitate more intensive uses in geographic information as a result of the limited availability of data.

With the increasing trend to sell geographic information and integrated information products and services, the notion of information as a 'free good' is becoming less popular. Market-based pricing for geographic information is establishing geographic information as business commodity that is increasingly restricted to those have the resources to pay for the most current, complete and extensive sets of geographic information to fuel their GIA. As a result of the decreasing availability of geographic information that is likely to arise with the increasing prices of geographic information, GIA practitioners will likely be challenged to do more with less. Geographic information will likely be mined more intensively at the cost of compliance with fair information practices.

Responses from federal, provincial and territorial agencies on issues of innovations in geographic information analysis were particularly traditional in nature and typically reflected a single purpose/single means approach to geographic information analysis. Limited recognition was expressed of the potential for further innovation in geographic information analysis as the trend to privitization in the public sector increases and public/private enterprise solutions continue to evolve. Despite the identification of the

cost of data as a critical factor in limiting innovations in geographic information analysis, few respondents explored the opportunities to be derived with public/private sector cost sharing, information brokerages or other privacy-sensitive, revenue-generating applications that would address the concerns over the cost of data and facilitate further innovations in more intensive forms of geographic information analysis.

The perceived disjoint relationship between applications in geographic information analysis and fair information practices appears to stem recognition of the potential threats to personal privacy that are posed with geographic information analysis. Without a clear understanding of the potential risks to personal privacy that are posed with the deployment of increasingly intensive forms of geographic information analysis, most program managers perceive little need to explore innovative solutions in optimizing the application of techniques in geographic information analysis with compliance in fair information practices. Serious consideration of compliance with fair information practices in geographic information analysis will apparently only occur once compliance with fair information is established as a design criterion for the development of the GIS technology and the associated applications in GIA.

5.8 Contravention of Fair Information Practices

Following from the trends observed in innovations in geographic information management and geographic information analysis, it is not surprising that no cases were identified by federal ministry respondents where the operational requirements in

geographic information management or geographic information analysis involved contravening fair information practices. Furthermore, no discernable differences were identified, between the public and private sectors, in the trends in contravention of fair information management practices arising from operational requirements in geographic information management or geographic information management analysis.

At the level of the provinces and territories, several areas were identified where the operational requirements in geographic information management involved contravening fair information. The nature of the examples highlighted the transformative nature of electronic records when applied in applications of geographic information analysis with the use of enabling GIS technologies. The respondents noted that the translation of records from hardcopy to electronic medium effectively creates new types of records that enable more intensive levels of analysis.

Several respondents noted that as a result of this transfer in medium from hardcopy to electronic, information that traditionally has not been thought of as personal in nature, or that has been publicly available without adverse affect, have the potential to take on new and privacy-sensitive characteristics when digitized and combined with other data using GIS technology and applications in GIA.

It is the understanding of the subtleties of the subject of the information in the context the medium in which the information is presented, that allows program managers in GIM and GIA to appreciate the potential for violation of fair information practices that arises with

the automation of access to geographic information along with the increasing functionality of GIA techniques in exploratory spatial and temporal data analysis.

Although the transformative nature of information in an electronic medium was identified by program managers in the areas of both geographic information analysis and access to information and privacy protection, it is instructive that this distinction is not specifically addressed in the provisions of access to information or protection of privacy legislation in any federal, provincial or territorial jurisdiction. The relative lack of acknowledgement of this issue in most access to information and privacy protection legislation across Canada may in part be attributed to the records rather the information management philosophy adopted in most pieces of legislation in this area. Most of the records management strategies focus upon the management of record with relatively little consideration given the informational content of the record. Information classification systems that are based on the sensitivity of the informational content of the record may provide considerable assistance in ensuring appropriate consideration for compliance with fair information practices in administering a 'records management' approach to access to information and privacy protection.

Direction on addressing the transformative nature of electronic information is typically located in policy directives issued by oversight agencies such as the Offices of the Information and Privacy Commissioners or in codes of best practices related to such exercises, such as conducting Privacy Impact Assessments.

The reactionary model that applies in most systems of legislative review in Canada, perpetuates the system whereby proposed revisions to statutes arise from existing rather than potential exposures or violations to fair information practices. The inability to proactively address exposures to fair information practices that arise from such applications as geographic information analysis may in part be attributed to the rapid pace with which applications in geographic information analysis are developed and deployed.

The disjoint nature of the relationship between the provisions of access to information and protection of privacy legislation, and, the operational parameters for geographic information management and geographic information analysis, belies the inability of program managers to identify where the operational requirements in geographic information management and geographic information analysis contravene fair information practices.

It is not surprising therefore that no discernable differences were identified, between the public and private sectors, in the trends in contravention of fair information management practices that arise from operational requirements in geographic information management or GIA.

5.9 Recommendations to enhance compliance with Fair Information Practices in Geographic Information Management and Geographic Information Analysis

One of the primary challenges encountered in this research has been the diversity of policy, legislation, standards, codes of best practice, guidelines and manuals, and, training, services and support in geographic information management, geographic information analysis and fair information practices that exists across Canadian federal, provincial and territorial jurisdictions.

Collectively, these factors express the critical elements that bound the discussion of rationalizing geographic information management with fair information practices. However, each jurisdiction in Canada has undertaken a slightly different path and as a consequence is at a slightly different stage in regulating geographic information management and techniques in geographic information analysis with respect to compliance with fair information practices.

Drawing upon the common experiences of Canadian federal, provincial and territorial jurisdictions would appear to provide a stable basis upon which to build a strategy for rationalizing geographic information management with fair information practices.

The impending extension of privacy protection legislation to the Canadian private sector will provide another basis upon which to draw upon the common experiences of the

private sector in each of the Canadian federal, provincial and territorial jurisdictions. As the Personal Information Protection and Electronic Documents Act comes into force across Canada between 2001 and 2004, a window of opportunity exists to establish greater levels of co-operation between Canadian federal, provincial and territorial jurisdictions in apply fair information practices in regulating geographic information management and the application geographic information analysis. Adding further impetus to the need for consistency in personal information protection is the ongoing initiative of the European Union to ensure that the transborder flow of personal information only occurs between jurisdictions where adequacy of protection of personal information is assured.

Synchronizing the application of fair information practices in geographic information management and geographic information analysis between the public and private sectors will require concerted co-operation between Commissioners and offices responsible for fair information practices across Canadian federal, provincial and territorial jurisdictions.

5.9.1 Geographic Information Management Frameworks

As the applications in GIA continue to expand in intensity of information use and diversity of disciplines with increasing GIS functionality, the importance of sound, flexible and applicable structures in geographic information management will increase.

Geographic Information Management Frameworks (GIMF) will be essential to maintaining compliance between multi-layered sets of factors that regulate the environment in which GIA is conducted with the use of enabling technologies such as GIS.

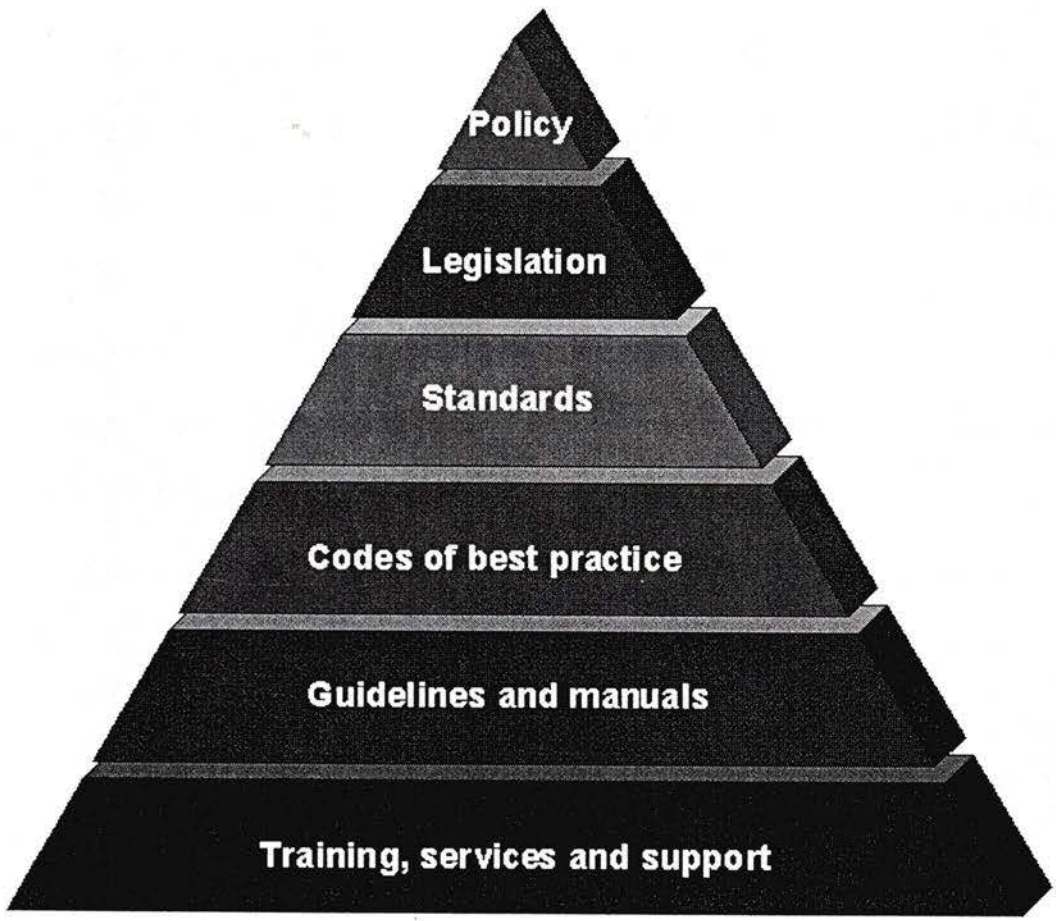

Figure 1: Geographic Information Management Framework (GIMF) Hierarchy

The GIMF pyramid, shown in Figure 1, illustrates the hierarchical structure and relative order of referential integrity that would be required between policy, legislation, standards, codes of best practice, guidelines and manuals, and, training services and support.

Establishing a consistent conceptual GIMF will be essential to managing the environment in which GIA is conducted in the public and private sectors. As noted in earlier discussion, the leveling of the playing field between the public and private sectors with extension of privacy protection to the Canadian private sector is bound to restrict or curtail current privacy-intrusive practices in the private sector. The financial, societal and opportunity costs associated with privacy protection will continue to be the focus of private sector scrutiny as policy, legislation, standards and codes of best practice that address fair information practices are extended in stages to Canadian private sector. As lucrative applications in GIA become further restricted with the broader application of fair information practices, it will be increasingly important to demonstrate a consistent and equitable application of fair information practices across the public and private sectors.

The GIMF hierarchy acknowledges the organizational, administrative and structural differences between the six layers of policy, legislation, standards, codes of best practice, guidelines and manuals, and, training, services and support. The GIMF hierarchy also recognizes the unconventional manner in which GIS technology drives GIA applications, which in turn results in reactive changes to codes of best practice, standards, legislation

and policy. Although the traditional 'top down' hierarchical structure applies to the formal amendments to policy , legislation, standards, codes of best practices, guidelines and manuals, and, training, services and support, the impetus for such amendments may arise at any level in the GIMF hierarchy.

Of critical importance in the GIMF hierarchy is the referential integrity that must exist between the six layers of the conceptual framework, to ensure that appropriate consideration is given to each of the six layers with every amendment to GIS technology, GIA applications and fair information practices.

