INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI[®]

**CARLETON UNIVERSITY
SCHOOL OF BUSINESS**

**INFORMATION PRIVACY:
An Exploratory Survey of Concerns
about Organisational Practices**

THESIS

SUBMITTED BY:

Roozbeh Ghiami-Mirhosaini,
B.Sc. (Honours) in Biology and Biotechnology

**In partial fulfilment of the requirements for the
degree of Master of Management Studies**

January 12, 2000

© Copyright
2000, Roozbeh Ghiami-Mirhosaini

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-48484-X

Canada

The undersigned recommend to
the faculty of graduate studies
acceptance of the thesis

**INFORMATION PRIVACY:
An Exploratory Survey of Concerns
about Organisational Practices**

submitted by
Roozbeh Ghiami-Mirhosaini B.Sc. (Honours) in Biology and Biotechnology
In partial fulfillment of the requirements for the degree of
Master of Management Studies

Thesis Co-Supervisor

Thesis Co-Supervisor

Director, School of Business

Carleton University
January, 2000

Abstract

For the past two decades there have been increasing concerns about the loss of control over personal information. Insufficiency of privacy laws, rapid advancements in information technology, and "commodification" of personal information have contributed to increasing concerns about information privacy. Despite increasing concerns, the information privacy research is very limited. No theoretical models exists and only a handful of empirical research is available.

This exploratory study is based on past research in the area of information privacy to examine some variables that are believed to affect the level of concerns of individuals about information privacy practices of organizations. A questionnaire completed by randomly selected students and faculty members of Carleton University was used to determine whether they had different levels of concerns when they were prompted to think about different types of information, organizations, and information storage technologies. The questionnaire was also used to investigate the presence of a hierarchy of concern dimensions. Results show that level of concern about information privacy practices of organisations is context sensitive based on information type, organisation type, and technology type. Results also show that a hierarchy of concern dimensions is present; however, the hierarchy of concern dimensions is context sensitive based on the type of information or type of organisation about which the respondents were prompted to think.

Acknowledgements

I thank God for giving me the courage to pursue my dreams and the strength of mind to withstand life's challenges. I am thankful to my wife Maryam for her continued support and understanding through this process and to my son Shervin for uplifting my spirit. I am also thankful to my parents Giti-ara and Hossein for believing in me and supporting me throughout my life.

Two people were integral to the completion of this thesis whose support I would like to acknowledge. I am very grateful to Dr. Uma Kumar for her kind advice and encouragement. She was always available when I needed assistance. I am also sincerely grateful to Dr. Roland Thomas for setting a high standard of excellence in statistical analyses and his continued support throughout this study.

I also thank Professors George Haines and Peeter Kruus for their valuable feedback and assistance with this thesis. To those faculty members and students who participated in my survey, I am greatly thankful. I could not have completed this thesis without their cooperation. And last but certainly not least, I thank Jean Blair who has been extremely helpful in providing guidance and assistance in all administrative matters.

Table of Contents

	Page
Title	i
Acceptance	ii
Abstract	iii
Acknowledgements	iv
Table of Contents	v
List of Tablets	viii
List of Figures	ix
1.0 Introduction	1
2.0 Literature Review	9
2.1 Information Privacy Concerns	9
2.1.1 Dimensions of Information Privacy Concerns	12
2.2 Causes for Information Privacy Concerns	14
2.2.1 Issues of Concern	14
2.2.2 Public Opinion Surveys	17
2.2.3 Available Legal Protection for Information Privacy	18
2.3 The Context Sensitivity of Information Privacy Concerns	21
2.3.1 Information Type	22
A) Performance Information	26
B) Personality Information	26
2.3.2 Organisation Type	27
A) Government Organisations	29
B) For-profit Organisations	31
C) Non-profit Organisations	31
2.3.3 Technology Type	33
A) Databases	36
B) Smart Cards	36
C) Manual File Storage	37
2.3.4 Other Variables Affecting Concerns	38
A) Previous Personal Experiences & Media Acquired Knowledge	38
B) Individual Personality Factors	39
C) Demographic Variables	40
2.4 Hierarchy for the Dimensions Information Privacy Concerns	40
3.0 Research Framework	42

4.0 Research Questions and Hypotheses	44
4.1 Group Differences	44
4.2 Sensitivity of Record Types	44
4.3 Information-handling Practices of Organisations	45
4.4 Safety of Information under Different Storage Technologies	46
4.5 Hierarchy of Concern Dimensions	47
 5.0 Research Methodology	 48
5.1 Research Design	48
5.2 Sampling Design	50
5.2.1 Sampling of the Faculty Members (P_1)	51
5.2.2 Sampling of the Undergraduate Students (P_2)	54
5.3 Data Collection	56
5.3.1 The Research Instrument	57
A) The Cover Letter	57
B) The Anonymity Agreement	57
C) The Questionnaire	57
 6.0 Data Analysis	 58
 7.0 Research Results	 61
7.1 Descriptive Statistics	61
7.2 Group Differences	63
7.2.1 MANOVAs	63
7.2.2 ANOVAs	67
7.3 Multiple Comparisons	70
7.3.1 Mean Concerns	70
7.3.2 Pair-wise t-tests	72
 8.0 Conclusions	 84
8.1 Conclusions Related to Group Differences	84
8.2 Conclusions Related to Information Types	85
8.3 Conclusions Related to Organisation Types	87
8.4 Conclusions Related to Storage Technology Types	89
8.5 Conclusions about Concern Dimensions	90
 9.0 Research Benefits	 91

10.0 Research Limitations	92
11.0 Bibliography	93
12.0 Appendices	102
12.1 Appendix A: Performance Information	102
i) Financial Records	102
ii) Transactional Records	102
iii) Police Records	103
iv) Library Records	104
v) Medical Records	105
vi) Drug Testing Records	110
12.2 Appendix B: Personality Information	112
i) Integrity and polygraph testing Records	112
ii) Ability Testing Records	113
iii) Genetic Information	114
12.3 Appendix C: Sample Cover Letter	123
12.4 Appendix D: Smith's instrument & instrument validation model	124
12.4 Appendix E: The Research Questionnaire	126

List of Tables

Table	Title	Page
5.1-I	Study variables & corresponding hypotheses, instruments and research questions	49
5.2-II	Full-time and regular part-time teaching staff (1997-1998)	52
5.2-II	Theoretical and actual sample sizes for P_1	53
5.2-III	Carleton University's part-time and full-time enrolment by level	54
5.2-IV	Theoretical and actual sample sizes for the undergraduate group	56
7.1-I	Descriptive statistics for information types	61
7.1-II	Descriptive statistics for organisation types	62
7.1-III	Descriptive statistics for storage technology types	62
7.2-I	MANOVA for group differences based on information types	63
7.2-II	MANOVA for group differences based on organisation types	63
7.2-III	Post-Hoc estimation of power and effect size (information types)	65
7.2-III	Post Hoc estimation and effect size (organisation types)	66
7.2-IV	ANOVA for group differences - information types	67
7.2-V	ANOVA for group differences - organisation types	68
7.2-VI	ANOVA for group differences on technology type storage safety	69
7.3-I	Mean Concerns (groups 1+2) in a descending order of magnitude (Information types)	70
7.3-II	Mean Concerns (groups 1+2) in a descending order of magnitude (organisation types)	71
7.3-III	Mean perception of safety (groups 1+2) in a descending order of magnitude	71
7.3-IV	Mean Concerns ordered in a descending order of magnitude (dimensions of concern)	72
7.3-V	The result of pair-wise t-tests for information	73
7.3-VI	The result of pair-wise t-tests for organisation types	77
7.3-VII	Results of pair-wise t-tests for perception of safety of storage technologies	80
7.3-VIII	The results of pair-wise t-tests for the four dimensions of privacy	81

List of Figures

Figure	Title	Page
I	Proposed Research Framework	42
II	Sampling Design of Study	51
III	Ranking concern levels about collection of different record types	74
IV	Ranking concern levels about unauthorised secondary use of different record types	74
V	Ranking concern levels about errors in different record types	75
VI	Ranking concern levels about improper access to different record types	75
VII	Ranking concern levels about various organisations' collection of personal information. The graph is not drawn to scale.	77
VIII	Ranking concern levels about various organisations' unauthorised secondary use of "personal information."	78
IX	Ranking concern levels about various errors in personal information that organisations have in their possession.	78
X	Ranking concern levels about improper accesses to "personal information" in various organisations.	79
XI	Ranking individual's perception of safety of personal information when different storage technologies are used to store them.	80
XII	Ranking of dimensions of concerns with respect to different information types. The graph is not drawn to scale.	82
XIII	Ranking of dimensions of concern with respect to organisation types.	82

1.0 Introduction

In Canada and the United States there are increasing concerns about the issue of information privacy – “the ability of the individual to personally control information about one’s self” (Equifax, 1995, 1991, and 1990; Stone et al., 1983). This trend stems largely from the unprecedented technological advances of the past two decades (Smith et al., 1996; Regan, 1995; Cavoukian and Tapscott, 1995; Smith, 1994).

Advances in the computerisation of records, data management systems, and network communications have enabled organisations¹ to accumulate, retrieve, analyse, manipulate, and transmit large amounts of personal information. Furthermore, data intensive techniques such as *profiling* (O’conner, 1995) and *data mining* (Frawley et al., 1992) have created “recombinant data” (Schoechle, 1995), which has made personal information usable as a commodity (Grupe, 1995; Kling, 1994; Kling et al., 1992, 1991; Luke et al., 1985). It has been suggested that it is the “commodification” (Larson, 1992) of this “economic good” (Lipinski, 1996) that threatens the information privacy of individuals and leads to increased levels of public concern (Smith, 1994).

The speed of technological advances has created much ambiguity for both the law and policy makers. Rapidly changing technologies have not permitted a timely adjustment of societal norms, nor have they allowed time for the enactment of appropriate laws needed to clarify the ambiguities surrounding information privacy issues (Cavoukian and Tapscott, 1995; Smith, 1994; Straub, 1990).

¹ Unless stated otherwise, throughout this thesis, the word “organisation” would include government agencies, non-governmental non-profit corporations, and privately or publicly owned for-profit corporations.

The existing privacy laws and conceptual frameworks do not address current privacy issues, and fail to protect personal privacy. These laws are outdated because they were introduced long before the recent and ongoing technological progression (Smith, 1994). Current privacy laws only regulate the public sector², leaving the private sector practically unregulated (The Privacy Commissioner³, 1994). At the same time, as the distinction between the private and the public sectors is becoming less clear, privacy protection in the public sector is eroding (The Privacy Commissioner, 1994). Furthermore, laws are inconsistent from one jurisdiction to another and lack concurrence with the recently emerged international privacy standards (Bennett, 1996). Consequently, the frequent "border-crossing" of information subjects it to legal standards that are either unenforceable or enforceable in a logically inconsistent manner (Bennett, 1996; Cavoukian and Tapscott, 1995; Fox, 1993).

Without a remedy for this situation, the exponential progression of technology will likely make the existing legal frameworks for the protection of individual privacy irrelevant. Consequently, the public will be at the mercy of the private sector and market forces, which would draw the boundaries of individual privacy according to their own requirements.

² With the exception of Quebec whose bill 68, enacted in 1993, protects personal information in the private sector. This bill covers entities that engage in "organized economic activity" in the province of Quebec, and applies to "all pieces of personal information collected, held, used, or distributed by another person" (Bennett, 1996).

³ A special ombudsman established under the Canadian Human Rights Act of 1977 appointed by and accountable to parliament. The office of privacy commissioner monitors the federal government's operations over personal information.

Currently, in the private sector, which operates practically free of legislated information privacy rules, it is the moral concepts of right and wrong of executives that guides the handling of personal information (Phillips, 1995; Smith, 1993 and 1994). The executives rarely adopt a “proactive stance in creating information privacy policies” and only take reactive measures in response to external threats (Smith, 1993, 1994). They establish the information privacy policies of their organisations by what has been called the “policy by the least steps” (Krier et al., 1977). In this path, their organisations may not only contribute to the invasion of privacy of individuals, but may also face risks. These risks may range from a public opinion backlash, lawsuits, a stricter regulatory environment, and profit loss to employee anxiety (Smith, 1994; Cespedes et al., 1993; Straub et al., 1990).

Many organisations have become aware of the public's increasing concerns about this issue (Phillips, 1995). They have become cognisant of the importance of minimising the risks associated with the haphazard handling of personal information (Smith, 1994). Among these organisations, some have attempted to draft their own voluntary privacy codes (Phillips, 1995) to proactively manage the information privacy issues (Smith, 1994). Self-regulation, however, is an inadequate measure for providing universal protection and enforceable uniform standards (Bennett, 1996; Cavoukian and Tapscott, 1995; Phillips, 1995). Organisations that self-regulate, such as the credit card companies, can provide no guarantees for systematic organisational compliance with these privacy codes and the promptness of response to consumer complaints (Cavoukian and Tapscott, 1995; Smith, 1994). In addition, voluntary codes suffer from inadequate code coverage,

sanctions, and consumer awareness of the issues of code provisions (Cavoukian and Tapscott, 1995; Smith, 1994).