Given the highly competitive nature of the information management industry and the soaring market for integrated information products, the trend in government to deregulate and privatize is likely to drive jurisdiction-wide applications in GIA further into the private sector.

Instituting the GIMF hierarchy will allow the public sector to set in place structures that establish levels of accountability for compliance with fair information practices while providing sufficient flexibility for the continued development of techniques in intensive information analysis. The GIMF hierarchy has the potential to allow optimal market growth of GIA with the application of enabling GIS technologies, in compliance with fair information practices.

5.9.2 Access to Information Considerations

In order to apply the GIMF in a consistent and equitable fashion, federal, provincial and territorial jurisdictions must be able to adhere to a common set of access to information management principles in relation the application of GIS technology, GIA and fair information practices.

When adopting GIS technology it is important for government organizations to see beyond the commercial value of the data, and to understand that public access to government information is a foundation of accountable government. It is recognized that this technology presents new challenges to government organizations.

However, given the potential and growth of GIS technology, federal, provincial and territorial jurisdictions need to consider the impact that GIS technology and GIA could have on access, and to make every attempt to enhance the public's access right. These jurisdictions should consider themselves trustees of the information in their custody and ensure that issues such as commercial value, copyright and property rights in selected information sets, do not erode public access.

5.9.2.1 Access to Information - GIS Management Principles

The following access to information principles were articulated by the Ontario Office of the Information and Privacy Commissioner. These recommendations formed the basis of

many of the recommendations that were identified in the jurisdictional summaries found in Chapter 4. As noted in the jurisdictional summaries, these recommendations could be applied equally to the federal, provincial and territorial jurisdictions across Canada.

The access to information GIS management principles are as follows:

- Government organizations should recognize public access to government-held information as a central underlying tenet of any program or service involving GIS technology. Before introducing any GIS application, the impact on access should be identified and assessed. Appropriate and effective measures (technological, legislative and policy) should be developed and implemented.
- Government organizations should use GIS technology to enhance access to government-held information. They should look to the introduction of GIS technology as a way of increasing the amount of information that is routinely distributed or actively disseminated.
- Government organizations should ensure that all GIS applications are designed in such a way that the public can exercise their access rights in a meaningful and timely manner.
- Government organizations should provide public education on their GIS applications to ensure that the public can exercise their access rights in a meaningful and timely manner.

- Government organizations should conduct in-house education about the access implications of GIS technology for all staff involved in the development of the application or the delivery of related programs and services.
- Government organizations should ensure that the complexity or cost of GIS technology, the commercial value of the data, fees, or copyright, do not become an unreasonable barrier to public access to government-held information.
- Government organizations should ensure that private sector involvement in GIS applications does not reduce public access to government-held information.
- Government organizations should ensure that their GIS databases are as accurate, complete and up-to-date as is reasonably possible.
- Government organizations should ensure that the use of GIS technology does not adversely affect the records management or retention of government information.
- Government organizations should review their GIS-related access policies and practices on an on-going basis to ensure that they are appropriate and effective.

5.9.3 Protection of Privacy Considerations

In order to apply the GIMF in a consistent and equitable fashion, federal, provincial and territorial jurisdictions must be able to adhere to a common set of protection of privacy management principles in relation the application of GIS technology, GIA and fair information practices.

5.9.3.1 Protection of Privacy - GIS Management Principles

The following set of protection of privacy principles were articulated by the Ontario Office of the Information and Privacy Commissioner. These recommendations formed the basis of many of the recommendations that were identified in the jurisdictional summaries found in Chapter 4. As noted in the jurisdictional summaries, these recommendations could be applied equally to the federal, provincial and territorial jurisdictions across Canada.

The protection of privacy GIS management principles are as follows:

- Government organizations should recognize protection of privacy as a central underlying tenet of any program or service involving GIS technology. Before introducing any GIS application, potential privacy issues should be explicitly identified and the impact of the proposed application on privacy assessed. Appropriate and effective privacy protective measures (technological, legislative and policy) should be developed and implemented.
- Government organizations should only use GIS technology to enhance government programs and services, and not as an instrument of social control or surveillance.
- Government organizations should collect, use, retain, and disclose data in an anonymized or aggregate format whenever possible in their GIS applications.
- Government organizations should recognize that information associated with a specific location may be privacy-sensitive.

- Government organizations should ensure that their GIS applications are open and transparent to the data subjects, and that the data subjects are aware of the existence of any technology or record-keeping system impacting their personal information.
- Government organizations should recognize the data subject as the owner of their personal information, and as a key stakeholder to be consulted when contemplating the introduction of GIS technology or the development of policies or practices that could potentially impact their privacy.
- Government organizations should provide public education identifying any privacy issues associated with the use of GIS technology, prior to implementation. They should also communicate their privacy protection policies and practices to the public in a manner that enables the public to exercise its rights.
- Government organizations should govern their GIS practices related to identifying information by established fair information practices, regardless of whether that information is considered "public."
- Government organizations should conduct in-house education about the privacy implications of GIS technology for all staff involved in the development of the application or the delivery of related programs and services.
- Government organizations should communicate their privacy protection policies and practices regarding GIS applications to all staff, and make staff accountable for adherence to those policies and practices.
- Government organizations should ensure that, if a proposed GIS application has the potential to modify information processing practices in a way that might

compromise existing levels of privacy, appropriate methods of restoring any lost degree of privacy are provided, at no cost to the data subject, unless compelling reasons for not doing so exist and can be demonstrated.

- Government organizations should review their GIS-related privacy policies and practices on an on-going basis to ensure that they are appropriate, effective and responsive to current privacy expectations, legislation, and technology.
- Government organizations should not withdraw access to essential services or products if the data subject refuses to permit the use of their personal information in a GIS for a purpose not identified at the time of collection, including the exchange or sale of personal information to a third party for marketing purposes.
- Government organizations should stipulate, in their contractual agreements, with private sector partners: (1) the privacy protection measures to be adopted when using their GIS data, (2) the purposes for which that information may be used and disclosed by their business partners, and (3) the penalties for misuse.

6.0 FINAL ANALYSIS

In the final analysis, these access to information and protection of privacy principles need to form the cultural basis upon which the six layers of the GIMF hierarchy are managed. For most of the Canadian federal, provincial and territorial jurisdictions, this represents a significant shift in culture.

One of the critical success factors in being able to effect this shift in culture is to meld the worlds of the privacy advocate with the worlds of the information broker, information systems analyst, facilities and services planner, and, GIS practitioner. The structure of the Privacy Impact Assessment provides a forum to bring together as many different disciplines as are likely to use or be affected by the information under consideration. Proactively addressing these issues of privacy impact, within an environment that is governed by a common set of access to information and protection of privacy GIS management principles, allows all parties to assess alternative futures and strike the optimal balance amongst these competing interests of access to information and privacy protection.

The bounds of the informational mosaic established through enabling technologies such as GIS and expanding applications of GIA are limitless and completely undefined by any one discipline. Our ability to rationalize geographic information management with fair information practices will be contingent on our ability to see beyond the limits of our singular disciplines and to strive to establish common multidisciplinary management

structures that provide a sense of stability and integrity in the rapidly evolving geographic information economy.

ENDNOTES:

1. Agre, Philip E. 1994. "Surveillance and Capture: Two Models of Privacy," The Information Society.

2. Agre, Phillip E. and Chrstine A. Harbs. 1994. Social Choice about Privacy: Intelligent Vehicle-highway Systems in the United States. Information Technology and People.

3. Agre, Philip E. and Marc Rotenberg, Eds., Technology and Privacy: The New Landscape. MIT: MIT Press, 1997.

4. Alberta Provincial Government (1993). *Freedom of Information and Protection of Privacy Act* (Alberta) 1993.

5. Aldrich, Robert. 1982. Privacy Protection Law in the United States. Washington D.C.: U.S. Department of Commerce, National Telecommunications and Information Administration.

6. American Express. 1991. *The American Express Consumer Privacy Principles*, January 1991; and Privacy Resource Kit, June 1991.

7. Antenucci, J.C., Brown K., Croswell P.L., Kevany M., Archer H. 1991. *Geographic Information Systems: A Guide to the Technology.* Van Nostrand Reinhold. New York.

8. Australia, Attorney-General's Department. 1996. Discussion Paper: Privacy Protection in the Private Sector. Canberra: Attorney-General's Department, September 1996.

9. Aronoff, S. 1989. *Geographic Information Systems: A Management Perspective.* WDL Publications. Ottawa.

10. Australian Land Information Council. 1990. *Data Custodianship/ Trusteeship.* Belconnen, ACT.

11. Australian Land Information Council. 1990. *A General Guide to Copyright, Royalties and Data Use Agreements.* Belconnen, ACT.

12. Australian Land Information Council. 1990. *Charging for Land Information.* Belconnen, ACT.

13. Australian Land Information Council. 1990. *Access to Government Land Information.* Belconnen, ACT.

14. Australia New Zealand Land Information Council. 1992. *Privacy,Confidentiality and Access to Information in Land Information Systems.* Belconnen, ACT.

15. Australian Law Reform Commission, "*Privacy*," Report No. 22, 1983, para 599.

16. Bank of Montreal. 1992. *Your Privacy: How the Bank of Montreal Protects it*, May 1992.

17. Bank of Montreal. 1993. *First Principles: Our Code of Conduct*, April 1993.

18. Bank of Nova Scotia. 1992. *ScotiaBank and You: A Question of Privacy*, February 1992.

19. Bank of Nova Scotia. February 1993. *Scotiabank: Complaint Resolution Standards and Procedures.*

20. Barlow, John Perry. "A Plain Text on Crypto Policy," Communications of the ICM 36 (1993): 21-26.

21. Baxter, J.D. 1990. *State Security, Privacy and Information.* New York. St. Martin's Press.

22. Beline, Craig T. *Transborder Data Flows: International Privacy Protection and the Free Flow of Information.* Boston College International and Comparative Law Review, Spring 1983. 591-624.

23. Bell, K.C. 1990. "Australian Council Cordinates Land Information." *GIS World.* August- September. pp.39-41

24. Beniger, James R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Harvard University Press. Cambridge.

25. Bennett, Colin J. "Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States," Governance 1 (1988a): 415-41

26. Bennett, Colin J. "Regulating the Computer: Comparing Policy Instruments in Europe and the United States," European Journal of Political Research 16 (1988b): 437-66.

27. Bennett, Colin J. "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson Drawing," Canadian Public Administration 33 (1990): 551-570.

28. Bennett, Colin J. "Computers, Personal Data and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s," Science, Technology and Human Values 16 (1991c): 51-69.

29. Bennett, Colin J. 1994. *"The Political Economy of Privacy".* Genome Project Conference, Centre for Social and Legal Research.

30. Bennett Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca and London: Cornell University Press. New York.

31. Bennett, Colin J. 1995. Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association. Resdale: CSA, 1995.

32. Bennett, Colin J. 1995. Privacy Protection on the Information Highway. Policy Options 16 (1995): 43-5.

33. Bennett, Colin J. 1995. *The Political Economy of Privacy: A Review of the Literature.* Hackensack, NJ: Center for Social and Legal Research.

34. Bennett, Colin J. 1996. Rules of the Road and Level-Playing Fields: The Politics of Data Protection in the Canadian Private Sector. International Review of Administrative Sciences 62 (1996): 479-92.

35. Bennett, Colin J. 1996a. "Privacy standards: an innovation in national and international policy." *Privacy Laws and Business Newsletter.* Vol. 36, September 1996: 8-10.

36. Bennett, Colin J. 1996b. "Protecting Privacy on the Canadian Information Highway: Policy Developments and Regulatory Options." *Canadian Journal of Information and Library Science,* 21: 1-19.

37. Bennett, Colin J. 1996a. Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector. Ottawa: Industry Canada. (www. privacy.org/pi/countries/canada/bennett _regulating_privacy.html)

38. Bennett, Colin J. 1996a. "The Public Surveillance of Personal Data: A Cross-National Analysis," in David Lyon And Elia Zureik eds. Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

39. Bennett, Colin J. & Charles D. Raab. 1997. "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response." *The Information Society,* 13 (4): (forthcoming).

40. Bennett, Colin J. 1997. "Adequate Data Protection by the year 2000: The Prospects for Privacy in Canada," International Review of Law, Computers and Technology 11: 79-93.

41. Bennett, Colin J. 1997b. "Understanding Ripple Effects: The Cross-National Adoption of Policy Instruments for Bureaucratic Accountability," Governance 10: 213-34.

42. Bennett, Colin J. 1997. Arguments for the Standardization of Privacy Protection Policy: Canadian Initiatives and American and International Responses. Government Information Quarterly 14(4): 351-362.

43. Bennett, Colin J. and Charles D. Raab. 1998. The Distribution of Privacy Risks: Who Needs Protection? The Information Society 14: 263-274.

44. Bennett, Colin J., Charles D. Raab, Robert M. Gellman, Nigel Waters. 1998. Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer. University of Edinburgh: European Commission.

45. Bensman, Joseph & Robert Lilienfeld. 1979. Between Public and Private: The Lost Boundaries of the Self. New York: Free Press.

46. Berelson, B. 1959. The State of Communication Research. *Public Opinion Quarterly.* Spring '59. Vol.23. pp.1-17.

47. Berry, J.K. 1993. *Beyond Mapping: Concepts, Algorithms and Issues in GIS.* GIS World Inc. Fort Collins.

48. Bolstad, P.V. and Smith J.L., 1992. "Errors in GIS." *Journal of Forestry.* Vol.90 No.11 pp. 21-31.

49. Bourn, Colin & John Benyon (eds.). *Data Protection: Perspectives on Information Privacy.* University of Leicester, Continuing Education Unit, 1984.

50. Branscomb, Anne Wells. 1994. Who Owns Information? From Privacy to Public Access. New York: Basic Books, 1994.

51. British Columbia Provincial Government (1992*). Bill 50: Freedom of Information and Protection of Privacy Act* (British Columbia) 1992.

52. British Columbia Information and Privacy Commissioner, Annual Reports 1993-99.

53. Burkert, Herbert. 1982. "Institutions of Data Protection: An Attempt at a Functional Explanation of European National Data Protection Laws," Computer Law Journal 3 (1982): 167-88.

54. Bygrave, Lee A. 1997. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. International Journal of Law and Information Technology 6(3): 247-284.

55. Canadian Bankers Association (CBA). 1996. *Privacy Model Code: Protecting Individual Bank Customers' Personal Information.* Toronto: CBA.

56. Canadian Imperial Bank of Commerce (CIBC). 1992. *Straight Answers: The CIBC Commitment to Privacy of Customer Information*, March 1992; Your Right to Privacy: Resolving your Complaint.

57. Canadian Direct Marketing Association (CDMA). 1993. *Privacy Code.* Don Mills: CDMA.

58. Canadian Direct Marketing Association (CDMA). 1995. *Direct Marketers Call for National Privacy Legislation.* CDMA News Release, October 3, 1995. Don Mills: CDMA.

59. Canadian Direct Marketing Association (CDMA). 1997, forthcoming. *Making the CSA Privacy Code Work for You.* PLUS 8808. Rexdale: CSA.

60. Canada, An Act to enact the Access to Information Act and the Privacy Act, SC 1980-81-82-83, C. 111, schedule II. The *Privacy Act* is at http//infoweb.magi.com/~privcan/

61. Canada. Communications Canada. 1992. Telecommunications Privacy Principles. Ottawa: Minister of Supply and Services Canada, 1992.

62. Canada, House of Commons Standing Committee on Justice and Solicitor General. Open and Shut: Enhancing the Right to Know and the Right to Privacy. Ottawa: Minister of Supply and Services, 1987.

63. Canada, Industry Canada. Privacy and the Canadian Information Highway. Ottawa: Industry Canada, 1994.

64. Canada, Information Commissioner. Annual Reports 1984-1999. Ottawa: Minister of Supply and Services.

65. Canada, Information Highway Advisory Council. Connection, Community, Content: The Challenge of the Information Highway. Ottawa: Minister of Supply and Services, September 1995.

66. Canada, Ministry of Justice Crossing the Borders of Privacy Ottawa: Ministry of Justice, 1991.

67. Canada, Privacy Commissioner. Annual Reports 1983-1999. Ottawa: Canada Communication.

68. Canada, Privacy Commissioner. 1992. Genetic Testing and Privacy. Ottawa: Minister of Supply and Services.

69. Canadian Life and Health Association (CLHIA). 1993. *Right to Privacy Guidelines*. Toronto: CLHIA.

70. Canadian Standards Association 1996. *Model Code for the Protection of Personal Information.* Canadian Standards Association. Ottawa, Ontario, Canada, p.ix

71. Canadian Survey Research Council. 1996. Canadian Attitudes to Survey Research and Issues of Privacy. Toronto: Canadian Survey Research Council, 1996.

72. Canadian Television Standards Council (CTSC). 1991. *Cable Television Customer Service Standards*. Ottawa: CTSC.

73. Canadian Department of Communication/Department of Justice Task Force. "*Privacy and Computers*," 1972, p. 164.

74. Carrol, N.J.,"*Protection of Personal Privacy in the Insurance Industry*,"Proceedings of the Privacy in Financial Services Conference, Toronto, 1994, p. 6.

75. Cassettari, S. 1993. *Introduction to Integrated Geo-information Management*. London. Chapman and Hall.

76. Cate, Fred H., 1997. Privacy in the Information Age. Washington: Brookings Institution Press, 1997.

77. Cavoukian, Ann and Don Tapscott. 1995. Who Knows: Safeguarding Your Privacy in a Networked World. Toronto: Random House, 1995.

78. Cawkell, A.E. 1987. *Evolution of an Information Society*. London. Aslib. Center for Public Integrity, Nothing Sacred - The Politics of Privacy. Washington: The Center for Policy Integrity, 1998.

79. Chaffey, Douglas Camp. 1993. "The Right to Privacy in Canada," Political Science Quarterly 108 (1993): 117-132.

80. Chambers, D. 1989. "Overview of GIS Database Design." *ARC News*. Vol.11 No.2 Spring 1989.

81. Chaum, David. 1985."Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM 28 (1985): 1030-1044.

82. Chaum, David. 1992. "Achieving Electronic Privacy," Scientific American August 1992: 96-101.

83. Citibank. 1992. *Privacy Code for Individual Customers*, January 1992.

84. Clarke, Roger A. 1989. "Information Technology and Dataveillance," Communications of the ACM 31 (1989): 498-512.

85. Clarke, Roger A. 1992. "The Resistable Rise of the National Personal Data System," Software Law Journal V (1992): 29-59.

86. Commission d'Accès à L'Information du Quebec (CAI). 1996a. Assessment of the Health Smart Card Pilot Project Conducted in the Region of Rimouski. Montreal: CAI, March 1996.

87. Commission d'Accès à L'Information du Quebec (CAI). 1996b. Background Paper on Identity Cards in Quebec. Montreal: CAI, October 1996. [http://www.sai.gouv.qc.ca/identang.htm]

88. Commission d'Accès à L'Information du Quebec (CAI) & Centre Information et Droit. (1996c) The Health Card and its Acceptability. Brussels: DG XIII Eurocards Concerted Action, August 1996.

89. Congalton, R.G. and Green, K., 1992. "The ABCs of GIS." *Journal of Forestry. Vol.*90 No.11 pp. 13-20

90. Council of Europe Convention No. 108 of 18 September 1980, Strasbourg.

95. Council of Europe, Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data. Strasbourg: Council of Europe, 1981.

96. Coward, P. and Heywood, I.,1991, *"Aspects of Uncertainty in Spatial Decision-Making"*. Proceedings of the 2nd European Conference on GIS, Brussels, Belgium, Vol. 1, pp. 233-242.

96. Culnan, Mary. "How Did They get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information use," MIS Quarterly Vol. 7, No. 3, September 1993.

97. Curry, Michael R. 1997. The Digital Individual and the Private Realm. Annals of the Association of American Geographers 87 (4): 681-699.

98. Curry, M.R. 1994. "Data Protection and Intellectual Property: Information Systems and the Americanization of the New Europe." *Environment and Planning A*

99. Curry, M.R. 1994. "Rethinking Rights and Responsibilities in Geographic Information Systems: Beyond the Power of the Image." *Cartography and Geographic Information Systems*

100. Dale, P.F., and McLaughlin, J.D. 1988. *Land Information Management*. Oxford. Clarendon Press.

101. Dammann, Ulrich, Otto Mallmann, and Spiros Simitis. 1977. Data Protection Legislation: An International Documentation. Frankfurt am Main: Metzner, 1977.

102. Dangermond, J. 1991. "Sharing Government's Digital Geographic Information with the Public." *GIS Law*. Vol 1. No. 3. pp. 19-20.

103. Dansby, B.H. 1991. "Survey and Analysis of State GIS Legislation." *GIS Law*. Vol. 1. No. 1. pp. 7-14.

104. Dansby, B.H. 1991. "Public Records and Governmental Liability." *GIS Law*. Vol. 1. No. 2. pp. 8-16.

105. Dansby, B.H. 1991. "Public Records and Governmental Liability - Part II." *GIS Law*. Vol. 1. No. 3. pp. 10-14.

107. Data Protection Registrar (UK). 1993. Ninth Report. London: HMSO.

108. Davies, Simon. 1992. Big Brother: Australia's Growing Web of Surveillance. Sydney: Simon & Schuster, 1992.

109. Davies, Simon. 1996. Big Brother: Britains Web of Surveillance and the New Technological Order. London: Pan Books, 1996.

110. Davies, Simon. 1995a. A Case of Mistaken Identity: An International Study of Identity Cards. Toronto: Information and Privacy Commissioner of Ontario.

111. Davies, Simon. 1995b. "The Worst ID They Ever Had," Wired, June 1995.

112. De Rijcke, I. and Logan, R., 1990. "The Consequences of Certain Choices in GIS/LIS Design: Enhancement in the Integrity of Land Ownership." Ottawa, ON. *Proceedings of the GIS for the 90's Conference.*

113. Department of Environment. 1987. *Handling Geographic Information; Report of the Committee of Inquiry Chaired by Lord Chorley*. London. Her Majesty's Stationery Office.

114. Digital Equipment Corporation, 1990. *White Paper: Integrated Spatial Information Systems.*

115. Dix, A., 1996, *The German RailwayCard: A model contractual solution of the adequate level of protection issue.* Proceedings of the 18th International Privacy and Data Protection Conference, Ottawa, Canada

116. Doern, G. Bruce & Richard W. Phidd. 1992. Canadian Public Policy: Ideas, Structure, Process 2nd ed. Toronto: Nelson Canada.

117. Doern, G. Bruce 1996. "Regulatory Bodies, Regimes and Institutions: A Framework and Issues for Reform," Paper prepared for the Conference on UK-North American Regulatory Institutions, University of Exeter, April 9-10, 1996.