In a 1995 report to the Canadian government, the Information Highway Advisory Council (IHAC) recognised the “need for a national standard” and recommended that “the government must pursue development of effective oversight and enforcement mechanisms” (IHAC, 1995; Phillips, 1995). Although this task is achievable by establishing new bureaucratic privacy protection institutions, there is no reason to believe that, in the long run, this alternative would be more successful than self-regulation in keeping up with the ever-changing technologies (Schoechle, 1995). The Canadian government has since behaved in a contradictory and confusing manner with respect to privacy issues. On the one hand, “Justice Minister Allan Rock has pledged that, by the year 2000, there will be a federal law to provide effective, enforceable protection of privacy rights in the private sector” (Privacy Commissioner, 1997). On the other hand, two departments of government, HDRC and Revenue Canada are participating in a legal challenge to employ *data matching* (Privacy Commissioner, 1997). This practice is offensive to the most basic principles of any privacy law. It “violates the search and seizure provisions of the Canadian Charter of Rights and Freedoms (by) ignoring the presumptions of innocence” (Privacy Commissioner, 1997).

Ideally, to regulate Canada’s privacy arena, there should be a mixture of a regulatory action and a voluntary action. The regulatory action could be in form of a minimal privacy law, overseen by the privacy commissioner and the voluntary action could be in form of sector-specific codes for each industrial sector (Bennett, 1996; Cavoukian and Tapscott, 1995). Alternatively, the use of codes similar to the ISO 9000

standards as a prototype for privacy strategy may be appropriate (Schoechle, 1995; Smith, 1994). ISO 9000 series are internationally recognised quality management and assurance standards, developed by the "International Organisation for Standardisation (ISO)." They describe the minimum requirements for ensuring organisations' product and process quality. An example of this alternative is the CSA Model Code (Bennett, 1996, Phillips, 1995), which has found the blessing of the Federal Information Highway Advisory Council.⁴ *CSA Model Code* is a recently developed model by the Canadian Standards association for the protection of personal information. This association passed the code in September 1995, and the Standards Council of Canada subsequently approved and published it in March of 1996. The CSA model is different from voluntary codes in that it can encourage a greater consistency of policy, greater consumer privacy awareness, and a higher level of responsibility for the collection, storage, and disclosure of personal data. Moreover, it can be a better yardstick for the measurement of the adoption of data protection (Bennett, 1996).

Regardless of the approach, a better understanding of the variables that affect the concerns of individuals, about the information privacy practices of various organisations, is essential for better legal or policy decisions. Unfortunately, the current research in the area of information privacy is very limited. There are no theoretical models and only a handful of empirical studies is available, which examine the dimensions of privacy concerns and the variables that affect them.

⁴ IHAC in its 1995 report to the Canadian government recommended to "creating a level playing field for the protection of personal information on the Information highway by developing and implementing a flexible legislative framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA Model Code, while allowing the flexibility to determine how they will refine their own codes" (IHAC 1995, pg. 141).

A great deal of knowledge about information privacy concerns, however, is available because of the ongoing public opinion polls⁵. The opinion polls, which are informative about the changes in the public's attitude toward the issue of privacy, are now reporting record levels of concern about individual privacy issues (Smith et al., 1996; Regan, 1995). However, the polls reflect only general concerns about privacy, without fully exploring the dimensions of this construct or a clear definition of privacy (Regan, 1995). Opinion polls suffer from a number of shortcomings. One difficulty is obtaining a random, non-biased sample. This problem leads to an underestimation or overestimation of the actual levels of concern about information privacy (Regan, 1995; Gandy, 1993). Reluctance of the "overly concerned" to participate in the poll or their unwillingness to provide accurate and reliable information would lead to an underestimation of concerns, whereas, only including the opinions of the "overly concerned" would give an overestimation of the levels of concern (Regan, 1995). Furthermore, opinion polls by nature tend to lead respondents to render uninformed responses either to please or deceive pollsters, or to merely have an opinion when a question is asked. The information privacy polls do not really pursue what it is about privacy that concerns people. They provide no insight regarding the nature of people's concerns. Each person could be thinking of a different aspect of the information privacy when asked about privacy concerns. Another concern with some public opinion polls is that they often serve a "special-interest-group" (Crespi, 1989), which pursue interests of a particular organisation or group of organisations. The results of such polls are released only if they support the position of the sponsoring organisation (Regan, 1995), another

⁵ An example is Louis Harris and Associates who have been conducting surveys on attitudes towards privacy since the 1970's.

process that leads to biased public information over the long-term. Finally, while public opinion polls may provide valid data regarding levels of public concerns about information privacy, their measurement accuracy is unclear (Regan, 1995).

The study presented here was an exploratory investigation of some of the variables, which were thought to affect levels of concern of individuals about the information privacy practices of organisations. It was inspired by investigations proposing theoretical relationships that included levels of privacy concerns as a construct in their theoretical frameworks (Stone and Stone, 1990). It was also stimulated by suggestions about the potential context sensitivity of the privacy concerns of individuals. This context sensitivity, which several authors have suggested to be based on either the type of personal information being handled (Tolchinsky, 1981; Fusilier and Hoyer, 1980; Ganster, 1979; Rosenbaum, 1973), or the type of organisation handling the personal information (Stone et al., 1983) became the main objective of this research.

Subsequent to earlier research, the present study attempted to explore whether individuals demonstrated different levels of reservation when considering: (1) the type of personal information being handled by organisations, or (2) the class of organisations handling their personal information. In addition, this study aimed to investigate whether the form of stimulus – *information type*, or *organisation type* – was instrumental in provoking a specific dimension of privacy concerns, i.e., collection, improper access, errors, or unauthorised secondary use (Smith et al., 1996). For example, one particular sub-goal was to investigate whether the actual collection of genetic information raised more information privacy concerns than did improper access to this type of information.

The study also investigated whether the hierarchy of the levels of concern was consistent with an earlier finding, which found that unauthorised secondary use of information generated the highest levels of concern in Canada.

Following a review of the literature on the topic, and the presentation of the research model and research hypotheses, subsequent chapters will present the findings of this research in detail.

2.0 Literature Review

This Chapter, which consists of five sections, reviews the available literature on the issue at hand. The first section identifies the various distinct areas of privacy concerns and directs the reader's attention to the issue of information privacy. In this section, the issue of information privacy concerns is defined and described in detail. Section two examines the causes for concern about information privacy practices and the public's concern about privacy, and provides a review of the existing privacy protection. Section three gives an overview of the dimensions of privacy concerns and presents evidence for the presumed presence of a hierarchy of dimensions. Section four will explore evidence suggesting that information privacy concerns of individuals are context sensitive. This context sensitivity has been proposed to be a function of information type and organisation type. Finally, the last section describes other factors that have been hypothesised to affect the levels of the information privacy concerns of individuals. The literature will be used as the basis for the proposed research framework.

2.1 Information Privacy Concerns

Regan (1995) identifies the three major areas of privacy concerns⁶ as:

- *Communication Privacy* – concerns about illegitimate interception of individual communications,
- *Psychological Privacy* – concerns about probing of individual thoughts and attitudes,
- *Information Privacy* - concerns about the use of personal information by information-intensive industries.

⁶ Regan derives these categories of concerns from Alan Westin's classification in his seminal work, *Privacy and Freedom*. In his work Westin talks about *data surveillance* (information collection and processing), *physical surveillance* (listening and watching), and *psychological surveillance* (probing the mind). 9

This thesis will examine the latter class of concerns, namely concerns about information privacy, or more specifically the level of concern of individuals about the information privacy practices of organisations.

A variety of analogues are available to define information privacy. In short, information privacy is the “respect of social order by which persons control access to information about themselves” (Charles Fried quoted in Regan, 1995). It is “the ability of individuals to personally control information about themselves” (Stone et al., 1983). Information about one’s self or “personal information” means any information about a person that is identifiable as that person’s (Cavoukian and Tapscott, 1995). Personal information, in other words, is a person’s name or any other specific identifier that can positively identify that person⁷.

As an extension of “privacy,” or “the right to be let alone” information privacy shares many of the attributes of the term “privacy.” It is a comprehensive, complex, and subjective issue, which is difficult to conceptualise. The complexity of this issue results, to some extent, from the variety of its perceived definitions, which depend on the type of information that one regards as private or worthy of protection. Hence, there may be as many unique ways to describe information privacy, as there are individuals.

⁷ This includes transaction records, police records, and genetic testing records, vital statistics, educational records, bank & loans records, medical records, credit card payment records, income & income tax records, employment or welfare payment records, immigration records, public records, organisational memberships, extracurricular activities and hobbies, military service records, motor vehicle registration and ownership, and accident records.

For example, privacy interest of some individuals may be focused on the collection and use of their medical records and the extent to which these are available to unintended parties. To others, information privacy may imply the ability to control the dissemination of information about a past record of bankruptcy, and the security features necessary to ensure that such information be kept from unauthorised persons. The complexity of information privacy may also result from disagreements about the ownership of the data (Smith, 1993), and from people's mix of views on the information practices of organisations, and on their tolerance thresholds⁸ (Westin, 1967).

Despite its long history, dating back to the 1960s, information privacy is a new field of research. Before the 1980s, the number of privacy-related publications approximated 2,000 articles (Stone and Stone, 1979). Following the relatively quiet 1980s, the 1990s witnessed increased interest by legislators and media because of the impacts of information technology on information privacy (Smith, 1993). The majority of recent publications emphasise the threats to privacy brought about by new information technologies, the lack of legal protection, and the need for the protection of personal privacy. Many investigators emphasise the importance of investigating the information privacy practices of organisations, and the perceptions of individuals about these practices and the societal responses. However, the number of empirical studies in this field remains surprisingly low. The following subsection will look at recent empirical efforts that explore the dimensions of information privacy concerns.

⁸ Westin (1967) suggests that there are three groups of people with respect to information privacy tolerance. Fundamentalists, who constitute 25% of the population, are generally concerned about control over their personal privacy. The second group, "the unconcerned consumers," who constitute about 18% of the population, are generally willing to forgo their privacy controls in return for better services. Finally, the pragmatists, the remaining 57% of the population, generally weigh the benefits of renouncing their privacy against the benefits gained from better consumer services.

2.1.1 Dimensions of Information Privacy Concerns

A number of investigators have examined various dimensions underlying information privacy concerns. However, the lack of a common unifying framework in describing the primary dimensions of concern has hindered the task of relating these dimensions.

During the early 1990s, Goodwin (1991) divided privacy concerns into two dimensions: (1) control over the environment, and (2) control over the disclosure of information. In a more recent study, Smith, Milberg, and Burke (1996) expanded Goodwin's model to reveal the four central dimensions of concern about the information privacy practices of organisations. The four dimensions introduced by these researchers, however, did not include individual control over his or her personal information or environment. Their work involved screening of a preliminary set of 72 items, in order to yield dimensions that actually measured information privacy concerns (Smith et al., 1996). They not only provided a framework describing the primary dimensions of the construct, but also developed and validated an instrument to measure Individual levels of concern. The four central dimensions of information privacy concerns include:

- *Collection of personal information*: “concerns that extensive amounts of personally identifiable data are being collected and stored in databases” (Stone and Stone, 1990; Linowes, 1989; Lauden, 1986, Stone et al., 1983; Miller, 1982; PPSC, 1977; HEW, 1973; and Westin and Baker, 1972);
- *Unauthorised Secondary Use of personal information*: “concerns that information is collected from individuals for one purpose, but is used for another secondary purpose,

without authorisation from the individuals” (Linowes, 1989; Stone et al., 1983; PPSC, 1977; HEW, 1973);

- *Errors in personal information*: “concerns that protections against deliberate and accidental errors in personal data are inadequate” (Date, 1986; Lauden, 1986; Miller, 1982; PPSC, 1977; HEW, 1973; Westin and Baker, 1972); and,
- *Improper Access to personal information*: “concerns that data about individuals are readily available to people not properly authorised to view or work with this data” (Linowes, 1989; Date, 1986; PPSC, 1977).

Smith and his colleagues also noted two tangential dimensions, *reduced judgement*, and *combining data*. However, they indicated that the former dimension has rarely been referred to as privacy concern per se, and the latter has usually been included with either the *Collection* or the *Unauthorised Secondary Use* of personal information.

The above dimensions represent the main concerns of individuals about of information privacy. In other words, they are the main essence of various types of concerns about information privacy. The following section will examine some of these dimensions, as well as the causes of concern, public opinion surveys and the current state of privacy protection.

2.2 Causes of Information Privacy Concerns

2.2.1 Issues of Concern

The first official warning about the issue of information privacy in the computer age came from Bernard Benson in 1961. In a speech at the annual convention of the Society of Technical Writers and Publishers, Benson, who was at the time the president of the computer-manufacturing company of California, voiced his concerns about privacy (Westin, 1967). Particularly concerned about the loss of individual privacy and liberty, Benson warned participants about the dangers of the data banks of the future. He cautioned that these data banks could contain everyone's "Federal Bureau of Investigation (FBI) records, records of childhood diseases, parents' attitudes, school records, employment records, tax records, contributions to charities, and the records of charge accounts and credit cards" (Quoted in Westin, 1967).

The key concern at that time was the creation of "womb to tomb" personal files for all citizens by governments (Westin and Miller, 1971). Since then, government organisations have collected, stored, and exchanged large amounts of personal information. More recently, however, privacy experts point to the private sector as the major collector and user of personal information on citizens (Willis, 1993).

The accumulation of personal information in organisational databases has gradually led to the public's increasing concern about the issue of information privacy. These concerns, however, are not because of the mere collection of personal information, but because of the ease of unauthorised access to personal information, its unauthorised use and misuse, and the consequences of its use. When people disclose personal

information, they only authorise the use of information for the originally intended purpose, and not for any other applications (Smith, 1993). For example, no one would expect an organisation to use the medical records of employment applicants to make hiring decisions. Similarly, many people resent it when organisations use data collected on their shopping habits to target them as prospects for other product sales. The possibility of unauthorised access to personal information could also be problematic. Those who have experienced a bankruptcy, or have suffered depression or mental problems, but have since recovered from their misfortune are particularly sensitive to publication of the details of affliction (Cavoukian and Tapscott, 1995). The result of leaks of such personal information into the public domain can be quite devastating, leading possibly to stigmatisation, discrimination, or humiliation of the affected individual.

Yet another problem is the number of errors present in a given data bank at a given time. Errors can arise at the data entry stage, or through exchange, transmission, and updating of data. Once erroneous data is embedded in a computer database, it becomes difficult to correct and is automatically treated as if true. Errors in individuals' records, even if minor, have the potential to cause grave inconveniences.

Finally, the secretive and concealed nature of information collection techniques can raise suspicion and concern about the intrusiveness and the legality of data collection. In a study using focus groups, Cespedes and Smith (1993) presented a scenario to the participants, in which a bank used customer profiles, purchased from a third party, to target customers for specific financial products. Although this practice is legal and may even enable the bank to deliver better customer service, the participants stated that they would be "pretty mad if [they] found out [their] bank was buying information about

them" (Cespedes and Smith, 1993). It seems that "the very 'secrecy' of the collection process breeds resentment" (Cespedes and Smith, 1993).

Today, with the unprecedented advances in information technology, the quantity and the speed of the information exchange has significantly increased. Moreover, the rapid decrease in the cost of data storage, as well as its ease of retrieval, has perpetuated the collection and storage of personal information without financially burdening the collecting organisations. As more information accumulates, organisations find new uses for it, as if the availability drives the need. Data mining, profiling and data matching are some examples of the creative schemes which organisations can now use to extract information from available databases. Organisations can utilise these techniques to look for patterns based on which they can make better business decisions. The information resulting from these sophisticated techniques are proving useful in database marketing (DBM⁹), fraud prevention, or other organisational purposes (Smith, 1993).

The increasing trends towards collection of personal information and the rapid advances in computer and communications technology have contributed to record level concerns about information privacy. The following section will look at some opinion polls to illustrate this phenomenon.

⁹ "Database Marketing uses information about consumers in order to improve the efficiency of what might be called the three Ts: *targeting* of current and potential buyers, *tailoring* marketing messages and products more specifically to customer groups, and *tying* good relations with customer groups by targeting and tailoring practices" (Smith, 1993).

2.2.2 Public Opinion Surveys

Recent opinion surveys conducted in Canada indicate high levels of concerns about the issue of information privacy. As mentioned in the introduction, these surveys reflect only general concerns about privacy, without fully exploring the dimensions of this construct or providing a clear definition (Regan, 1995). Furthermore, these polls do not measure the extent of individuals' actual experiences with respect to invasions of their privacy. This section presents three Canadian surveys that were conducted in the 1990s by three different organisations. The results illustrate the importance of the issue of information privacy to the Canadian public.

The first survey of 3,000 Canadian households, conducted in 1992 by Ekos Research Associates, found record level concerns about privacy. In this survey, 92 percent of respondents indicated moderate or higher levels of concern about their privacy with a particular emphasis on information privacy (Ekos Research Associates Inc., 1993). Asking respondents to rank ten different information types, this survey found particular concern about financial and medical information, as well as buying habits (Ekos Research Associates Inc., 1993). Furthermore, the survey found that the degree of concern is dependent on the type of organisation involved. It illustrated that those organisations involved in direct home selling elicited the highest levels of concern. The Ekos survey also found that even though there are high concerns about the privacy of information, the majority of Canadians surveyed had not experienced serious privacy invasions (Ekos Research Associates Inc., 1993).

Louis Harris and Associates conducted the second survey in 1994 for Equifax Canada Incorporated. This survey, which questioned 1,250 Canadians, also indicated high levels of concerns about privacy. This survey, however, showed that the majority of people support the collection and use of personal information by credit bureaux for purpose of credit risk assessments. It indicated that people are highly concerned about the unauthorised transformation of information, collected by one organisation for one purpose, to other institutions for use for some different and unauthorised purpose.

The third Canadian survey of interest was conducted by the “*fédération nationale des associations de consommateurs du Québec*” in collaboration with Ottawa’s “*Public Interest Advocacy Centre*” (FNACQ/PIAC, 1995). This survey, which questioned 2,000 Canadians in December of 1994, also indicated high levels of concern about information privacy. However, unlike the previous surveys, this survey suggested that individuals had considerable experience with invasions of information privacy. They reported that over 50 percent of respondents had experienced or thought they had experienced some type of privacy intrusion. These opinion polls clearly establish the existence of concerns about the issue of information privacy. The next section will look at the legal protection available to judge whether or not these concerns are merited.

2.2.3 Available Legal Protection for Information Privacy

Except in Québec, which has a general data protection statute applying to the private sector, no other Canadian jurisdiction provides privacy protection for personal information of individuals (Owens, and Lyons, 1998). Canadians living outside Québec,

whose information privacy has been invaded, must look for solution to their problems in common law or equity (Owens, and Lyons, 1998). Torts and equitable actions, which are relevant to this case, include actions relating to intrusion into one's private life and actions relating to disclosure or use of personal information (Owens, and Lyons, 1998). Actions of the first category consists of trespass, nuisance and privacy invasion, and the actions of the second category consists of defamation, negligence, breach of confidence, and the breach of fiduciary duty (Owens, and Lyons, 1998).

In case of privacy violations, if there is a contract between the parties, the provisions of the contract may restrict the ability of the individual to sue based on tort law or equity. Furthermore, in Canada the privacy tort is not clear with respect to information privacy intrusions, where no physical means are used to invade one's personal information (Owens and Lyons, 1998).

The torts in the second category of actions, relating to the disclosure or use of personal information, provide some protection. For example, in the case of defamation, if the personal information of an individual is communicated to one or more other persons, the individual can file a lawsuit under this tort (Owens and Lyons, 1998). However, this action is only possible if the information communicated is false (Owens and Lyons, 1998). Under the torts in this category of actions, there is some protection when harm is caused by unauthorised use or disclosure sensitive information in databanks (Owens and Lyons, 1998). However, it is unclear whether this would apply to personal information (Owens and Lyons, 1998). In the case of personal financial information, the action of breach of confidence to protect the individual depends on information type and the situation under which this information is disseminated (Owens and Lyons, 1998).

Unauthorised use of information may also be challenged under the action of breach of fiduciary duty. This duty applies to the relationship between two or more parties, one of which is dominant and has the authority over and the trust of the other parties. In such cases the dominant party must act in good faith and is prohibited from disseminating information to parties outside those in the relationship (Owens and Lyons, 1998).

In addition to the above protection, one can look at contract law for information privacy protection. However, the terms of a contract can act not only to protect privacy rights, but can also act to limit the scope of the protection (Owens and Lyons, 1998).

Although some protection seems to exist for the protection of information privacy of individuals, the above noted laws fall short of true protection for individuals. It is often difficult to demonstrate tangible damages as a result of information privacy invasion (Owens and Lyons, 1998). Even when one can convincingly show that damages were caused by the unauthorised use of one's personal information, one would receive only insignificant compensation (Owens and Lyons, 1998). Consequently, it would not deter future misconduct in handling personal information. Furthermore, the legal costs for individuals, who have suffered the invasion of their privacy, may be too high to justify legal action (Owens and Lyons, 1998).

The present legal protection against information privacy invasions is clearly insufficient. Hence, concerns of people about individual privacy are well justified. The following section discusses the issue of context sensitivity of these concerns. It reviews the available literature on this issue, based on information type, and organisation type.

2.3 The Context Sensitivity of Information Privacy Concerns

It has been suggested that the “information privacy practices of organisations, the perceptions of these practices and societal responses are inextricably linked in many ways” (Milberg, et al. 1995; Smith, 1994; Culnan, 1993; Stone, et al., 1983). However, there is no solid theoretical base to explain these relationships.

In 1993, Smith conducted an exploratory study to understand the practices and policies of organisations in the area of information privacy. His study consisted of 152 interviews, carried out between January 1990 and July 1992, with executives, managers, and non-management employees of seven organisations, as well as interviews and focus groups with consultants, trade association representatives and privacy advocates. He selected the interviewees from organisations that used varying types of personal information about current and potential customers. The results of the study suggested that consumers have varying privacy thresholds. These privacy thresholds were found to be dependent on the type of information that was collected, the method of information collection, and the people who collected the information. These results were in agreement with earlier studies by Stone (1990) and Culnan (1993), who had also suggested that the levels of privacy concerns were context sensitive. These and other researchers had suggested that the context sensitivity was based on organisation type (Stone et al., 1983) and information type (Culnan, 1993; Stone et al., 1990; Tolchinsky, 1981; Fusilier and Hoyer, 1980; Ganster, 1979; Rosenbaum, 1973).

The issue of context sensitivity of information privacy concerns was the driving force behind this research. In addition to the factor of information type and organisation

type, some other variables relevant to the level of privacy concern were also considered in this study. These variables included the type of technology used to store the information, previous personal experiences, and individual personality factors. However, because of time and resource limitations these variables were not fully explored. The following subsections review the evidence supporting the issue of context sensitivity.

2.3.1 Information Type

Early studies (Tolchinsky, 1981; Fusilier and Hoyer, 1980; Ganster, et al., 1979; Rosenbaum, 1973) have provided evidence for the existence of a relationship between information type and the perceptions of privacy invasions. The field study by Rosenbaum (1973), for example, suggested that individuals' perceptions of privacy invasion are a function of the type of information collected by an organisation. Ganster et al. (1979), who conducted a survey to explore the nature of employee perceptions and attitudes toward information handling practices in five multinational organisations, also submitted similar findings. They suggested that the perceived control over personal data, following its disclosure be related to individuals' attitudes towards the information handling practices of organisations (Ganster, et al., 1979). Furthermore, they showed that the type of information disclosed has an influence on the perceptions of the appropriateness of the disclosure (Ganster, et al., 1979).

Fusilier and Hoyer (1980) examined the relationship between information type and perceptions of privacy. These two researchers had hypothesised that: (1) depending on the outcome of disclosure, (2) the type of disclosure, and (3) the type of information

disclosed, individuals will experience less invasion of privacy, if they perceive that they have control over the use of the disclosed information (Fusilier and Hoyer, 1980). However, they were not able to support the results reported by Ganster and his team, and concluded that the type of information and the type of disclosure do not appear to be related to perceptions of privacy invasions. However, they recommended further research to determine what type of information might be perceived as sensitive. They suggested that the inconsistencies between their study and the earlier findings might be the result of differences in the average age and level of experience of the two samples.

Later in 1981, Tolchinsky and colleagues investigated the importance of information type in perceptions of privacy. They reported that a number of variables, including the willingness to disclose personal information, the consequences of information disclosure, the type of information disclosed, and the location of disclosure seem to affect the perceived invasion of privacy. They found that the perception of privacy invasion is greater in some cases than in others. For example, it is greater (1) when the information is disclosed without permission as opposed to being willingly disclosed, (2) when the consequences of disclosure are favourable as opposed to unfavourable, (3) when personality rather than performance information is disclosed, and finally (4) when personal information is disclosed to an external user rather than to an internal users (Tolchinsky, et al., 1981). Moreover, they ranked the order of importance of these variables as: (1) disclosure permission, (2) disclosure location, (3) disclosure consequences, and (4) type of information disclosed (Tolchinsky, et al., 1981).