118. Dutton, William H. & R.G. Meadow, 1986. "A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties." In Government Infrastructures ed. K. B.Levitan. New York: Greenwood Press, 1986.

119. Dutton, William & Robert Meadow. 1985. "Public Perspectives on Government Information Technology: A Review of Survey Research on Privacy, Civil Liberties and the Democratic Process." Report prepared for the US Congress Office of Technology Assessment (OTA). Washington DC: OTA.

120. Eger, J.M. 1978. Emerging Restrictions on Transnational Data Flow: Privacy Protection or Non-Tariff Trade Barriers? *Law and Policy in International Business* 10: 1055-1103.

121. Ekos Research Associates. 1993. Privacy Revealed: the Canadian Privacy Survey. Ottawa: Ekos, 1993.

122. Electronic Funds Transfer Working Group (EFT). 1992. *Canadian Code of Practice for Consumer Debit Card Services*. May 1, 1992.

123. Ericson, Richard V. and Kevin D. Haggerty, 1997. Policing the Risk Society. Toronto: University of Toronto Press, 1997.

124. Etzioni, Amatai. 1993. Spirit of Community: Rights, Responsibilities and the Communitarian Agenda. New York: Simon and Schuster.

125. European Union. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data. Brussels: OJ No. L281. October 24 1995.

126. Fabowale, Lola. 1994. *Voluntary Codes: A Viable Alternative to Government Legislation?* Ottawa: Public Interest Advocacy Centre.

127. Finance Canada. 1996. *1997 Review of Financial Sector Legislation: Proposals for Changes.* Ottawa: Department of Finance, June 1996. [http://www.fin.gc.ca]

128. Flaherty, David H. 1967. Privacy in Colonial New England. Charlottesville: University Press of Virginia.

129. Flaherty, David H. 1979. Privacy and Government Data Banks: An International Perspective. London: Mansell, 1979.

130. Flaherty, David H. 1983. "*Data Protection and Privacy: Comparative Policies*," a report to the Government Information Technology Project, Office of Technology Assessment, U.S. Congress, January 1983, p. 85

131. Flaherty, David H. 1984a. Nineteen Eighty-Four and After. Final Report of the Bellagio Conference on Current and Future Problems of Data Protection. London: University of Western Ontario Privacy Project.

132. Flaherty, David H. 1984b. "The Need for an American Privacy Protection Commission," Government Information Quarterly 1: 235-58.

133. Flaherty, David H. 1984. *Protecting Privacy in Two-Way Electronic Services.* White Plains, NY: Knowledge Industry Publications, 1984.

134. Flaherty, David H. 1984. *Privacy and Data Protection: An International Bibliography.* David H. Flaherty, ed. London: Mansell Publishing Ltd., 1984.

135. Flaherty, David H. 1986. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies," Science, Technology, and Human Values 11 (1986): 7-18.

136. Flaherty, David H. 1988. *The Emergence of Surveillance Societies in the Western World.* Government Information Quarterly, Vol. 5, No. 4, 1988. 377-387.

137. Flaherty, David H. 1989. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, NC: University of North Carolina Press, 1989.

138. Flaherty, David H. 1993. *"Computers and Privacy: Whether to Regulate the Private Sector,"* 1993, p. 8.

139. Flaherty, David H. 1996. "Privacy and Identity." Speech of October 1996 [www.oipcbc.org].

140. Foster, H.D., and Carey, R.F. 1976. *The Simulation of Earthquake Damage.* Victoria. Western Geographical Series. Vol.12. pp.221-239.

141. Foucault, Michel. 1979 Discipline and Punish: The Birth of the Prison. New York: Vintage Books, 1979.

142. Frankel Mark. S. & Albert Teich eds. 1994. The Genetic Frontier: Ethics, Law and Public Policy. Washington: American Association for the Advancement of Science, 1994.

143. Freedman, Warren. 1987. The Right of Privacy in the Computer Age. New York: Quorum Books, 1987.

144. Gandy, Oscar. 1992. The Panoptic Sort. Boulder: Westview Press, 1992.

145. Gandy, Oscar.. "Information Privacy and the Crisis of Control," in Communication: For and Against Democracy ed. Peter Bruck.

146. Gandy, Oscar. 1991. "The Anticipatory Response: Avoiding the Destructive Gales of Popular Resistance." Paper presented to Nineteenth Annual Telecommunications Policy Research Conference, Soloman Island, Maryland, September 1991.

147. Gandy, Oscar. & Todd Kristel. 1990. "Conditioning Consent: In Search of the Social Locations of Privacy Orientations in the Age of Surveillance." In Developments of Communications and Democracy: Main Papers and Abstracts of the 17th IAMCR Conference, ed. S. Splichal. Ljubljana: International Association for Mass Communication Research, 1990.

148. Gellman, Robert M. 1993. "Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions," Software Law Journal VI (1993): 199-238.

149. Gellman, Robert M. 1996. Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules. Villanova Law Review 41 (1): 129-172.

150. Givens, Beth, 1997. The Privacy Rights Handbook - How to Take Control of Your Personal Information. New York: Avon Books, 1997.

151. Government of Canada (1985). *Access to Information Act* (Canada) R.S.C. 1985, c. A-1 as amended.

152. Government of Canada (1985). *Privacy Act* (Canada) R.S.C. 1985, c.P-5 as amended.

153. Government of Canada, November 7, 1995. Press Release. "Banks Appoint an Industry Ombudsman to Review Small Business Complaints."

154. Great Britain, Home Office. 1972. Report of the Committee on Privacy. (The Younger Committee, Cmnd. 5012). London: HMSO, 1972.

155. Green, K.,1992. "Spatial Imagery and GIS." *Journal of Forestry.* Vol.90 No.11 pp. 32-36.

156. Greenleaf, G. 1995. The 1995 EU Data Protection Directive on Data Protection - An Overview. *The International Privacy Bulletin* 3 (2): 1-21.

157. Grove, M. and Hohmann, M., 1992. "Social Forestry and GIS." *Journal of Forestry.*Vol.90 No.12 pp. 10-15.

158. Goodchild, M. and Gopal, S. 1989. *The Accuracy of Spatial Databases*. New York. Taylor and Francis.

159. Goodey, B.R. 1969." Messages in Space: Some Observations on Geography and Communications." *North Dakota Quarterly*. Spring. pp.34-49.

161. Harris Louis and Alan F. Westin. 1990. The Equifax Report on Consumers in the Information Age. Georgia: Equifax Inc. 1990.

162. Harris Louis. 1992. The Equifax Canada Report on Consumers in the Information Age. Ville d'Anjou: Equifax Canada Inc. 1992.

163. Harris Louis. 1994. The Equifax Canada Report on Consumers and Privacy in the Information Age. Ville d'Anjou: Equifax Canada Inc. 1994

164. Harris Louis. 1995. *The Equifax Canada Report on Consumers and Privacy in the Information Age.* Ville d'Anjou: Equifax Canada.

165. Hixson, Richard F. 1987. Privacy in a Public Society: Human Rights in Conflict. New York: Oxford University Press, 1987.

166. House of Commons, Standing Committee on Justice and Solicitor-General. 1987. *Open and Shut: Enhancing the Right to Know and the Right to Privacy.* Ottawa: Supply and Services Canada.

167. Howlett, Michael & M. Ramesh. 1995. Studying Public Policy: Policy Cycles and Policy Subsystems Toronto: Oxford University Press.

168. Hunter, G.J. and Goodchild, M.F. 1993. *"Managing Uncertainty in Spatial Databases: Putting Theory into Practice".* Proceedings of the Urban and Regional Information Systems Association. Atlanta, Georgia, U.S.A., Vol. 1, pp. 1-14.

169. Hunter, Lawrence & James Rule. 1994. "Toward Property Rights in Personal Information." Unpublished paper, January 15, 1994.

170. Industry Canada. 1994. Privacy and the Canadian Information Highway. Ottawa: Industry Canada, 1994.

171. Industry Canada.1996. Building the Information Society: Moving Canada into the 21st Century. Ottawa: Industry Canada, 1996.

172. Information Highway Advisory Council. 1995. Connection, Community, Content: The Challenge of the Information Highway. Ottawa: Minister of Supply and Services Canada, 1995.

173. Institute for Public Policy Research (IPPR). 1995. Identity Cards Revisited: A Consultation Paper. London: IPPR and Justice.

174. Insurance Bureau of Canada (IBC). 1992. *Model Privacy Code*. Toronto: IBC.

175. Inter-Agency Committee on Geomatics, 1996. Barriers to the Use of Geomatics Data. Ottawa. Inter-Agency Committee on Geomatics.

176. Justice Canada. 1972. Privacy and Computers Ottawa: Information Canada.

177. Justice Canada. 1987. *Access and Privacy: The Steps Ahead*. Ottawa: Supply and Services Canada.

178. Justice Canada. 1990. *Crossing the Borders of Privacy: Transborder Flows of Personal Data from Canada.* Ottawa: Justice Communication and Public Affairs.

179. Katz, James E. 1987. "Telecommunications and Computers: Whither Privacy Policy?" Society 25 (1987): 81-86.

180. Katz, James E. & Annette R. Tassone. 1990. "Public Opinion Trends: Privacy and Information Technology," Public Opinion Quarterly, Spring 1990. 54: 125-43.

181. Katz, James E. 1991. "Public Concern Over Privacy: The Phone is the Focus," Telecommunications Policy. April 1991: 166-169.

182. Katz, James E. & Merton M. Hyman. 1993. "Dimensions of Concern over Telecommunications Privacy in the United States," The Information Society, 1993. 9: 251-275.

183. Kennett, S.A., 1992. "Issues and Options for Intergovernmental Cooperation in Environmental Impact Assessment." *Resources: Canadian Institute of Resource Law*. No 39 Summer 1992.

184. Kennett, S.A., 1992. "Is British Columbia Leading the Way in Natural Resources Management? Part 1: The Commission on Resources and the Environment." *Resources: Canadian Institute of Resource Law*. No 40 Fall 1992.

185. Kessler, B.L.,1992. "Glossary of GIS Terms." *Journal of Forestry*. Vol.90 No.11 pp. 37-45.

186. Kirby, Michael D. 1980. "Transborder Data Flows and the 'Basic Rules' of Data Privacy," Stanford Journal of International Law 16 (1980): 27-66.

187. Konsynski, B.R., and McFarlan, E.W. 1990. "Information Partnerships - Shared Data, Shared Scale." *Harvard Business Review*. September-October. pp.114-120.

188. Lachowski, H., Maus, P. and Platt, B., 1992. "Integrating Remote Sensing and GIS." *Journal of Forestry*. Vol.90 No.12 pp. 16-21.

189. Lapernere, R., Cote, R. and LeBel, G., 1992. "The Transborder Flow of Personal Data from Canada: International and Comparative Law Issues," 32 Jurimetrics, 1992, p.547.

190. Laperriere, Rene. 1994. *Privacy and the Private Sector: Protection of Privacy in the Federal Private Sector*. Montreal: Groupe de Recherche Informatique et Droit, March 1994

191. Lawson, Ian. 1992. *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector*. Ottawa: Public Interest Advocacy Centre.

192. Lawson, Ian. 1995. *Privacy and the Information Highway: Regulatory Options for Canada*. Ottawa: Industry Canada.

193. Laudon, Kenneth C. 1996. Markets and Privacy. Communications of the ACM. 39 (1996): 92-104.

194. Laudon, Kenneth C. 1986. Dossier Society. New York: Columbia University Press.

195. Laurini, R., and Thompson D. 1992. *Fundamentals of Spatial Information Systems*. London. Academic Press.

196. Liberty, 1989. Identity Cards and the Threat to Civil Liberties. Civil Liberty Briefing No. 12, September 1989.

197. Linowes, David F., 1989. Privacy in America: Is Your Private Life in the Public Eye? Urbana: University of Illinois Press, 1989.

198. Linowes, David F., and Colin J. Bennett. 1986. "Privacy: Its Role in Federal Government Information Policy," Library Trends 31 (1986): 19-42.

199. Lipset, Seymour Martin. 1990. Continental Divide: The Values and Institutions of the United States and Canada. New York: Routledge.

200. Loader, Brian D. Ed., 1997. The Governance of Cyberspace. New York: Routledge, 1997.

201. Lopez, X.R. 1993. Database Copyright Issues in the European GIS Community. *Government Information Quarterly*. Vol.10. No.3. pp.305-318.

202. Lyon, David. 1991. "British Identity Cards: The Unpalatable Logic of European Membership?" The Political Quarterly 62 (1991): 377-385.

203. Lyon, David. 1991. "Bentham's Panopticon: From Moral Architecture to Electronic Surveillance," Queen's Quarterly 98 (1991): 596-617.

204. Lyon, David. 1992. "The New Surveillance: Electronic Technologies and the Maximum Security Society," Crime, Law and Social Change 18: 159-172.

205. Lyon, David. 1994. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press. 1994.

206. Lyon, David & Elia Zureik. 1995 forthcoming. New Technology, Surveillance and Social Control. Minneapolis: University of Minnesota Press.

207. Lyon, David. 1997. The End of Privacy. Policy Options 18(3): 3-7. Lyon, David & Elia Zureik (eds.) Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press. 1996.

208. Manitoba Provincial Government (1985-86). *The Freedom of Information Act (*Manitoba) S.M. 1985-86, c.6 (C.C.S.M., c.175)

209. Marsh, N. ed. 1987. Public Access to Government-Held Information: A Comparative Symposium. London: Stevens, 1987.

210. Marx, Gary. 1988. Undercover: Police Surveillance in America. Berkeley: University of California Press, 1988.

211. Masser, I., and Blakemore, M. 1991. *Handling Geographical Information*. New York. Longman Scientific and Technical.

212. Mazmanian, Daniel A. & Paul A. Sabatier. 1983. Implementation and Public Policy. Glenview, Ill: Scott, Foresman.

213. McAllister, S., 1991. "Environmental Jurisdiction under the Australian Constitution." *Resources: Canadian Institute of Resource Law.* No 33 Winter 1991.

214. McBride, T. 1987. "Data Privacy: An Options Paper," paper released by the Minister of Justice, New Zealand, 1987, p. 92.

215. Mellors, C. & Pollitt, D. 1984. "Legislating for Privacy: Data Protection in Western Europe," Parliamentary Affairs 37 (1984): 199215.

216. Michell-Viret, Christopher. 1989. *"An assessment of the level of Federal-Provincial Co-operation in the Management of Alberta Water Resources".* M.Sc. , University of Alberta. Edmonton, Alberta, Canada, pp. 412.

217. Michell-Viret, Christopher., Giffen, Barry., Guthrie, James., Jacob, Ron., McKay, Laurel. 1992. *"Information System Inputs to Programs, Applications of IS/GIS in Government".* Proceedings of the Urban and Regional Information Systems Association. Washington, D.C., U.S.A., Vol. 5, pp. 206-240.

218. Michell-Viret, Christopher. 1993. *"Data access: a keystone to GIS."* Proceedings of the 7th Annual Symposium on Geographic Information Systems in Forestry, Environment and Natural Resources Management. Vancouver, British Columbia, Canada, Vol. 2, pp. 1049-1056.

219. Michell-Viret, Christopher. 1995. *"GIS, Integrated Information Resources Management and Data Access: Challenges in Information Ethics."* Proceedings of GIS'95, the Ninth Annual Symposium on Geographic Information Systems. Vancouver, British Columbia, Canada, Vol 1, pp.196-202.

220. Michell-Viret, Christopher. 1997. *"Surfer of the Information Highway or Informational Serf: Cultural Implications of our Information Management Practices."* Proceedings of the Eleventh Annual Symposium on Geographic Information Systems. Vancouver, British Columbia, Canada, Vol.1, pp.581-586.

221. Michell-Viret, Christopher. 1997. *"Technological Slave or Informational Serf: Cultural Implications of operating on the Information Highway."* Proceedings of the Urban and Regional Information Systems Association. Park Ridge. IL, U.S.A., Vol. 1, pp. 203-214.

222. Michell-Viret, Christopher. 1998. *"Planning Globally, Acting Privately: Privacy in our Global Information Economy."* Proceedings of the Urban and Regional Information Systems Association. Park Ridge. IL, U.S.A., Vol. 1.

223. Michell-Viret, Christopher. 1999. "*Private Lives, Public Partnerships: Advances in Private Sector Privacy Protection.*" Proceedings of the Urban and Regional Information Systems Association. Park Ridge. IL, U.S.A

224. Michell-Viret, Christopher. 2001. "*Virtual Privacy: Tracking Electronic Footprints in Cyberspace.*" Proceedings of the Fifteenth Annual Symposium on Geographic Information Systems. Vancouver, British Columbia, Canada, Vol.1.

225. Millar, Melanie. 1995. "Protecting Privacy in Canada: Evaluating Recent Solutions Proposed for and by the Private Sector," Government Information in Canada 2:1.3. (www.usask.ca/library/gic/v2n1/millar/millar.html)

226. Milrad, L.H. 1990 "Multiparticipant GIS Projects: Some Legal Issues." *Proceedings of the GIS for the 90's Conference*. Ottawa. ON.

227. Milrad, L.H. 1991 "Contracting for GIS Technology: Part 1." *GIS Law*. Vol.1. No.1. pp. 14-15.

228. Milrad, L.H. 1991 "Contracting for GIS Technology: Part 2." *GIS Law*. Vol.1. No.2. pp. 16-17.

229. Milrad, L.H. 1991 "Contracting for GIS System - The Purchaser's Perspective: Part 1." *GIS Law*.Vol.1. No.3. pp. 15-18.

230. Monti, M. 1995. *Council Definitively Adopts Directive on Protection of Personal Data*. European Commission Press Release, IP/95/822, July 25, 1995.

231. Muraskin, W. 1993. "Individual Rights vs The Public Health: The Problem of the Asian Hepatitis B Carries in America." *Social Science Medicine.* Vol.36. No.3. pp.203-216.

232. National Aeronautics and Space Administration. 1987. Overview of Research Needs and the Research Agenda. Arlington. VA. *Proceedings of the International Geographic Information Systems (IGIS) Symposium.*

233. National Bank of Canada. 1992. *Strictly Between You and Us: Confidentiality of Personal Information*, June 1992.

234. National Centre for Geographic Information and Analysis. 1995. *Law and Information Policy for Spatial Databases.* Orono. ME. National Centre for Geographic Information Analysis.

235. National Centre for Geographic Information and Analysis. 1992. A Research Agenda for Geographic Information and Analysis. New York. *NCGIA Technical Report 92-7.*

236. New Brunswick Provincial Government (1978), *Right to Information Act* (New Brunswick) S.N.B. 1978, c.R-10.3, as amended

237. Newfoundland Provincial Government (1981). *The Freedom of Information Act* (Newfoundland) S.N. 1981, c.5 as amended by S.N. 1981, c.85.

238. New South Wales, The Privacy Committee of New South Wales, 1991. "Privacy and Data Protection in New South Wales: A Proposal for Legislation," submission to the Independent Commission Against Corruption, No. 63, June 1991, pps. 28-29, 36, 38.

239. Nichol, S. 1991."*Canadian Land Surveyor's Approach to Copyright, Liability and Privacy Issues in the Information Economy*." *ALS News*, Nov/91.

240. Nora, Simon & Alan Minc. *The Computerization of Privacy*. Cambridge: MIT Press, 1980.

241. Nova Scotia Provincial Government (1990). *Freedom of Information Act* (Nova Scotia) S.N.S. 1990, c.11

242. Obermeyer, N. and Pinto, J. 1994. *Managing Geographic Information Systems*. New York. Guilford.

243. O'Brien, David M. 1979. *The Privacy, Law and Public Policy*. New York. Praeger Publishers.

244. Onsrud, H.J. and Rushton, G. 1995. *Sharing Geographic Information*. New Jersey. Rutgers.

245. Onsrud, H.J. 1991 "In Support of Open Access for Publicly Held Geographic Information." *GIS Law*. Vol. 1 No. 1.

246. Onsrud, H.J. 1991 "Evidence generated by GIS." *GIS Law*. Vol. 1 No. 3.

247. Ontario, Information and Privacy Commissioner. 1993. Smart Cards. Toronto: IPC.

248. Ontario, Information and Privacy Commissioner. 1994a. *Privacy Protection Makes Good Business Sense*. Toronto: OIPC.

249. Ontario, Information and Privacy Commissioner. 1994b. *Privacy Alert: A Consumer's Guide to Privacy in the Marketplace*. Toronto: OIPC.

250. Ontario, Information and Privacy Commissioner & Netherlands Registration Chamber. 1995. Privacy-Enhancing Technologies: The Path to Anonymity. Toronto: OIPC.

251. Ontario, Information and Privacy Commissioner (1995). *Privacy Protection Models for the Private Sector*. Toronto, Ontario, Canada

252. Ontario, Information and Privacy Commissioner (1997). *Geographic Information Systems*. Toronto, Ontario, Canada

253. Ontario Provincial Government (1993). *Managing Access to Government Data: Tradeable Data*. Toronto, Ontario, Canada. pp. 16

254. Ontario Provincial Government (1987). *Freedom of Information and Privacy Act* (Ontario) S.O. 1987, c.25.

255. Ottawa Citizen, (1997)."Federal Smart Cards: Privacy vs. Savings," February 1, 1997.

256. Organization for Economic Cooperation and Development (OECD). 1976. *Policy Issues in Data Protection and Privacy.* OECD Informatics Studies no. 10. Paris: OECD.

257. Organization for Economic Cooperation and Development (OECD). 1981. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris, OECD, 1981.

258. Organization for Economic Cooperation and Development (OECD). 1994. "*Privacy and Data Protection Issues and Challenges*," Information Computer Communications Policy, Paris, 1994, pp. 12-13, 14, 17.

259. Paterson, Moira. 1998. Privacy Protection in Australia: The Need for an Effective Private Sector Regime. Federal Law Review 26: 371-400.

260. Peladeau, Pierrot. 1990. "The Informational Privacy Challenge: The Technological Rule of Law." In Ryszard I. Cholewinski, Ed. Human Rights in Canada: Into the 1990's and Beyond. Ottawa: Human Rights Research and Education Centre, 1990, 93-116.

261. Perey, A. and Janisch. H,. 1994. "International Restrictions on the Exchange of Information: Privacy, Transborder Data Flows and Trade in Services," a paper prepared for the Privacy in Financial Services Conference, Toronto, 1994, p. 3, 9.