Other investigators have documented that some types of information, such as medical and financial information, are more sensitive than other types of information

(Lou Harris and Associates, Inc., 1990; Stone, et al., 1983; Woodman, et al., 1982). The interviews conducted by Smith (1993) also revealed that the majority of people consider their medical and financial information to be especially sensitive. However, people do not seem to consider transactional information, resulting from the purchase of goods and services, to be particularly important. People perceive transactional information to be of even less importance if: (1) the organisation using and examining the data is the organisation from which the purchases were made, and (2) if they agreed to the scrutiny of information (Smith, 1993). This was congruent with the findings of a number of earlier studies, which had suggested that there are generally four situations where people are less likely to perceive information privacy practices to be invasive. The first situation is when information is collected in the context of an existing relationship. The second situation is when people think they have the ability to control future use of their personal information. The third situation is when is information that is collected is relevant to the transaction. Finally, people are less likely to perceive an information practice to be privacy-invasive when they believe the information will be used to draw reliable and valid inferences about them (Baker, 1991; Stone and Stone, 1990; Clarke, 1988; Stone, et al., 1983; Woodman, et al., 1982; Tolchinsky, et al., 1981).

Smith (1994) reported that the way in which corporations handle personal data seems to vary considerably from one industry to another. He suggested that there might be a “presumed hierarchy in the offensiveness of certain information practices.” For example, the collection and use of new information may be associated with less formal policies than the sharing of information. Smith also suggested that the sensitivity of the type of information a company handles may have some impact on the formality of the

companies' policies and on employees' perceptions (Smith, 1994). For example, policy would be less formal when employees perceive that the information being handled is less sensitive, and more formal when the information is perceived to be more sensitive.

The preceding research findings support an investigation of the relationship between concerns about the privacy practices and the different information types. To carry out a research, different types of information were classified into one of the two categories of *personality* or *performance* information, as suggested by Tolchinsky and his team (1981). The following sub-sections describe each of the two categories. A detailed description of record types within each of the two classes of information and their importance is emphasised in later sections.

Before one can proceed to look at different types of information, however, it is necessary to make a note. Throughout this proposal the terms "information" and "record" have been extensively used to refer to personal information. It is important to note the difference between the two. The definition of a "record" has dramatically changed during the past two decades. Traditionally, a "record" meant a document printed, or hand-written on paper. Today, it can consist of data appearing in "card files, tape files, data files, data bases, computer screens, programs, electronic mail, voice mail, word processing documents, image data bases, or other forms of electronic media regardless of its physical form or characteristics" that could be permanent or transient (Grupe, 1995). In other words, "a record is a collection of related data treated as a unit" (Watson, 1996). An example is a person's payroll data. A "record" may contain both performance and personality-types of information. One should note that in classifying information under the two categories of performance and personality, the assumption was made that a

record only contains only one or the other type of information and not both.

A) Performance Information

The majority of personal records portray individuals' past performances or previous actions. These records contain "performance information." Performance information of an individual is any information that recites the events that the individual has been involved in or actions in which the individual has taken in the past. Performance information does not include information about individual characteristics, beliefs or traits. One may find performance information in Financial Records, Transactional Records, Library Records, Police Records, Medical Records and Drug Testing Records.

Appendix A of Section 12.0 provides a detailed explanation of the importance of these record types and the reasons for considering them sensitive.

B) Personality Information

Personality information consists of information about a person's characteristics and traits, which may be used to predict that person's future behaviour, and performance. The personality category of information could be interest to employers, insurance companies, educational institutions and others that could benefit from predicting future behavioural, psychological or biological performance of individuals. Records that contain this type of information include Integrity (honesty) and Polygraph Testing Records, Ability (intelligence, or psychological) Testing Records, and Genetic Records. *Appendix B of Section 12.0* provides a detailed explanation of the importance of these record types and the reasons for considering them sensitive.

2.3.2 Organisation Type

In 1977, the Privacy Protection Study Commission published a report about the information privacy practices of organisations. In this report, the commission indicated that there was a lack of available information on the values, beliefs, and attitudes of the general public about these practices. In 1981, an opinion poll by Louis Harris and associates, a research firm in the United States, which had been conducting surveys on American attitudes toward privacy since 1970, identified the biggest invaders of privacy. Drawing from a list of 18 private and public sector organisations, the poll ranked the biggest invaders of privacy in the private sector as finance companies, credit bureaux, insurance and credit card companies, and newspapers, magazines, and television respectively. The poll revealed that the American public perceives the biggest invaders of privacy in the public sector to be the internal revenue services, Central Intelligence Agency (CIA), Federal Bureau of Investigations (FBI), Government welfare agencies, and Census Bureau respectively.

Discussion on the issue of privacy inspired a group of researchers to carry out a field experiment. They compared information privacy values, beliefs, and attitudes across six type of organisations including employers, insurance companies, law enforcement agencies, credit grantors, lending institutions, and international revenue services (Stone, et al., 1983). They found that organisation type has a significant impact on information privacy values, beliefs and attitudes (Stone, et al., 1983).

Later in 1990, another survey revealed a continuing distrust of institutions (Equifax, 1990). This survey indicated that people were concerned about the loss of

control over their personal information to credit bureaux, government, and other institutions. This finding was further confirmed by other surveys that found individuals to be distrustful of large institutions and governments, and to have grave concerns for their personal information (Rosenberg, 1992).

In Canada, the “National Canadian Public Opinion Survey” conducted a survey in 1992 to study the perceptions of privacy invasions. This poll found that people had the highest levels of concern about companies that sold goods directly to people at their homes. The poll named the biggest invaders of privacy as telephone companies, retail stores, credit bureaux, cable companies, insurance companies, banks, governments, police, survey companies including Statistics Canada, employers, doctors and hospitals respectively. Survey companies were found to provoke the highest and hospitals the lowest level of concern (Ekos, 1993).

Considering the limitations of this study and for the sake of simplicity, organisations were classified into three categories of government, for-profit, and non-profit organisations. People, in general, perceive government organisations to be distinctly different from other types of organisations. In a study, for example, Gandy (1989) found that participants of a focus group used quite a distinct schema when thinking about privacy in relation to government as compared to their employers, and to organisations providing them with goods and services (Gandy, 1989). Generally, government organisations are concerned about serving the public rather than making financially profitable decisions. For-profit organisations, on the other hand, are primarily concerned with financial gain. These organisations include public and private corporations, partnerships and sole proprietorships.

Non-profit organisations are distinct from both the government and the for-profit organisations. Universities, associations, and charities are some forms of non-profit organisations. The following subsections review each organisation type in more details.

A) Government Organisations

The public has always been concerned about government surveillance. This concern is portrayed in “1984,” a book written in 1948 by the British author George Orwell. He portrayed a futuristic world where surveillance by the government was a fact of life. Orwell introduced the term “big brother,” to refer to the state whose watchful eyes monitored citizens at all times and at all places. However, Orwell had never imagined how computer and telecommunication technologies would revolutionise surveillance.

Governments have held the first position in personal information collection for many years. There are two reasons for this phenomenon. One is that governments need a wide range of personal information to properly manage and provide necessary social services to the public (Johnson, and Nissenbaum, 1995). Second is that early computers were expensive and only government organisations could afford to purchase and maintain them.

One procedure that government organisations may use, to take advantage of the vast amount of information in their possession, is “computer matching.” Computer matching is “a technique whereby information within two or more records or files is compared to identify situations that could indicate program ineligibility or payment errors” (Kusserow, 1984). It is “the electronic comparison of two or more databases containing personal information, a form of mass dataveillance” (Cavoukian and Tapscott, 1995). Computer matching makes it possible to screen a number of databases to find

incriminating evidence against individuals, who are unknown at the beginning of the match. This technique gives the government the ability to detect fraud, recoup debts, or verify eligibility for certain government programs (Cavoukian and Tapscott, 1995).

Proponents of this practice claim that “computer matching is an efficient and effective technique for coping with today’s expensive, complex, and error-prone government programs” (Kusserow, 1984). However, the opponents allege that, despite its attractiveness as an investigative tool, this technique violates individual rights and ignores the presumption of innocence that is intended to protect people. Furthermore, they say that the cost cutting claims of computer matching are unfounded (Cavoukian and Tapscott, 1995; Shattuck, 1984). Another problem with computer matching is the errors resulting from erroneously or inaccurately recorded data.

In Canada, the government has introduced a policy for data matching, which provides some safeguards to protect individuals against privacy invasion. For example, the policy for computer matching calls for the submission of “an assessment containing the purpose, the legal authority, a cost benefit analysis, and other details of the proposed computer match” to the privacy commissioner (Cavoukian and Tapscott, 1995). However, these safeguards have not provided satisfactory results, since in practice federal agencies do not strictly adhere to policy guidelines (Cavoukian and Tapscott, 1995).

Although, the public continues to be concerned about the information privacy practices of government organisations, these organisations are somewhat regulated and do not pose as great a threat as previously thought. The new technologies, however, have provided other large organisations with the means to invade individual privacy.

B) For-profit Organisations

Although there is still some concern about the potential abuses of personal information by the government, in a capitalist enterprise society large for-profit organisations present a far greater threat (Schoechle, 1995). The commodification of personal information, the power of computer technologies, the availability of data manipulation techniques, and the inadequacy of current privacy laws provide means for “risk-averse organisations” to pursue their economic values. These values are based on self-interest, wealth accumulation and profit (Schoechle, 1995, and Wilson, 1988). For example, to fulfil their economic goals these organisations could reduce risk by defining what constitutes a deviant employee and eliminate those considered deviant from the list of employment candidates and current employees (Schoechle, 1995). This may create a pressure toward normalcy, which may unjustly prevent some people from access to services, jobs, or education.

C) Non-profit Organisations

Non-profit organisations are entities that are “not formed for pecuniary gain or profit of, and whose net earnings or any part thereof is not distributable to, its members, trustees, officers, or other private persons” ” (Oleck, 1974). In these organisation, however, “the payment of reasonable compensation for service rendered and the distribution of assets on dissolution is not deemed pecuniary or profit or distribution of earnings” (Oleck, 1974). This definition implies that non-profit organisations must eliminate all “profit-making” for their members and “investment-profit making” for their objectives (Oleck, 1974). Non-profit organisations are usually based on “voluntary association for the attainment of social, religious, educational, fraternal, economic or

other such purposes” (Oleck, 1974). Some examples of non-profit organisations include educational institutions, trade associations, credit unions, hospitals, professional associations, humane societies, religious and benevolent organisations and charitable organisations.

Non-profit organisations may or may not be charitable. A charitable organisation means “an entity organised and operated exclusively for religious, charitable, scientific, testing for public safety, literary, or educational purposes, exclusively for the prevention of cruelty to children or animals, or exclusively for a home for the aged...” (Oleck, 1974). Although a non-profit organisation is not necessarily charitable the reverse is always true. In this thesis, non-profit organisation shall include charitable organisations as well as non-charitable non-profit organisations.

As with any other organisation, non-profit organisations are formed to meet a specific objective. Computer technology enables these organisations to use personal information in the same manner as other types of organisations to meet their objectives. In this sense, the potential for abuse of personal information is also present in non-profit and charitable organisations.

2.3.3 Technology Type

Organisations have always been involved in collecting, storing, and exchanging personal information. Thus, the potential to invade one's information privacy has existed even before the advent of computer technology. However, with the emergence of every new technology, the question of the effects of technology on individual privacy resurfaces.

Earlier studies regarding the harmful consequences of computerised record-keeping systems – increase in organisational data processing capacity, more access to personal data, and the creation of technical record keepers – have shown that computer technology is a catalyst and not the cause of the public concern about privacy (Regan, 1995). Two concurrent 1969 studies funded by the United States' Russell Sage Foundation and the National Academy of Sciences, conducted by Alan Westin and Michael Baker, exemplify such studies. These studies concluded that computerisation of records was not the villain and refuted the claims for the early arrival of what was predicted in Orwell's '1984' novel (Regan, 1995). By the 1970s, the United States' congressional subcommittees, a federal agency committee, and the National academy of Science, who were interested in this area, had all agreed that the problem was the invasion of individual privacy and not the technology (Regan, 1995).

These earlier findings are in conformity with a realistic view¹⁹ of technology, as opposed to a deterministic and neutralist view of technology. The realistic view, which is a middle ground between the two extremes, maintains that technology has a force of its

¹⁹ Technology realism (as opposed to determinism and neutralism) maintains that there is a dynamic relationship between technology and society, which determines the direction and uses of technology.

own but is influenced by social and political forces. It looks at technology as an agent of change. It states that “technology changes, or at least influences, ideas and interests within government or other organisations, and sets the course for further technological advancements” (Regan, 1995).