262. Pitz, G.F. and McKillip, J. 1984. *Decision Analysis for Program Evaluators*. London. Sage.

263. Plesser, R. L. & E.W. Cividanes. 1991. *Privacy Protection in the United States.* Washington DC: Piper & Marbury.

264. Posner, R.A. 1978. *An Economic Theory of Privacy.* Washington D.C.. Regulation. May/June 1978. pp.19-26.

265. Posner, R.A. 1978b. "The Right to Privacy," Georgia Law Review 12: 393-422.

266. Poster, Mark, 1990. The Mode of Information. New York: Polity Press, 1990.

267. Poxter, John D., 1990. *State Security, Privacy and Information.* New York: Harvester Wheatsheaf, 1990.

268. Privacy and American Business. 1995. *Handbook of Company Privacy Codes.* Hackensack, NJ: Privacy and American Business.

269. Privacy Commissioner of Canada (OPC). 1989. Aids and the Privacy Act Ottawa: Minister of Supply and Services.

270. Privacy Commissioner of Canada (OPC). 1990. Drug-Testing and Privacy Ottawa: Minister of Supply and Services.

271. Privacy Commissioner of Canada (OPC). 1991. *Annual Report 1990-91.* Ottawa: Minister of Supply and Services, 1991.

272. Privacy Commissioner of Canada (OPC). 1992. *Annual Report 1991-92.* Ottawa: Minister of Supply and Services.

273. Privacy Commissioner of Canada (OPC). 1992b. Genetic Testing and Privacy Ottawa: Minister of Supply and Services.

274. Privacy Commissioner of Canada (OPC). 1993a. *Annual Report 1992-93.* Ottawa: Canada Communication Group.

275. Privacy Commissioner of Canada (OPC). 1993b. *Regulating Financial Institutions: Protecting the Privacy of Customers' Personal Information.* A Submission by the Privacy Commissioner of Canada to the Standing Senate Committee on Banking, Trade and Commerce.

276. Privacy Commissioner of Canada (OPC). 1994. *Annual Report 1993-94.* Ottawa: Canada Communication Group.

277. Privacy Commissioner of Canada (OPC). 1994. *Annual Report 1994-95.* Ottawa: Canada Communications Group.

278. Privacy Commissioner of Canada (OPC). 1996. Annual Report 1995-96. Ottawa: Canada Communications Group.

279. Privacy Commissioner of Canada (OPC). 1996. Privacy Framework for Smart Card Applications. Ottawa: OPC.

280. Public Interest Advocacy Centre (PIAC). 1995. *Surveying Boundaries: Canadians and their Personal Information.* Ottawa: PIAC.

281. Quebec Provincial Government (1982). *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (Quebec) S.Q. 1982, c.30 (R.S.Q., c. A-21) as amended

282. Quebec Provincial Government. (1993). *An Act Respecting the Protection of Personal Information in the Private Sector.* Quebec Official Publisher.

283. Raab, Charles D. 1993a. "Data protection in Britain: governance and learning", Governance, 6 (1993a): 4366.

284. Raab, Charles D. 1993. "Measuring the Performance of Data Protection Systems." Paper presented to the 6th Annual Conference of Privacy, Laws and Business, St. Catherine's College, Oxford.

285. Raab, Charles D. 1993b."The governance of data protection" in J. Kooiman (ed.), Modern Governance. London & Beverly Hills: Sage, 1993b.

286. Raab, Charles D. & Colin J. Bennett. 1994. "Protecting Privacy across Borders: European Policies and Prospects," Public Administration 72 (1994).

287. Raab, Charles D. 1995. "Taking the Measure of Privacy on the Information Highway." Paper presented to the PICT International conference on the *Social and Economic Implications of Information Communication Technologies*, London, May 1995.

288. Raab, Charles D. (1996) "Taking the Measure of Privacy: Can Data Protection be Evaluated." In special issue of *International Review of Administrative Sciences* on "Implementing Data Protection: The Politics of Privacy in Information Societies" eds. van de Donk, Bennett and Raab (forthcoming).

289. Raab, Charles D. Privacy, democracy, information", in Brian D. Loader Ed. The Governance of Cyberspace. New York: Routledge, 1997.

290. Radford, Greg. 1993. "Watershed Planning Using GIS to Make Sustainable Decisions," Plan Canada, July 1993. p.19

291. Rankin, Murray. 1997. Freedom of Information In Canada: Will the Doors StayShut. Ottawa: Canadian Bar Association, 1977.

292. Rankin, Murray. 1984. "Privacy and Technology: A Canadian Perspective," Alberta Law Review XXII (1984): 323-347.

293. Reagan, Michael D. 1987. Regulation: The Politics of Policy Boston: Little Brown.

294. Regan, Priscilla M. 1981. "Public Uses of Private Information: A Comparison of Personal Information Policies in the United States and Britain." Ph.D., Cornell University.

295. Regan, Priscilla M. 1984. "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations," Journal of Public Policy 4 (1984): 19-38.

296. Regan, Priscilla M. 1990. "Protecting Privacy and Controlling Bureaucracies: Constraints of British Constitutional Principles." Governance 3 (1990): 33-54.

297. Regan, Priscilla M. 1993a. "Surveillance and New Technologies: Changing Nature of Workplace Surveillance," Paper presented to the Strategic Research Workshop on "New Technology, Surveillance and Social Control," Queen's University, May 1993.

298. Regan, Priscilla M. 1993b. "Ideas of Interests: Privacy in Electronic Communications," Policy Studies Journal 21: 450-469.

299. Regan, Priscilla M. 1994. "The Globalization of Privacy: Implications of Recent Changes in Europe." American Journal of Economics and Sociology 52: 257-74.

300. Regan, Priscilla M. 1995. (forthcoming). Privacy, Technology and Public Policy. Chapel Hill: University of North Carolina Press.

301. Regan, Priscilla M. 1995. Legislating Privacy: Technology, Social Values and Public Policy. Chapel Hill: Horth Carolina Press, 1995.

302. Regan, Priscilla M. 1996. American Business and the European Data Protection Directive: Lobbying Strategies and Tactics. Paper presented to the *Visions for Privacy in the 21st Century* conference. Victoria, B.C. May 9-11, 1996.

303. Reidenberg, J. R. 1993. Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms. *Harvard Journal of Law and Technology* 6: 287-305.

304. Reidenberg, J. R. 1995. Setting Standards for Fair Information Practice in the U.S. Private Sector. *Iowa Law Review* 80 (3): 497-551.

305. Reidenberg, J.R. and Francoise Gamet-Pol. The Fundamental Role of Privacy and Confidence in the Network. Wake Forest Law Review 30 (1): 105-125.

306. Riley, Thomas D.. & Harold Relyea , 1983. Freedom of Information Trends in the InformationAge. London: Cass, 1983.

307. Roberts, A. (1998). *Freedom of Information Research Project.* School of Policy Studies, McGill-Queens University Press. Montreal.

308. Roger, E., and Kincaid, D.L. 1981."The Convergence Model of Communication and Network Analysis". *Communication Networks.* New York. Free Press.

309. Rotenberg, M. 1991. *Privacy Law in the United States: Failing to Make the Grade.* Washington DC: Computer Professionals for Social Responsibility.

310. Rotenberg, M.. 1994. "Privacy: Political Right or Economic Good," Address given to the 1994 Conference on Computers, Freedom and Privacy (CFP '94), Chicago, March 1994.

311. Rothfeder, Jeff. 1992. Privacy for Sale. New York: Simon and Shuster, 1992.

312. Rourck, R.W., 1993. "How Good is GIS in Local Government?" *GIS World.* June, 993 pp.52-56.

313. Royal Bank of Canada. 1991. *Privacy Code for Individual Customers, and Straight Talk about Client Privacy,* October 1991.

314. Rule, James B., 1974. Private Lives and Public Surveillance: Social Control in the Computer Age. New York: Schocken Books, 1974.

315. Rule, James B., Douglas MacAdam, Linda Stearns, and David Uglow. 1980. The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York: Elsevier, 1980.

316. Rule, J. and Hunter, L, 1994. *"Toward Property Rights in Personal Information,"* January, 1994.

317. Samar, Vincent J. 1991. The Right to Privacy: Gays, Lesbians and the Constitution. Philadelphia: Temple University Press, 1991.

318. Samarajiva, Rohan. 1994. Privacy in Electronic Public Space: Emerging Issues. Canadian Journal of Communication 19: 87-99.

319. Samet, H. 1989. *Application of Spatial Data Structures.* New York. Addison Wesley.

320. Samet, H. 1989. *The Design and Analysis of Spatial Data Structures.* New York. Addison Wesley.

321. Saskatchewan Provincial Government (1990-91*). The Freedom of Information and Protection of Privacy Act* (Saskatchewan) 1990-91 c. F-22.01

322. Schwartz, Paul. 1989. "The Computer in German and American Constitutional Law: Towards an American Right of Information Self-Determination," American Journal of Comparative Law 37: 675-701.

323. Schwartz, Paul. 1992. "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer," Hastings Law Journal 43 (1992): 1321-88.

324. Schwartz, Paul. 1995. European Data Protection Law and Restrictions on International Data Flows. Iowa Law Review 80 (3): 471-96.

325. Schwartz, Paul. 1995. Privacy and Participation: Personal Information and Public Sector Regulation in the United States. Iowa Law Review 80 (3), March 1995: 553-618.

326. Schwartz, Paul. 1995. The Protection of Privacy in Health Care Reform. Vanderbilt Law Review 48 (2): 295-347.

327. Schwartz, P.M & J. M. Reidenberg. 1996. *Data Privacy Law: A Study of United States Data Protection.* Charlottesville, VA: Michie.

328. Schwartz, Paul. 1997. Privacy and the Economics of Personal Health Care Information. Texas Law Review 76 (1): 1-75.

329. Shaw, Erin et al. 1994. The Privacy Handbook: A Practical Guide to your Privacy Rights in British Columbia and how to protect them. Vancouver: BC Civil Liberties Association, 1994

330. Sieghart, P. 1976. Privacy and Computers. London. Latimer New Dimensions.

331. Simitis, Spiros. 1987. "Reviewing Privacy in an Information Society," University of Pennsylvania Law Review 135 (1987): 707-46.

332. Simitis, Spiros. 1995. From the Market to the Polis: The *EU Data Protection Directive* on the Protection of Personal Data. *Iowa Law Review* 80 (3): 445-69.

333. Smith, H. Jeff. 1994. Managing Privacy: Information Technology and Corporate America. Chapel Hill: University of North Carolina Press, 1994.

334. Stone, Deborah. 1997. Policy Paradox: The Art of Political Decision-Making Hew York: Norton.

335. Stentor. 1992. *Model Code for Fair Information Practices*. Ottawa: Stentor Telecom Policy Inc.

336. Stentor. 1994. Privacy and the Information Highway: Stentor Submission to the Information Highway Advisory Council. Ottawa: Stentor Telecom Policy Inc.

337. Tomlinson, J. 1991. *Cultural Imperialism*. John Hopkins University Press. Baltimore.

338. Tonks, A. 1993. Information Management and Patient Privacy in the NHS. London. *British Medical Journal.* No.6914. Vol.307. 13Nov93. pp.1227-1228.

339. Toronto Dominion Bank. 1991. *Guidelines of Business Conduct,* November 1991.

340. Toronto Dominion Bank. 1991. *The TD Commitment: Protecting Your Privacy*, December 1991.

341. Trubow, G. B. 1992. The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flow. *Northwestern Journal of International Law and Business* 13 (1): 159-176.

342. Turkle, Sherry, 1997. Life on the Screen - Identity in the Age of the Internet. New York: Touchstone, 1997.

343. United Kingdom Data Protection Registrar. 1996. *Data Protection and the EU Directive 95/46/EC: Questions to Answer.* Wilmslow: Data Protection Registrar.