Technology neutralists, however, view technology as an independent force. They maintain that people are responsible for shaping technologies to their liking. In the neutralist paradigm, management values technology because it can consolidate its social control over individuals by providing additional control over their personal information (Brown, 1996). This will lead to what Burris calls “panoptic power” over individuals (Burris, 1993). This idea is compatible with Marxist ideology, which looks at technology as a means of social control, which creates a class of technocrats administering the system who effectively deprive the masses from their rights (Burris, 1993). Neutralists believe that “Information Entrepreneurialism”²⁰ is perpetuating a trend toward the development of information technologies, justified by corporations and governments in the name of administrative efficiency, fraud prevention, or convenience for the consumer that permit more invasions of privacy (Davies, 1994). Neutralists name smart cards, biometrics identification technologies²¹ and SMS²² as examples of impending privacy

²⁰ This term refers to a set of social practices that focus on “active attempts of coalitions within organisations to organise corporate production to take advantage of changes in key social relationships and in information technology, push to increase monitoring of indirect social relationships, and gain market and organisational advantage” (Kling, 1994). The belief is that there are systematic arrangements within society and industry that reward organisations for development of “informationalised services” (Kling, 1994). An inclination toward the “improvement in absolute capabilities and cost/performance ratio,” trends in “precision marketing,” and the “micro-practice of *Information Capitalism* (an economic arrangement to gain profit from the use or sale of information) by individuals who manage the information technologies” are some explanations given for this phenomenon.

²¹ A form of identification that is based on “what an individual is” as opposed to what one has - a card - or what one knows - a password or PIN. This form of identification includes finger printing, retina scanning systems, voice recognition systems, and hand writing patterns or signature recognition systems (Davies, 1994).

invading technologies that are in the process of becoming universally accepted. Neutralists believe that, despite increasing concerns about privacy issues, the public is prudently accepting new privacy-invading schemes (Davies, 1994). Neutralism indicates that the recent popularity of personal computers, to some extent, account for public's acceptance of new technologies (Davies, 1994). However, it is not clear whether this acceptance is genuine or stems from public's naiveté about the repercussions of privacy invasion.

Finally, determinists view technology as an independent force, which determines the fate of all societal patterns of existence and the course of societal change (Winner, 1977). For example, Jacques Ellul, in his book 'The Technological Society,' argues that "technology is integrated into society in an invidious way" by what he calls techniques²³, which, when entered into every area of life, cease to be external to man; it becomes his substance" (Ellul, 1964). This paradigm looks at technology as the cause of invasions of privacy; hence it treats technology as an independent variable, and the privacy invasions as the dependent variable (Regan, 1995). Determinists believe that humans will eventually lose control of their created technology and become its servants.

There are many different methods of data storage and data processing architectures. For the purposes of this thesis, modes of data storage were classified into three technology types. These technologies included databases, smart cards, and manual file storage systems.

²² SMS is the Microsoft's System Management Server. This technology enables the network specialists to view and control workstations from a remote site (Riley, 1996).

²³This is defined as "the totality of methods rationally aimed at, arrived at, and having absolute efficiency in every field of human activity" (Ellul, 1964).

A) Databases

The term database may be defined as “a collection of related files,” or “a collection of different types of data or one or more files, organised according to a structure that minimises redundancies of the data, treated as a whole unit” (Watson, 1996). Speaking of relation between these files refers to the fact that these files contain information that serves a common purpose. For example, the files may be about a particular person being an employee, a student or a patient.

For the purpose of this thesis, the term “database” included all types of databases (centralised or distributed) regardless of being LAN-based architectures, client/servers, personal databases, or mainframes.

B) Smart Cards

A “smart card” is a small plastic card, the size of a credit card, with an integrated circuit, consisting of a microprocessor, memory, a processing unit and in some cases a cryptographic unit and a coiled antenna (Morris, et al., 1995). Hence, it is capable of storing, retrieving, and processing considerable amounts of information stored on the chip. The technology for imbedding computer chips in plastic cards is less than 15 years old. Ronald Moreno was the first person to develop the basic idea of implanting electronic chips into plastic. Michael Ugon who imbedded a processor and a memory along with the microchip into plastic cards (Morris, et al., 1995) later improved this technology.

The use of smart cards for various daily functions such as banking, long distance calling, car washing, shopping, and health care is on the rise and; it is becoming a universally accepted convenience in number of countries around the world (Morris, et al., 1995). Despite the smart cards’ optimisation for maximum security, there are a number of

privacy concerns with respect to their use particularly in health care. Like any other computer data, we can agree that medical information on smart cards needs to be “backed up,” to prevent information loss due to misplaced, damaged, or stolen cards. This requires a centralised database, maintained by a third party – being a government or private body– to handle sensitive personal information (Morris, et al., 1995). To uniquely identify each individual, an identification number would then be necessary. It is this notion of administering an identification number that causes privacy concerns about this technology. However, as the society becomes more desensitised to privacy invading technologies the ease of use, cost effectiveness and the promise of improved health care may overcome these concerns. Morris and colleagues (1995) name three distinct approaches for the use of smart cards. The “key medical information” approach only allows a minimal amount of personal data to be stored in the central database. This, to some extent, protects sensitive data from the unauthorised users. In the second approach, the smart card acts as an access key, without which access to information on the card would not be possible. The last approach is to have the complete medical information of the patient on the card. This will necessitate the adjunct use of a centralised database. In addition zoning of the card can allow users to only access relevant zones on a need to know basis. For instance, a pharmacist may only access the zone for medications and not zone for vaccination history.

C) Manual File Storage

People have always offered their personal information to organisations in one form or another. Before the advent of computers, personal information was somewhere in the world, but it was relatively safe because organisations were dependent on pieces of

paper as their main storage system. Thus, collecting information to create the profile of an individual meant travelling from one location to another and combing through filing piles of paper stored in filing cabinets. Dependence on manual file storage systems has since largely disapproved. Although many companies still use manual file storage as a complement to their computer databases, the trend is toward a paper-less organisation.

2.3.4 Other Factors Affecting Concerns

Other factors have been suggested to affect the levels of information privacy concerns. These factors include (1) previous personal experiences, (2) media-acquired knowledge, (3) individual personality factors, and (4) demographic factors. Each of these are briefly discussed below.

A) Previous Personal Experiences and Media -acquired Knowledge

Based on earlier research (Culnan, 1993; Stone and Stone, 1990; and Westin, 1990), Smith (1996) suggested two possible "causal" variables, which may affect the levels of information privacy concern. The first variable, previous personal experience refers to individuals' previous exposures to, or past victimisation resulting from, personal information misuses, which may increase levels of concern. The second variable, media-acquired knowledge refers to information covered in the media or individual's level of knowledge about the issue of information privacy. This variable may affect the levels of concern about information privacy practices of organisations. To determine whether these variables had any effect on the levels of concern, Smith (1996) added two questions to his instrument and presented the questionnaire to 77 business graduate students from

two geographically separated regions. These questions, which were patterned after those in Equifax (1990), were as follows:

- 1) "How often have you personally been the victim of what you felt was an improper invasion of privacy?" and;
- 2) "How much have you heard or read during the last year about the use and potential misuse of computerised information about consumers?"

Using a regression analysis, with previous personal experiences and media-acquired knowledge as independent variables and the overall information privacy concerns as dependent variable, Smith (1996) determined that the research proposition for the affects of these variables is strongly supported.

B) Individual Personality Factors

Others have suggested other factors that may have correlation with information privacy concerns (Stone, 1986; Bersceid, 1977; Levin and Askin, 1977, Laufer and Wolfe, 1977; Warren and Lasslet, 1977; Cozby, 1973) with information privacy. These factors include 1) trust versus distrust, 2) paranoia, and 3) social criticism²⁴.

To confirm the correlation between these factors and concerns about information privacy, Smith (1996) included scales that measure these factors in his instrument, and presented the instrument to undergraduate business students. He found a positive correlation between "cynical distrust," "paranoia, social criticism" and the "overall level of concern." Thus individuals with high levels of distrust, individuals who are paranoid, or individuals "who reject society's values, norms, and practices," would exhibit high

²⁴ "The degree of acceptance or rejection of the values, norms, and practices of ...society" (Jessor and Jessor , 1977 quoted in Smith, 1996).

levels of concern about the use and dissemination of their personal information (Smith, 1996).

It has been suggested that individuals who exhibit high levels of concern about the issue of information privacy are more likely to refuse participation in “activities that require the provision of personal information” (Stone, et al., 1983). It has also been suggested that these individuals are “more likely to contact official agencies or companies regarding information privacy practices (Stone, et al., 1983). Smith (1996) supported this research proposition in an experiment using 77 business graduate students from geographically separated areas. He found that higher levels of information privacy concern are positively correlated with stronger intentions to take privacy-related actions (Smith, 1983).

C) Demographic Variables

The experience with opinion surveys indicates that demographic factors such as age or education are related to both concerns and survey participation (Singer, et al., 1993). Furthermore, concerns about confidentiality and privacy significantly reduce the probability of response (Singer, et al., 1993). Although there are no studies available to document the relationship between these demographic variables and levels of concern, it is conceivable that these variables affect privacy concerns.

2.4 Hierarchy for the Dimensions of Information Privacy Concerns

It has been suggested that there may be a hierarchy for the various dimensions of privacy concerns. Smith and his colleagues (1996), for instance, observed that “the highest levels of concern were associated with the improper access to and unauthorised

secondary use of personal information, and the lowest levels of concern were associated with the collection of and errors in personal information.” They also reported that the hierarchy of concern varies between samples (Smith, et al., 1996). In another study, Milberg and her associates (1995) examined the relationships among nationality, cultural values, personal information privacy concerns, and information privacy regulation. In this study they revealed that concerns vary across countries. They found the lowest levels of concern in Thailand and the highest in Canada. Furthermore, looking at the relative importance or hierarchy of dimensions of concerns across nationalities, they found that the dimensions of concerns were consistent across nationalities (Milberg, et al., 1995). In fact, they found that unauthorised secondary use of personal information was the highest concern dimension in seven of the nine countries sampled; and the second in the next two (Milberg, et al., 1995). They also found that in Canada, the rank ordering of the levels of concern was unauthorised secondary use, improper access, collection and errors respectively.

3.0 Research Framework

Based on the available evidence the following framework was proposed. This model proposes a relationship between *information type*, *organisation type* and the four central dimensions of concerns. Figure-I illustrates the proposed research framework.

Figure 1: Proposed Research Framework

In this framework “*information type*,” as an independent variable, includes a *performance* category of information, and a *personality* category of information. The performance category of information consists of six types of records – financial, transactional, police, library, medical and drug testing records. A detailed description of each type of record in this category is provided in *appendix A*. The personality category of information consists of three types of records – Integrity testing, ability-testing, and genetic testing records. These record types are discussed in more details in *appendix B*.

The model’s second independent variable – *organisation type* – includes government organisations, for-profit organisations, and non-profit organisations. Each of these organisation types was discussed earlier in *chapter 3.3.2*.

As indicated earlier, there are reasons to believe that other variables may influence levels of concern of individuals. These include technology type used for information storage, previous personal experiences, media-acquired knowledge, personality factors, and demographic variables (age and education). These variables were not included in the model at this time because of time and resource limitations. However, for future explorations a number of questions were included in the research instrument. Personality factors were not considered for future exploration because these factors occur randomly and may not be of great importance when samples are selected randomly. To explore demographic variables the study population was divided into two groups based on age and education (professors and students). This grouping was used to permit separate analyses if the groups were found to be different.

4.0 Research Questions and Hypotheses

4.1 Group Differences

Age and level of education were suspected to affect levels of concern. If they did affect the levels of concern, then it was of interest to carry out separate analyses based on age and education groupings. If no effect was observed, then it was necessary to carry out analyses on respondents as one large group. Therefore, the following questions were put forward.

Research Question 1:

Do individuals of different age groups exhibit different levels of concerns about information privacy?

H₁: Individuals of different age groups exhibit different levels of concern about information privacy.

Research Question 2:

Do individuals with different education levels exhibit different levels of concern about information privacy?

H₂: Individuals with different education levels exhibit different levels of concern about information privacy.

4.2 Sensitivity of Records Types

Different types of records were categorised in to two different categories, namely *performance* and *personality* categories of information. To explore the relative sensitivity of each type of record, within each category of information in provoking concerns, the following question was posed for testing.

Research Question 3:

Do individuals exhibit varying levels of concern when they are prompted to think about different record types within each category of information?

H_{3a}: In the personality category of information, for all dimensions of concern, "genetic records" provoke more concerns than "ability testing records" and "integrity testing records."