344. United Kingdom. 1995. Identity Cards: A Consultation Document. Cmnd. 2879. London: HMSO.

345. Uniform Law Conference of Canada (ULCC). 1996. *Data Protection in the Private Sector: Options for a Uniform Statute.* Ottawa: ULCC, August 1996.

346. United States Council for International Business, 1994. "*Private Sector Leadership: Policy Foundations for a National Information Infrastructure (NII). U.S. Business Views on Telecommunications, Information Security, Privacy, and Intellectual Property*," July 1994, p. 17.

347. United States Information Infrastructure Task Force (IITF). 1995. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, Final Version, June 6. Washington DC: IITF, Information Policy Committee, Privacy Working Group.

348. United States, House of Representatives, Subcommittee of the Committee on Government Operations, 1979. Hearings on Public Reaction to Privacy Issues. 96th Cong. 1st Sess. June 6, 1979.

349. United States, House of Representatives, Subcommittee of the Committee on Government Operations. 1984. Hearings on Privacy and 1984: Public Opinions on Privacy Issues. 98th Cong. 1st Sess. April 4, 1984.

350. United States Congress. Office of Technology Assessment (OTA). 1982. Computerized Criminal History Systems. Washington D.C.: US Government Printing Office.

351. United States Congress. Office of Technology Assessment (OTA). 1986. Federal Government Information Technology: Electronic Record Systems and Individual Privacy. Washington, DC: Government Printing Office, 1986.

352. United States Department of Health, Education, and Welfare (HEW). 1973. Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, D.C.: HEW, 1973.

353. United States Privacy Protection Study Commission (PPSC). 1977. Personal Privacy in an Information Society. Washington, D.C.: Government Printing Office, 1977.

354. Urban and Regional Information Systems Association. 1993. *Marketing Government Geographic Information: Issues and Guidelines.* URISA. Washington D.C.

355. Varney, C. 1996. Consumer Privacy in the Information Age: A View from United States FTC. *Privacy Laws and Business* 36: 2-7.

356. Wacks, Raymond. 1989. *Personal Information, Privacy and the Law*. Oxford: Clarendon Press, 1989.

357. Warren, Samuel and Louis Brandeis. 1890. "The Right to Privacy," Harvard Law Review 4 (1890): 193-220.

358. Westin, Alan F. 1967. Privacy and Freedom. New York: Atheneum, 1967.

359. Westin, Alan F. 1977. *Computers, Health Records and Citizen Rights*. New York: 1977.

360. Westin, A.F. 1981. *The Dimensions of Privacy.* New York. Garland Publishing.

361. Westin, Alan F. 1991. "Managing Consumer Privacy Issues -- A Checklist," *Transnational Data And Communications Report*, July/August 1991.

362. Westin, Alan F. 1994. "Privacy and Genetic Information: A Sociopolitical Analysis," in Mark S. Frankel & Albert Teich eds. The Genetic Frontier: Ethics, Law and Policy. Washington DC: American Association for the Advancement of Science.

363. Westin, Alan F. 1996. Testimony before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services, U.S. House of Representatives, Washington D.C. June 11, 1996.

364. Whitfield, Diffie and Susan Landau, 1998. Privacy on the Line - The Politics of Wiretapping and Encryption. MIT: MIT Press, 1998.

365. Winner, Langdon. 1977. Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought. Cambridge: MIT Press, 1977.

366. Wright, Richard. 1996. "In strictest confidence?" *Canadian Banker,* November/December 1996.

367. Wright, Richard. 1997. "The complaint catchers." *Canadian Banker,* March/April 1997.

368. Worrall, L. 1990. *Geographic Information Systems: Developments and Applications.* London. Belhaven Press.

APPENDIX 1.0 DEFINITIONS

The definitions provided in the questionnaire were as follows:

Fair Information Practices:

1. Accountability: An organization is responsible for information under its control and shall designate an individual or individuals who are accountable for the organizations compliance with the following principles.

2. Identifying Purpose: The purposes for which the information is collected shall be identified by the organization at or before the information is collected.

3. Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of information, except where inappropriate.

4. Limiting Collection: The collection of information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention: Information shall not be used or disclosed for purposes other than those for which the it was collected, except with the consent of the of the individual. Information shall only be retained as long as necessary to for the fulfillment of those purposes.

6. Accuracy: Information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards: Information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of information.

9. Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of the individual's information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individuals accountable for the organization' s compliance

Geographic Information:

All information types that describe spatial and temporal relationships between objects.

Geographic Information Analysis:

Techniques in information analysis that allow users to determine the relationship between geographic information types.

Geographic Information Management:

Techniques in information management that are applied to the management of geographic information.

Geographic Information Management Framework:

A policy and/or organizational structure that is designed to address all aspects of managing geographic information through a complete information management lifecycle, including the collection, use, disclosure, security and disposition of geographic information.

Information Management Lifecycle:

A structured process that is designed to address all aspects of managing the information, including the collection, use, disclosure, security and disposition of the information.

Geographic Information System:

A GIS is a database management system that facilitates the storage, retrieval, manipulation and analysis of spatial and temporal data and its display in the form of maps, tables and figures. The information in a GIS describes entities that have a physical location and extent in some spatial region of interest, while queries involve identifying these entities based on their spatial and temporal attributes and relationships between entities. Geographic data refers to spatial data in terms of their position with respect to a known co-ordinate system, their attributes (which are unrelated to their position) and their spatial inter-relationships with one another.

APPENDIX 2.0 QUESTIONNAIRE

LETTER OF INTRODUCTION

1701 Claridge House
11027- 87 Avenue
Edmonton, Alberta
Canada, T6G 2P9
January, 1999

Addressee
-
-

Re: Questionnaire on Geographic Information Management Practices

Thank you for taking the opportunity to complete the attached questionnaire on the relationship between the applications of Geographic Information Management Practices and Fair Information Practices, within your jurisdiction.

The information drawn from the questionnaire will form the basis for the doctoral dissertation that is being undertaken within the Department of Geography at the University of Victoria. The goal of the questionnaire is three fold and is intended to:

1. Identify the conceptual models for geographic information management in the Canadian public sector.

2. Identify the parameters for geographic information analysis in the Canadian public sector.

Identify the legislative, regulatory and voluntary codes of fair information practices that are presently being used to regulate geographic information management and analysis in the Canadian public sector.

Kindly return the completed questionnaire and statement of informed consent by **15 March, 1999**. A self addressed stamped envelope is included for your convenience. Should you require any clarification regarding the completion of the attached questionnaire, I may be contacted at mvy@powersurfr.com or by telephone at (403) 433-5333. I sincerely appreciate the time and effort taken to complete this questionnaire.

Christopher Michell-Viret
E-Mail: mvy@powersurfr.com
Telephone: (403) 433-5333
Facsimile: (403) 439-3111

STATEMENT OF INFORMED CONSENT

Addressee
-
-
-
-

Re: Statement of Informed Consent

You have been asked to participate in a research study that examines the relationship between the applications of Geographic Information Management practices and Fair Information Practices in Canada. This research study is being undertaken by Christopher Michell-Viret, a doctoral graduate student under the supervision of Dr. Peter Keller (250) 721-7333, at the Department of Geography, University of Victoria, Victoria, B.C. Please contact Mr. Michell-Viret at (403)433-5333 or at mvy@powersurfr.com if you have any questions about the study.

The information drawn from the questionnaire will form the basis for Mr. Michell-Viret?s doctoral dissertation and the results of the study will be published as his dissertation and, possibly, in academic or professional journals. In addition, these results may be presented at academic or professional conferences.

The goal of this study is three fold and is intended to:

1. Identify the conceptual models for geographic information management in the Canadian public sector.

2. Identify the parameters for geographic information analysis in the Canadian public sector.

3. Identify the legislative, regulatory and voluntary codes of fair information practices that are presently being used to regulate geographic information management and analysis in the Canadian public sector.

Your participation in this study is entirely voluntary and you may withdraw from it at anytime without any penalties. Should you withdraw from the study, any data that has been collected from you will be destroyed.

If you agree to participate, you will be asked to complete a mail-out survey that will be followed up with personal interviews where further clarification or analysis of information management practices is required. It is estimated that it will take you approximately two hours to complete the questionnaire. The follow-up interview will take approximately one hour and will be conducted by telephone, within three weeks of receiving your questionnaire response.

The information that you provide to me with regard to this research project is provided on a confidential basis and confidentiality is an essential aspect of your agreement to provide such information. The confidential nature of this information will be protected to the full extent that university research may be protected under the Government of Canada Tri-Council Agreement on the Ethical Conduct for Research Involving Humans. The information will be secured in locked filing cabinets or on password protected hard-drives. Access to the information will be restricted to the members of the doctoral committee.

The information collected as part of this survey will be used solely for the purposes of this doctoral , or as described above, possibly for other publications or presentations. Your anonymity and confidentiality will be protected during the dissemination of the study results. This information will not be used to either directly or indirectly to market information management services.

In the course of the research, the researcher may uncover inconsistencies between policy and practice in public information management policy. The participant may be at risk of embarassment or investigation by the Office of the Information and/or Privacy Commissioner in the respective jurisdiction. You should be aware that under that *Freedom of Information and Protection of Privacy Act,* or through some other official process, the data you provide may be sought by another tribunal, court or person.

If a court, tribunal or other agency created by statute issues a subpoena or lawful demand for the production of such information, or a person makes a request for the production of such information under the *Freedom of Information and Protection of Privacy Act*, I will assert that:

(a) such information was provided to me in confidence,
(b) confidentiality was essential aspect of your agreement to provide such information,
(c) obtaining access to such information is an integral aspect of this research project which will contribute to knowledge and understanding of rationalizing Geographic Information Management practices with Fair Information Practices and thereby benefit the public and society, and
(d) consequently, such information is privileged from production or disclosure.

Where an objection to disclose of confidential information is made, the final decision on whether the information must, notwithstanding the objection, be disclosed is made by a court of law.

Thank you for considering my request to participate in this study. By signing the consent below, you are acknowledging that you understand the information provided above and that you have had the opportunity to have any of your questions about the study answered.

Signature	Date
Respondent's Name	
Position	
Association	Telephone Number
Address	Facsimile Number
	E-Mail Address

PLEASE RETURN THIS INFORMED CONSENT STATEMENT TO THE RESEARCHER WITH THE QUESTIONNAIRE RESPONSE BY 15 MARCH, 1999. THANK YOU.

QUESTIONNAIRE

PURPOSE

The purpose of this proposed research programme is to determine whether geographic information is managed in Canada in a manner that permits its use in geographic information analysis without compromising fair information practices.

SCOPE

The survey involves conducting a review of Canadian geographic information management practices. The survey will be comprised of a mail-out survey and personal interviews. Both components of the survey will focus on Canadian public sector geographic information management practices and the manner in which fair information practices have been incorporated into procedures for geographic information analysis.

FOCUS

The focal issues in this survey are:

1. The identification of the conceptual models for geographic information management in the Canadian public sector.

2. The identification of the parameters for geographic information analysis in the Canadian public sector.

3. The identification of the legislative, regulatory and voluntary codes of fair information practices that are presently being used to regulate geographic information management and analysis in the Canadian public sector.

STATEMENT OF DISCLOSURE

The information collected as part of this survey will be used solely for the purposes of this doctoral , or for a consistent purpose. This information will not be used to market information management services. The use of this information for any other purposes will be subject to the express prior authorization of the survey respondents.

DEFINITIONS

Fair Information Practices- As defined in Appendix 1, appended to this questionnaire.