H_{3b}: In the performance category of information, for all dimensions of concern, "financial records" followed by "medical records" and "transactional records" provoke the highest levels of concern.

Another question was also put forward to explore whether the two categories of information provoked different levels of concern.

Research Question 4:

Do individuals exhibit varying levels of concerns when they are prompted to think about the two – performance and personality – categories of information?

H₄: For all dimensions of concern performance-type records raise more concern than personality-type records.

4.3 Information-handling Practices of Organisations

Specific types of organisations handle different types of information about individuals. Survey results and public opinion polls presented earlier suggest that individuals' concerns may vary depending on the type of organisation handling their personal information. The following questions the possibility of such effect.

Research Question 5:

Do individuals exhibit varying levels of concern when they are prompted to think about different types of organisations?

A review of the literature suggests that individuals are highly concerned about the invasion of their information privacy by for-profit organisations.

H₅: for all dimensions of concern, individuals exhibit the highest levels of concern when they are prompted to think about for-profit organisations, and the lowest levels of concerns when they are prompted to think about non-profit organisations.

4.4 Safety of Information under different Storage Technologies

Although no moderating variables were included in the research model, a question was included with the research instrument to explore perceptions about the safety of personal information using different technology types²⁵ (*databases, smart cards, and manual filing storage systems*) used for information storage.

Research Question 6:

Do individuals demonstrate varying levels of concern about the safety of their personal information when different types of technologies are used to store their personal information?

The following hypothesis addressed this question.

H₆: Individuals exhibit varying levels of concerns about the safety of their personal information when they are prompted to think that their personal information is stored using computer data bases, smart cards or manual storage files.

²⁵ Adopting the realist view of technology and considering technology as a catalyst rather than the cause of public concerns, the a priori belief was that technology, by itself, has only facilitated the collection, the storage and the exchange of information, changing rather than instituting this process. The study assumed Westin's (1967) position that the organisational usage of technologies and benefits resulting from their usage is what threatens privacy and raises concerns, not their mere existence.

4.5 Hierarchy of Concern Dimensions

An additional undertaking included investigating the existence of a hierarchy of concerns with respect to different types of stimulation – *information type*, and *organisation type*. Based on findings presented in *chapter 3.4*, the following questions were posed for testing.

Research Question 7:

Is there a hierarchy for the dimensions of the information privacy concerns of individuals when they are prompted to think about information type?

Research Question 8:

Is there a hierarchy for the dimensions of the information privacy concerns of individuals when they are prompted to think about organisation type?

The following hypotheses were used to test these questions.

H₇: *In order of importance, the rank ordering of the dimensions of information privacy concerns is secondary use, improper access, collection and errors respectively, given that the individuals are prompted to think about information type.*

H₈: *In order of importance, the rank ordering of the dimensions of information privacy concerns is secondary use, improper access, collection and errors respectively, given that the individuals are prompted to think about organisation type.*

5.0 Research Methodology

The ultimate objective of this study was to investigate the context sensitivity of the levels of concern of individuals, about the information privacy practices of organisations. That is to say, the aim was to investigate whether the type of information used by organisations or the type of organisations handling personal information had any effect on the levels concerns about information privacy. The primary goal was to identify 1) the type of information that elicited the most and the least concerns, and 2) the most trusted and the least trusted types of organisations. Furthermore, as individuals were prompted to think about different types of stimuli, it was of interest to investigate whether there was a perceived relative importance (or hierarchy) for the four dimensions of privacy concern. For the purpose of future studies, a question about technology type was also included to explore whether individuals demonstrated different levels of concern about the safety of their personal information, when it was stored using different information storage technologies. This chapter describes the research methodology. It consists of four sections, which outline research design, sampling, data collection, and data analysis.

5.1 Research Design

This study was a one time, cross sectional, field survey to investigate the level of concerns of individuals about information privacy practices of organisations. It was carried out in November 1998. To collect data the research targeted the academic population of Carleton University – a Canadian university located in Ottawa, Ontario.

This population is comprised of (1) faculty members and (2) all currently registered part-time and full-time students. The student sub-population was delimited to only third and fourth year students. Assuming that professors were both older and more educated, the population was divided into two groups based on a combination of two demographic variables, namely age and education.

Each sample of subjects drawn from the population was exposed to all levels of the study's independent variables. Each respondent completed a self-administered questionnaire with structured response categories. For each subject, the questionnaire elicited 91 responses. These responses were obtained by asking 18 questions in total. The following table lists each variable, and corresponding research question, hypotheses, and instrument question number(s).

Table 5.1-I: Study variables & corresponding hypotheses, instrument & research questions, responses elicited.

Variables		Instrument Questions	Number of responses elicited	Research Questions	Hypotheses
Independent (or Moderating)	Dependent				
Demographic variables: Age & Education	None	None	None	1,2	H ₁ , H ₂
Information Type	Collection	4-6	27	3, 4	H _{3a} , H _{3b} , H ₄
	Errors	7	9		
	Unauthorised Secondary Use	8-9	18		
	Improper Access	10	9		
Organisation Type	Collection	11-13	9	5	H ₅
	Errors	14	3		
	Unauthorised Secondary Use	15-16	6		
	Improper Access	17	3		
Technology type	N/A	18	3	6	H ₆
Hierarchy of Concern Dimensions				7, 8	H ₇ , H ₈
Previous Personal Experiences	N/A	1	1	N/A	N/A
Media Acquired Knowledge	N/A	2	1	N/A	N/A
Personality Factors (Trust, and Acceptance of Social values and practices)	N/A	3	2	N/A	N/A

In addition, subjects provided answers to three demographics questions providing additional information on their age, level of education, and gender. Student respondents were asked to reply to two additional questions, one to determine the number of courses for which they had registered, and the other to determine their major field of study. A copy of the questionnaire is available in Appendix C.

The questionnaire included an introductory section to provide respondents with sufficient background information to be able to complete the questions. The introductory section also provided reassurance about the anonymity of responses. Based on experience with a pre-test of the questionnaire on five individuals, the respondents were notified that approximately 15 minutes was required to complete the questionnaire. To increase response rate, questionnaires were presented to respondents in person and followed up by sending e-mails and revisits.

Data collected from all questionnaires were analysed using the Social Sciences Statistical Package (SPSS). Mean differences between groups were examined using the analysis of variance techniques (MANOVA, ANOVA and post hoc procedures). Pair-wise t-tests were used to rank mean responses to different stimulation (multiple comparisons of means) – information type, organisation type, technology type – and privacy concern dimensions.

5.2 Sampling Design

Assuming that the population was divided into two non-overlapping groups or strata (professors & students), a combination of stratified and cluster-sampling techniques

was employed to randomly select individuals from each group. Using this technique, the population (denoted P) was partitioned into two sub-populations or strata (denoted as P_1 and P_2). Figure-II illustrates the design of this study.

Figure-II: Sampling Design of the Study

5.2.1 Sampling of the Faculty Members (P_1)

The sampling frame for collection of samples from P_1 was the Directory (white pages) of Carleton University Departmental Members. A copy of this directory was available on university's web site. It contained a total of 1,112 individual names with their electronic mail addresses and telephone numbers. This list included all persons holding tenured, preliminary, and term positions and all other departmental staff.

To identify and eliminate departmental staff and faculty members on sabbatical from the sample frame, names on the list were compared to those listed in university's undergraduate calendar as teaching staff. A total of 155 individual names was identified

and eliminated. The final sample frame for this population consisted of 957 names. Based on an annual report published by the Institutional Research Department of Carleton University, there were only 641 full-time and regular part-time teaching staff positions during the 1997-1998 academic year (see table 5.2-1). The difference between the two numbers (316 names or 33%) was attributed to (1) new teaching positions in 1998-1999 year and (2) individuals who did not belong to the study population. To determine the required sample size the larger list was used. However, sampled individuals who did not belong to the study population were identified during questionnaire distribution and did not receive the questionnaire.

Table 5.2-II: Full-time and Regular Part-time Teaching Staff (1997-1998)

Name of the Faculty	Positions (a)			On Campus (b)		
	Male	Female	Total	Male	Female	Total
Sciences	99	10	109	81	9	90
Public Affairs & Management	121	61	182	99	45	144
Arts & Social Sciences	156	89	245	131	67	198
Engineering & Design	98	7	105	81	5	86
Grand Totals	474	167	641	392	126	518

(a) Includes all persons holding tenured, preliminary, and term appointments.
Also includes those on leave of absence.

(b) Excludes faculty members on paid and unpaid leave, and those on sabbatical.

Using sample size tables (Cohen, 1977), the required sample size (n) was determined as a function of the anticipated effect size (d), the pre-set significance criterion (α), and the desired power. In this case, the author expected a moderate effect size of d ranging between 0.5 and 0.7 and set α to be equal to 0.05 ($\alpha_2 = 0.10$). Cohen (1977) suggests, "when an investigator has no other basis for setting the desired power value, the value 0.80 be used." By setting the desired power at 0.80, the Type II Error

(b)²⁷ is set at 0.20. Cohen (1965) provides several reasons for this arbitrary power value assignment. The most important reason considers the “implicit convention for using α of 0.05” (Cohen, 1977). The idea in this reasoning is that “the general relative seriousness of these kinds of errors is the order of 0.20 / 0.05, i.e., that Type I errors are the order of four times as serious as Type II errors ” (Cohen, 1977). Based on Cohen’s (1977) sample size tables, this translated into a sample size of approximately 26 (when $d = 0.7$), and 50 (when $d = 0.5$) for this group.

To select a simple random sample, numbers from 1 to 957 were assigned to each name on the sample frame. Since it was expected that only approximately 67% of the 957 individuals belong to the study population, to obtain a final sample of 50 names, a total of 74 names were randomly selected using a hand calculator²⁸. Table 5.2-II illustrates the desired and actual number of samples for the study.

Table 5.2-II: Theoretical and actual sample sizes for P_1 :

		Desired Sample		Actual Sample		Total
		Desired Numbers	Approx. %	Actual Numbers	Approx. %	
		74	100%	74	100%	74
Individuals that did not belong to study population and were removed	Sabbatical	24	33%	6	8%	31
	Not found			4	5%	
	Deselected			2	3%	
	Departmental Staff			19	26%	
Non-Response**	Refused	24	33%	2	3%	14
	Did Not Reply			11	15%	
	Incomplete Response			1	1%	
Actual Response		50	67%	29	41%	29

** Total non-response in this population was 18% (15% + 3%)

²⁷ $b = 1 - \text{power} = \text{type II Error}$

²⁸ $74 - (74 * 0.33) = 50$ (or $74 * 67\% = 50$)

5.2.2 Sampling the Undergraduate Students (P_2)

Carleton University's "Class Schedule Guide" was used to draw a sample from this population (P_2). Different classes offered during the fall term were placed in a list in order of course numbers. Because of resource and time limitations, first and second year and all Interactive T.V. (ITV) courses²⁹ were excluded. A number of classes for were selected for questionnaire distribution. Once the classes for questionnaire distribution were identified, the class instructors were asked to participate in the study. Table 5.2-III illustrates the information available on full-time and part-time student enrolment by level as at November 1, 1997. Assuming that the numbers have remained relatively unchanged from 1997 to 1998, the total population (P_2) including only 3rd and 4th year undergraduate students was estimated at approximately 5,500.

Table 5.2-III: Carleton University's part-time and full-time enrolment by level *

	Q Year	First Year	Second Year	Third Year	Fourth Year	Fifth Year	Diploma / Certificate	Masters	Ph.D.
Full-time Undergraduate Students	22	3,727	3,236	2,698	1418	61	—	—	—
Part-time Undergraduate Students	1	225	325	847	555	6	—	—	—
Full-time Graduate Students	28	—	—	—	—	—	12	1,142	459
Part-time Graduate Students	9	—	—	—	—	—	7	565	134
Totals	60	3,952	3,561	3,545	1,973	69	19	1,707	593
Total 3rd & 4th year	5,518 Students								
Under-graduates Total	13,100 Students								
Graduates Total	2,356 Students								

* Source: The annual report of Institutional Research Department of Carleton University.

²⁹ These are courses offered for distant education.

Using Cohen's (1977) tables the author presumed a design effect equal to 4 to account for the fact that clustering increases variance, a moderate effect size ($0.5 \text{ to } 0.7 = d = \mu - \mu_0 \div \sigma$), and an 80% power. Cohen's sample size was then multiplied by design effect of 4 to get the actual sample size required. This is a conservatively large estimate of the effect of clustering, whose effect will ensure that the sample size is large enough to detect real effects of interest. The final result of this exercise was a sample size of 104 to 200 ($26 \times 4 = 104$, $50 \times 4 = 200$). The following formula was then used to get the number of classes needed for the study.

$$\text{Number of classes needed} = \text{Actual sample size} \div \text{Average class size.}$$

Based on unofficial information obtained from Carleton University's Institutional Research Department, the average third and fourth year class size was found to be approximately 20 students. Therefore, the number of classes (clusters) needed for the study was calculated to be between 5 and 10 ($104 \div 20 = 5.2$, and $200 \div 20 = 10$).

Since the study was carried out during the month of November, non-response due to instructor's busy schedules was expected. For this reason, 40 classes were selected initially and the corresponding instructors were contacted to obtain permission for questionnaire distributions. Questionnaires were then distributed in selected classes. Since each student was likely to have registered in more than once class, an additional question was added to the questionnaire to determine the number of classes for which each participant was registered. Based on this information the responses were to be weighted to account for the probability of multiple selections. However, preliminary investigation revealed little difference between weighted and non-weighted estimates of means, so in the interest of simplicity, weights were not included in the SPSS analysis.

Students were also asked not to complete the questionnaires if they had done so in a different class. Table 5.2-IV illustrates the desired and actual number of students that were selected for the study.

Table 5.2-IV: Theoretical and actual sample sizes for the undergraduate group:

	Desired	Actual
Number of instructors contacted	40	20
Number of Clusters (Classes)	5 - 10	14
Number of Students	104 - 200	106

The actual number of instructors contacted was lower than expected because of time limitations and schedule conflicts. Of the 20 instructors contacted, four could not participate because they were behind on their teaching schedules, and two were not interested in participating in surveys. The number of students in each class was also lower than expected. Being close to the end of the term, some students were absent from classes. Furthermore, two students had completed the questionnaire in another class. The exact number of non-respondents in this group is unknown because in some classes questionnaires were returned during the next scheduled class time.

5.3 Data Collection

The researcher contacted each of the selected sampling units in P_1 and asked them to participate in the study. The subjects who agreed to participate received the self-administered questionnaire. To ensure anonymity of respondents, the faculty members were asked to use the university's internal mail to return their completed questionnaires. Questionnaires distributed to P_2 were collected from students in class either at the time they were distributed or in the following scheduled class period.

5.3.1 The Research Instrument

A) The Cover Letter

A cover letter accompanied the questionnaire to encourage responses. The opening words emphasised the importance of the study and the value of the respondents' participation. The letter clarified the intentions of the questionnaire and ensured strict confidentiality and anonymity. Appendix C illustrates a sample cover letter.

Detailed instructions pertaining to the questionnaire were also provided. The respondents were recommended to return their questionnaires anonymously using the university's internal mail (faculty members only), or to return completed questionnaires during their next scheduled class and hand them to their instructors (undergraduate students).

B) Anonymity Agreement

The participants will receive assurance that their responses remain absolutely anonymous. The participants will be reminded that all information provided is kept in strict confidence and will only be used for the purpose of this study.

C) The Questionnaire

The questionnaire used in this study (See Appendix E) was a modified version of an instrument prepared by Smith and his colleagues (1996) for researchers studying dimensions of privacy. Smith and his team developed their instrument to provide researchers in the field of privacy with a tool to measure the levels of concern of individuals about the information privacy practices of organisations. Appendix D illustrates the instrument development and the validation process as appeared in Smith, et al. (1996) and their 15-item instrument.

6.0 Data Analysis

The design of the study involved two groups of subjects, with each subject being measured on different dimensions of the dependent variable. For each record type and each organisation type, the questionnaire collected three responses on *collection*, two on *unauthorised secondary use* and one for each of *errors* and *improper access*. Responses for *collection* were averaged together to obtain the average response for *collection*. The same was done for responses on *unauthorised secondary use*. To eliminate fatigue and boredom effects a counter-balancing technique was employed, i.e., two sets of questionnaires were used, each set differing from the other only in the order in which the treatments were presented to the respondents.

A number of analyses were performed to assess proposed associations. Since the study's four dependent variables were conceptually related, a multivariate analysis of variance (MANOVA) was carried out for each of the record types and organisation types to detect group differences (students versus faculty) in levels of concern. Post hoc procedures followed each MANOVA to assess multivariate assumptions, power, and effect size. As a post hoc procedure, MANOVAs were followed by univariate tests each at a α level equal to 0.05, an appropriate procedure in cases where the multivariate null hypothesis is true (Stevens, 1996) and where the number of dependent variables is small. This procedure keeps the overall α level under control and provides greater power for detecting group differences. To detect group differences on technology types, a univariate analysis of variance was used.

To determine which information type is perceived to be more sensitive, the mean concerns for each type of record were ordered in a descending order of magnitude. Then, using pair-wise t-tests and the Dunn / Bonferonni³⁰ techniques the mean concerns were compared. The same technique was also employed to establish a ranking for levels of concerns with respect to handling of information by different types of organisations and perceived safety of information when different storage technologies were employed.

In this analysis, α was set at 0.05. For information type the maximum number of possible comparisons was 36 ($8 + 7 + 6 + 5 + 4 + 2 + 1 = 36$), since there were nine different information types. Therefore, $\alpha' = \alpha/C \Rightarrow \alpha' = 0.05 / 36 = 0.00139$. This confirms a significant difference when $p \leq 0.00139$. For Organisation Type and Technology Type comparisons the maximum number of possible comparisons was 3 ($2 + 1 = 3$), because there were three types of organisations and three types of technologies. Therefore, $\alpha' = \alpha/C \Rightarrow \alpha' = 0.05 / 3 = 0.017$ and that p was considered significant for values smaller than 0.017. For the four dimensions of privacy α' was 0.0083 ($\alpha' = \alpha/C \Rightarrow \alpha' = 0.05 / 6 = 0.0083$), since the possible comparisons were six ($3 + 2 + 1 = 6$).

As discussed earlier, sample size estimation for the student stratum took account of the variance inflation caused by clustering (using an assumed design effect of 4). The

³⁰ Dunn/Bonferroni is a method appropriate for pair-wise or general comparisons. This method is based on the idea of dividing the total α into parts. It divides evenly α among the C comparisons, by setting α' for each comparison to $\alpha' = \alpha/C$. This method is based on use of t distributions with ' C ' planned comparisons (Toothaker, 1991). It controls α for some group of comparisons, and thus maintains low Error Rates Per Family (Toothaker, 1991). "Error rate per family (ERPF) is the average number of erroneous statements (false rejections, Type I errors) made in a group (family) of comparisons (Toothaker, 1991). Using Bonferroni inequality, which says that *"the probability of one or more events is less than or equal to the sum of the probabilities of the separate event,"* Dunn (1961) contributed a table for t with probabilities α' for various values of C and df_w . The decision rule is to reject H_0 if $t \geq t_{\alpha', df_w}^*$, otherwise fail to reject H_0 (Toothaker, 1991). If α' is set as $\alpha' = \alpha/C$, then p (at least one Type I error) $< C\alpha'$ is conservatively bounded by α as shown by: $C\alpha' = C \alpha/C = \alpha$ the divisions of α and calculation of critical values is automatically done for the researcher by choice of critical values from Dunn's table (Toothaker, 1991).

analyses described above do not take this design effect into account. Analyses that account for clustering (Thomas, 1993) complicate the analyses to a considerable extent, so that an alternative strategy is pursued here. Since the effect of ignoring clustering is to increase the possibility of false rejections. A simple way to compensate is to lower the significance level at which tests are conducted. Normally, family-wise error rates for multiple comparisons are set higher than the standard 5%. For example, Stevens (1996) recommends setting an overall level of 15%, to provide a compromise between overall error protection and power for individual comparisons. In this study, overall family-wise error rates are maintained at 5% level rather than 15% in order to compensate for the effect of clustering.

7.0 Research Results

7.1 Descriptive Statistics

This section presents summary information about the distribution, variability, and central tendency of each of the study variables. It includes sample size, mean, and standard deviation.

Table 7.1-I: Descriptive statistics for information types.										
		Performance Information						Personality Information		
		F*	T*	P*	L*	M*	D*	I*	A*	G*
Group 1 = 106 (Students)										
Mean	Collection	5.78	5.64	4.70	3.88	5.06	4.58	4.77	4.93	5.17
	USU	6.65	6.56	6.40	5.78	6.50	6.42	6.36	6.37	6.58
	Errors	6.16	6.00	6.39	4.61	6.21	6.18	5.84	5.71	5.97
	Improper Access	6.83	6.75	6.56	5.49	6.76	6.56	6.45	6.37	6.70
Std. Deviation	Collection	1.25	1.25	1.57	1.53	1.54	1.62	1.39	1.25	1.34
	USU	0.90	0.99	1.16	1.57	1.11	1.15	1.10	1.15	1.04
	Errors	1.30	1.41	1.19	2.16	1.28	1.29	1.52	1.45	1.46
	Improper Access	0.59	0.76	1.16	1.94	0.71	0.99	1.17	1.21	0.85
Group 2 = 29 (Professors)										
Mean	Collection	6.06	5.97	5.17	3.89	5.41	4.75	4.79	4.93	5.16
	USU	6.47	6.36	6.28	5.76	6.42	6.40	6.43	6.38	6.2
	Errors	6.48	5.97	6.48	5.28	6.28	6.31	6.28	6.10	6.17
	Improper Access	6.62	6.48	6.52	5.56	6.41	6.28	6.55	6.38	6.24
Std. Deviation	Collection	0.94	0.90	0.94	1.44	1.17	1.29	1.16	1.01	1.15
	USU	1.25	1.34	1.44	1.97	1.34	1.30	1.30	1.33	1.53
	Errors	1.55	1.80	1.55	2.07	1.65	1.85	1.67	1.72	1.71
	Improper Access	1.2075	1.30	1.27	2.13	1.35	1.44	1.21	1.37	1.46
Group 1 + 2 = 135 (Students + Professors)										
Mean	Collection	5.84	5.71	4.80	3.88	5.133	4.62	4.78	4.94	5.17
	USU	6.61	6.51	6.37	5.78	6.48	6.41	6.37	6.37	6.50
	Errors	6.23	5.99	6.41	4.76	6.22	6.21	5.93	5.79	6.01
	Improper Access	6.79	6.69	6.55	5.50	6.69	6.50	6.47	6.37	6.60
Std. Deviation	Collection	1.19	1.19	1.46	1.50	1.48	1.55	1.34	1.20	1.30
	USU	0.99	1.07	1.22	1.65	1.15	1.18	1.14	1.18	1.16
	Errors	1.35	1.50	1.27	2.15	1.36	1.42	1.56	1.51	1.52
	Improper Access	0.77	0.90	1.18	1.97	0.89	1.10	1.18	1.24	1.02

* F= Financial Records, T= Transactional Records, P= Police Records, L=Library Records, M=Medical Records, D= Drug Testing Records, I=Integrity Testing Records, A= Ability Testing Records, G= genetic Testing Records

Table 7.1-II: Descriptive statistics for organisation types.				
Group 1 = 106 (Students)		For-profit Organisations	Non-profit Organisations	Government Organisations
Mean	Collection	5.96	4.76	4.86
	USU	6.59	6.31	6.25
	Errors	5.90	5.80	6.25
	Improper Access	6.67	6.59	6.80
Std. Deviation	Collection	1.26	1.38	1.54
	USU	1.02	1.14	1.17
	Errors	1.61	1.58	1.42
	Improper Access	0.81	0.97	0.72
Group 2 = 29 (Professors)				
Mean	Collection	6.02	5.64	5.26
	USU	6.53	6.43	6.19
	Errors	6.59	6.00	6.45
	Improper Access	6.55	6.38	6.59
Std. Deviation	Collection	1.41	1.38	1.82
	USU	1.25	1.29	1.47
	Errors	1.18	1.58	1.27
	Improper Access	1.21	1.32	1.24
Group 1 + 2 = 135 (Students + Professors)				
Mean	Collection	5.97	4.95	4.95
	USU	6.57	6.34	6.24
	Errors	6.04	5.84	6.29
	Improper Access	6.64	6.55	6.76
Std. Deviation	Collection	1.29	1.43	1.60
	USU	1.07	1.17	1.23
	Errors	1.55	1.58	1.39
	Improper Access	0.91	1.06	0.86

Table 7.1-III: Descriptive statistics for storage technology types.				
Organisation Type	Group	N	Mean	Std. Deviation
Manual Filing	1	106	3.25	1.82
	2	29	3.17	1.98
	Total	135	3.23	1.85
Databases	1	106	2.96	1.84
	2	29	2.41	1.35
	Total	135	2.84	1.76
Smart Cards	1	106	3.26	1.70
	2	29	3.24	1.46
	Total	135	3.26	1.64

7.2 Group Differences

7.2.1 MANOVAs

The first two study hypotheses (hypothesis 1 & 2) suggested that the individuals of different age groups and education levels exhibited different levels of concern about information privacy. With an assumption that the population was divided into two non-overlapping groups, with one group (professors) including individuals with higher age and education than the other group (students), two sets of MANOVAs assessing group differences were performed. The first set of MANOVAs investigated group differences on level of concerns based on type of personal records. The second set of MANOVAs assessed group differences when respondents were prompted to think about the type of organisation handling personal records. Tables 7.2-I and 7.2-II list the findings.