Geographic Information- All information types that describe spatial and temporal relationships between objects.

Geographic Information Analysis- Techniques in information analysis that allow users to determine the relationship between geographic information types.

Geographic Information Management- Techniques in information management that are applied to the management of geographic information.

Geographic Information Management Framework- A policy and/or organizational structure that is designed to address all aspects of managing geographic information through a complete information management lifecycle, including the collection, use, disclosure, security and disposition of geographic information.

Information Management Lifecycle: A structured process that is designed to address all aspects of managing the information, including the collection, use, disclosure, security and disposition of the information.

1. JURISDICTIONAL SETTING

1(a) Does your jurisdiction have Freedom of Information and Protection of Privacy legislation in place? If affirmative, please specify which piece(s) apply.

1(b) Does your jurisdiction have mandatory or voluntary codes of practice that regulate the collection, use, disclosure and/or retention of geographic information? If affirmative, please provide a description of the codes of practice.

1(c) Does your jurisdiction have mandatory or voluntary codes of practice that regulate the application of techniques in geographic information analysis? If affirmative, please provide a description of the codes of practice.

1(d) Do the codes of practice, referred to questions 2 and 3, comply with fair information practices? Please qualify your response where the codes of practice partially comply with fair information practices.

2. MODES OF GEOGRAPHIC INFORMATION MANAGEMENT

2(a) Has a Geographic Information Management Framework (GIMF) been established for the management of geographic information, within your jurisdiction? If affirmative, please provide details of the conceptual model(s) for geographic information management and the organizational structure of the GIMF.

2(b) Does the GIMF include the management of geographic information through the full information management lifecyle? Please specify which stages are captured in the GIMF information management lifecycle.

2(c) Please specify whether there is a legislative, regulatory or voluntary authority for establishing and/or maintaining the GIMF?

2(d) Do the GIMF extend to both the public and private sectors? Please provide details of the extent of application of the GIMF.

3. MODES OF GEOGRAPHIC INFORMATION ANALYSIS

3(a) Has an authority been established, within your jurisdiction, to regulate the application of techniques in geographic information analysis? If affirmative, please provide details of the structure of the authority.

3(b) Does your jurisdiction have mandatory or voluntary codes of practice that regulate the application of techniques in geographic information analysis? If affirmative, please provide a description of the codes of practice.

3(c) Does the authority and code of practice, referred to questions 1 and 2, comply with fair information practices? Please qualify your response where the codes of practice partially comply with fair information practices.

3(d) Have a set of parameters been established for conducting geographic information analysis? If affirmative, please specify the basis upon which these parameters are based.

3(e) Does the authority for the regulation of the application of techniques in geographic information analysis and the respective code of practice extend to both the public and private sectors? Please provide details of the extent of application of the authority and code of practice.

4. APPLICATION OF FAIR INFORMATION PRACTICES

4(a) Is the management of geographic information based on the application of fair information practices? If affirmative, please specify whether compliance with fair

information practices is based on legislative, regulatory and/or voluntary requirements.

4(b) Is the management of geographic information analysis based on the application of fair information practices? If affirmative, please specify whether compliance with fair information practices is based on legislative, regulatory and/or voluntary requirements.

4(c) Does the authority for the application of fair information practices extend to both the public and private sectors? Please provide details of the extent of application of the application of fair information practices.

4(d) Do the codes of practice apply equally to personal and nonpersonal information? If not, please indicate how codes of practices differ between the management of personal and nonpersonal information.

4(e) Do you anticipate that the Government of Canada Bill C-54, Personal Information Protection and Electronic Documents Act, or, the European Union Directive on Personal Data Protection (95/46/EC) will require significant changes to your codes of practice? I f affirmative, please indicate the nature and extent of changes that are anticipated in your codes of practice with respect to each of these pieces of legislation. (See Appendices 3 and 4)

5. IMPACT ON GEOGRAPHIC INFORMATION MANAGEMENT AND ANALYSIS

5(a) Has the application of fair information practices affected the effectiveness of techniques in geographic information management? If affirmative, please provide examples of the affects.

5(b) Has the application of fair information practices affected the efficiency of techniques in geographic information management? If affirmative, please provide examples of the affects.

5(c) Has the application of fair information practices affected the effectiveness of techniques in geographic information analysis? If affirmative, please provide examples of the affects.

5(d) Has the application of fair information practices affected the efficiency of techniques in geographic information analysis? If affirmative, please provide examples of the affects.

5(e) Do the affects of the effectiveness and efficiency of the application of fair information management practices on geographic information management differ

between the public and private sectors? If trends in the public and private sectors are discernable, please provide examples of the differences in trends.

5(f) Do the affects of the effectiveness and efficiency of the application of fair information management practices on geographic information analysis differ between the public and private sectors? If trends in the public and private sectors are discernable, please provide examples of the differences in trends.

6. INNOVATIONS IN GEOGRAPHIC INFORMATION MANAGEMENT

6(a) Has the application of fair information practices resulted in innovation(s) in techniques in geographic information management? If affirmative, please specify the nature of the innovation(s) in the technique in geographic information management.

6(b) For each innovation in geographic information management, please indicate whether more diverse forms of geographic information analysis were possible without compromising fair information practices. If affirmative, please provide examples of the increased diversity of forms of geographic information analysis.

6(c) For each innovation in geographic information management, please indicate whether more intensive forms of geographic information analysis were possible without compromising fair information practices. If affirmative, please provide examples of the increased diversity of forms of geographic information analysis.

6(d) Are there discernable differences, between the public and private sectors, in the trends in innovations in geographic information management? If trends in the public and private sectors are discernable, please provide examples of the differences in trends in geographic information management.

7. INNOVATIONS IN GEOGRAPHIC INFORMATION ANALYSIS

7(a) Has the application of fair information practices resulted in innovation(s) in techniques in geographic information analysis? If affirmative, please specify the nature of the innovation(s) in the technique in geographic information analysis.

7(b) For each innovation in geographic information analysis, please indicate whether more diverse forms of geographic information analysis were possible without compromising fair information practices. If affirmative, please provide examples of the increased diversity of forms of geographic information analysis.

7(c) For each innovation in geographic information analysis, please indicate whether more intensive forms of geographic information analysis were possible without

compromising fair information practices. If affirmative, please provide examples of the increased diversity of forms of geographic information analysis.

7(d) Are there discernable differences, between the public and private sectors, in the trends in innovations in geographic information analysis? If trends in the public and private sectors are discernable, please provide examples of the differences in trends in geographic information analysis.

8. CONTRAVENTION OF FAIR INFORMATION PRACTICES

8(a) Please identify areas where operational requirements in geographic information management involve contravening fair information practices? If affirmative, please provide state the operational requirements in geographic information management along with the examples of the geographic information practices that contravene fair information practices.

8(b) Please identify areas where operational requirements in geographic information analysis involve contravening fair information practices? If affirmative, please provide state the operational requirements in geographic information analysis along with the examples of the geographic information practices that contravene fair information practices.

8(c) Are there discernable differences, between the public and private sectors, in the trends in contravention of fair information management practices that arise from operational requirements in geographic information management? If trends in the public and private sectors are discernable, please provide examples of the differences in trends in the contravention of fair information management practices that arise from operational requirements in geographic information management.

8(d) Are there discernable differences, between the public and private sectors, in the trends in contravention of fair information management practices that arise from operational requirements in geographic information analysis? If trends in the public and private sectors are discernable, please provide examples of the differences in trends in the contravention of fair information management practices that arise from operational requirements in geographic information analysis.

PLEASE NOTE:

The mail-out survey will be followed up with personal interviews where further clarification or analysis of information management practices is required. If you have any queries, concerns or require clarification in the course of completing this questionnaire, please contact the researcher:

Christopher Michell-Viret
Doctoral Candidate
University of Victoria
Victoria, British Columbia
Canada

Tel: (403) 433-5333
Fax: (403) 439-3111
E-Mail: mvy@powersurfr.com

THANK YOU.

PLEASE RETURN THIS INFORMED CONSENT STATEMENT TO THE RESEARCHER WITH THE QUESTIONNAIRE RESPONSE BY 15 MARCH, 1999. THANK YOU.

APPENDIX 1

Summary of Fair Information Practices

1. **Accountability**
   An organization is responsible for information under its control and shall designate an individual or individuals who are accountable for the organizations compliance with the following principles.
2. **Identifying Purpose**
   The purposes for which the information is collected shall be identified by the organization at or before the information is collected.
3. **Consent**
   The knowledge and consent of the individual are required for the collection, use, or disclosure of information, except where inappropriate.
4. **Limiting Collection**
   The collection of information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention**
   Information shall not be used or disclosed for purposes other than those for which the it was collected, except with the consent of the of the individual. Information shall only be retained as long as necessary to for the fulfillment of those purposes.
6. **Accuracy**
   Information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards**
   Information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openess**
   An organization shall make readily available to individuals specific information about its policies and practices relating to the management of information.
9. **Individual Access**
   Upon request, an individual shall be informed of the existence, use, and disclosure of the individual's information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance**
    An individual shall be able to address a challenge concerning compliance with the above principles to the designated individuals accountable for the organization's compliance

VITA

Surname: Michell-Viret **Given Names: Christopher St.Elmo**

Place of Birth: Lusaka, Zambia

Educational Institutions Attended:

University of Alberta	**1977 to 1989**
University of Victoria	**1993 to 2002**

Degrees Awarded:

B.Sc. (General)	**University of Alberta**	**1983**
B.Sc. (Geography)	**University of Alberta**	**1984**
M.Sc. (Geography)	**University of Alberta**	**1989**
M.A. (Geography)	**University of Victoria**	**2002**

Publications:

Michell-Viret, Christopher. 2001 **"Virtual Privacy: Tracking Electronic Footprints in Cyberspace",** Proceedings of GIS'2001, the 15th Annual Symposium on Geographic Information Systems.

Michell-Viret, Christopher. 1999 **"Private Lives, Public Partnership: Advances in Private Sector Privacy Protection",** Proceedings of the Urban and Regional Information Systems Association.

Michell-Viret, Christopher. 1998 **"Redefining John Doe: Privacy in the Global Information Economy",** Proceedings of GIS'98, the 12th Annual Symposium on Geographic Information Systems.

Michell-Viret, Christopher. 1998 **"Planning Globally, Acting Privately: Privacy in the Global Information Economy",** Proceedings of the Urban and Regional Information Systems Association.

Michell-Viret, Christopher. 1997 **"Technological Slave or Informational Serf: Cultural Implications of operating on the Information Highway",** Proceedings of the Urban and Regional Information Systems Association.

Michell-Viret, Christopher. 1995 **"GIS, Integrated Information Resources Management and Data Access: Challenges in Information Ethics",** Proceedings of GIS'95, the Ninth Annual Symposium on Geographic Information Systems.

.../2

Michell-Viret, Christopher. 1993 **"Data Access: A Keystone to GIS"**, Proceedings of GIS'93, the Seventh Annual Symposium on GIS in Forestry, Environmental and Natural Resources Management.

Michell-Viret, Christopher., Giffen, Barry., Guthrie, James,. Jacob, Ron., MacKay, Laurel. 1992. **"Information Systems Inputs to Programs, Applications of IS/GIS in Government"**, Proceedings of the Urban and Regional Information Systems Association.

UNIVERSITY OF VICTORIA PARTIAL COPYRIGHT LICENCE

Title of Thesis:

The Rationalization of Geographic Information Management Practices with Fair Information Management Practices.

Author 

Christopher St.E. Michell-Viret
20 June, 2002