Table 7.2-I: MANOVA for group differences based on information types.										
Information Types		Performance Information						Personality Information		
Record Types		F*	T*	P*	L*	M*	D*	I*	A*	G*
Wilk's λ	F	1.74	1.14	0.71	0.82	0.99	0.78	0.54	0.55	2.13
	Sig.	0.15	0.34	0.59	0.51	0.40	0.54	0.71	0.70	0.08
	Eta Squared	0.05	0.03	0.02	0.03	0.02	0.02	0.02	0.02	0.07

* F= Financial Records, T= Transactional Records, P= Police Records, L=Library Records, M=Medical Records, D= Drug Testing Records, I=Integrity Testing Records, A= Ability Testing Records, G= genetic Testing Records

Table 7.2-II: MANOVA for group differences based on organisation types.				
Organisation Types		For-profit organisation	Non-profit organisation	Government organisations
Wilk's λ	F	2.37	3.45	1.46
	Sig.	0.06	0.01	0.22
	Eta Squared	0.07	0.10	0.04

The multivariate null hypotheses (hypotheses 1 and 2) stated that there is no difference between professors (older and more educated respondents) and students (younger and less educated respondents) with respect to the level of their information privacy concerns. A preliminary examination of the MANOVA procedures revealed no significant F values; thus, indicating no difference between the two groups with respect to information and organisation types.

Further investigation revealed a potential for violation of MANOVA assumptions. In all cases, the Box test¹ was found to be significant. To determine whether the multivariate test statistic is liberal or conservative, further investigation was carried out. Looking at the generalised variances, it was noted that the larger group size was associated with the larger generalised variance. Since the generalised variance was with the larger group size and the group effect was not significant it was necessary to determine whether the reason for lack of significance was the test's being conservative or the sensitivity of the Box test to minor violations of non-normality. Using Independent Sample t-test, the p- values for the pooled and separate variance standard error terms were examined and found to be similar or identical for all cases. Moreover, using the explore function of the SPSS multivariate normality was examined and found to be reasonable. This additional information provided further support to accept the null hypotheses 1 and 2.

¹ "Box test tests the null hypothesis that the observed covariance matrices of the dependent variables are equal across groups."

Following the MANOVA procedures, to estimate the power at the 0.05-level and to evaluate the size of the multivariate effect measure, F values were converted to T^2 values (Hotellings's T^2) and subsequently to D^2 (Mahalanobis Distance²) using the following equations:

$$\text{Equation (1)} \quad F = [(N-p-1)/(N-2)p] T^2 \Rightarrow T^2 = (N-2) p F / (N-p-1)$$

$$\text{Equation (2)} \quad D^2 = (N T^2) / n_1 n_2$$

Since the group sizes were different, following Cohen (1977), the harmonic mean was used as the n in the above equations:

$$\text{Harmonic mean} = \tilde{n} = 2n_1 n_2 / (n_1 + n_2)$$

Using Stevens (1980, 1996) power of Hotelling's T^2 tables the power values were estimated for all cases. The following table lists the T^2 , D^2 , power value and the effect size for each of the F values obtained in 7.2-I.

Table 7.2-III: Post Hoc Estimation of Power and Effect Size (Information Types)									
	Performance Information						Personality Information		
	F*	T*	P*	L*	M*	D*	I*	A*	G*
F	1.74	1.14	0.71	0.82	0.99	0.78	0.54	0.55	2.13
Hotelling's T^2	7.16	4.72	2.93	3.39	4.08	3.23	2.23	2.27	8.79
Mahalanobis Distance D^2 (Effect Size)	0.31	0.21	0.13	0.15	0.18	0.14	0.10	0.10	0.39
Power	< 0.45	< 0.45	< 0.45	< 0.45	< 0.45	< 0.45	< 0.45	< 0.45	< 0.45

Note: For values of $D^2 < 0.64$ the power is generally poor (<0.45) and never really adequate (i.e., .0.70) for $\alpha = 0.05$ (Stevens, 1996).

* F= Financial Records, T= Transactional Records, P= Police Records, L=Library Records, M=Medical Records, D= Drug Testing Records, I=Integrity Testing Records, A= Ability Testing Records, G= genetic Testing Records

² "Mahalanobis distance is a multivariate measure. It is a natural generalisation of the univariate measured. In this measure the means have been replaced by mean vectors and s (standard deviation) has been replaced by its squared multivariate generalisation of within variability, the sample covariance matrix S" (Stevens, 1996).

The following table presents a similar estimation for organisation types. The table lists the T^2 , D^2 , power value and the effect size for each of the F values obtained in 7.2-II.

Table 7.2-III: Post Hoc Estimation of Power and Effect Size (Organisation Types)			
	For-profit organisation	Non-profit organisation	Government organisations
F	2.37	3.45	1.47
Hotelling's T^2	9.79	14.23	6.04
Mahalanobis Distance D^2 (Effect Size)	0.43	0.62	0.27
Power	<0.45	< 0.45	< 0.30

Note: For values of $D^2 < 0.64$ the power is generally poor (<0.45) and never really adequate (i.e., .0.70) for $\alpha = 0.05$ (Stevens, 1996).

Tables 7.2-III and 7.2-IV show that the values for D^2 are small and, as a result, the power is generally poor. In addition to low power, the multivariate effect size is too small to consider significance. Therefore, it is safe to accept the null hypotheses for group differences and state that the two groups are not different with respect to information and organisation types.

7.2.2 ANOVAs

As a post hoc procedure, the above MANOVAs were followed by univariate ANOVAs each at a α level equal to 0.05. The results are provided in tables 7.2-IV, and 7.2-V.

Table 7.2-IV: ANOVA for group differences –information types										
Information Types		Performance Information						Personality Information		
Record Types		F*	T*	P*	L*	M*	D*	I*	A*	G*
Collection	F	1.27	1.72	2.39	0.00	1.34	0.26	0.01	0.00	0.00
	Sig.	0.26	0.19	0.13	0.98	0.25	0.61	0.95	0.99	0.99
Unauthorised Secondary Use	F	0.77	0.75	0.22	0.01	0.94	0.01	0.09	0.00	2.15
	Sig.	0.38	0.39	0.64	0.13	0.72	0.94	0.76	0.96	0.15
Errors	F	1.29	0.01	0.13	2.18	0.06	0.19	1.80	1.57	0.31
	Sig.	0.26	0.91	0.72	0.14	0.81	0.66	0.18	0.21	0.53
Improper Access	F	1.71	1.94	0.03	0.02	3.57	1.49	0.19	0.00	4.66
	Sig.	0.19	0.17	0.88	0.88	0.06	0.22	0.66	0.97	0.03

Table 7.2-V: ANOVA for group differences – organisation types				
Organisation Types		For-profit organisation	Non-profit organisation	Government organisations
Collection	F	0.07	4.27	1.41
	Sig.	0.80	0.03	0.24
Unauthorised Secondary Use	F	0.50	0.24	0.06
	Sig.	0.82	0.63	0.80
Errors	F	4.64	0.36	0.49
	Sig.	0.03	0.55	0.49
Improper Access	F	0.38	0.944	1.15
	Sig.	0.54	0.333	0.23

The post-hoc one-way ANOVAs assessing differences amongst the two groups revealed no significant F values. Therefore, it is safe to accept the null hypotheses that there is no difference between the two groups with respect to the study variables.

Hypothesis number six suggested that the individuals exhibit varying levels of concerns about the safety of their personal information when they are prompted to think that their personal information is stored using different means of information storage. To test this hypothesis an additional ANOVA was conducted to assess group differences with respect to individuals' perception of technology type storage safety. The result of this test is presented in table 7.2-VI. As illustrated, no significant values to indicate group differences were detected.

Table 7.2-VI: ANOVA for group differences on Technology type storage safety.			
	Manual Storage	Databases	Smart Cards
F	0.04	2.24	0.00
Sig.	0.85	0.14	0.95

7.3 Multiple Comparisons

7.3.1 Mean Concerns

Since no group differences were noted between students and faculty members, the two groups were pooled together and treated as a homogeneous population that demonstrate similar concerns about information privacy.

Table 7.3-I lists mean concerns of individuals for each type of information in a descending order of magnitude. This table was produced as the step in testing hypothesis H_{3a} , H_{3b} , and H_4 . These hypotheses were proposed to test research questions 3 and 4, which questioned the sensitivity of each type of information in stimulating individual concerns.

Table 7.3-I: Mean concerns (groups 1+2) in a descending order of magnitude*							
Record Type	Collection	Record Type	USU	Record Type	Errors	Record Type	Improper Access
Financial	5.84	Financial	6.61	Police	6.41	Financial	6.79
Transactional	5.71	Transactional	6.51	Financial	6.23	Transactional	6.69
Genetic	5.17	Genetic	6.50	Medical	6.22	Medical	6.69
Medical	5.13	Medical	6.48	Drug	6.21	Genetic	6.60
Ability	4.93	Drug	6.41	Genetic	6.01	Police	6.55
Police	4.80	Integrity	6.37	Transactional	5.99	Drug	6.50
Integrity	4.78	Police	6.37	Integrity	5.93	Integrity	6.47
Drug	4.62	Ability	6.37	Ability	5.79	Ability	6.37
Library	3.88	Library	5.78	Library	4.76	Library	5.50

*Note: A higher number mean a higher concern.

Table 7.3-II lists the mean concerns about the information-handling practices of different organisations. This table was produced as the first step to test hypothesis H_5 . This hypothesis tested research question 5, which questioned concerns about information-handling practices of organisations.

Table 7.3-II: Mean concerns (groups 1+2) in a descending order of magnitude*							
Organisation	Collection	Organisation	USU	Organisation	Errors	Organisation	Improper Access
For-profit	5.97	For-profit	6.57	Government	6.29	Government	6.76
Non-profit	4.95	Non-profit	6.34	For-profit	6.04	For-profit	6.64
Government	4.95	Government	6.24	Non-profit	5.84	Non-profit	6.55

*Note: A higher number mean a higher concern.

Table 7.3-III lists the mean perception of safety for technologies used to store personal information. It was produced for testing hypothesis H₆. This hypothesis tested research question 6, which questioned perceptions about the safety of personal information when different storage technologies were employed.

Table 7.3-III: Mean perception of safety (groups 1+2) in a descending order of magnitude	
Storage Technology	Mean Perception of Safety*
Smart Cards	3.26
Manual Filing	3.23
Databases	2.85

*Note: A higher number means a higher perceived safety.

Table 7.3-IV lists mean concerns with respect to the dimensions of privacy. This table was produced to address hypotheses H₇, H₈. These hypotheses tested research question 7 and 8, which questioned the relative importance or hierarchy of dimensions of concerns with respect to type of information or type of organisation handling personal information.

Table 7.3-IV: Mean concerns ordered in a descending order of magnitude.							
Dimension	Financial	Dimension	Transactional	Dimension	Medical	Dimension	Drug
Improper Access	6.79	Improper Access	6.69	Improper Access	6.69	Improper Access	6.50
USU	6.61	USU	6.51	USU	6.48	USU	6.41
Errors	6.23	Errors	5.99	Errors	6.22	Errors	6.21
Collection	5.84	Collection	5.71	Collection	5.13	Collection	4.62
Dimension	Police	Dimension	Library	Dimension	Integrity	Dimension	Ability
Improper Access	6.55	USU	5.78	Improper Access	6.47	Improper Access	6.37
Errors	6.41	Improper Access	5.50	USU	6.37	USU	6.37
USU	6.37	Errors	4.76	Errors	5.93	Errors	5.80
Collection	4.80	Collection	3.88	Collection	4.78	Collection	4.93
Dimension	Genetic	Dimension	Government	Dimension	For-profits	Dimension	Non-Profits
USU	6.50	Improper Access	6.76	Improper Access	6.64	Improper Access	6.55
Improper Access	5.50	Errors	6.29	USU	6.57	USU	6.34
Collection	5.17	USU	6.24	Errors	6.04	Errors	5.8444
Errors	4.7556	Collection	4.9504	Collection	5.968	Collection	4.9506

7.3.2 Pair-wise t-tests

As discussed earlier, in this study α was set at 0.05 and pair-wise t-tests were conducted for comparisons to determine which pairs of concerns in each table were different from the other pairs. Also, as indicated earlier, for information type pairs of means a significant difference is acknowledged when a $p \leq 0.00139$ was noted. For organisation type and safety of information storage technology pairs of means the significant value was set for values smaller than 0.017. For the four dimensions of privacy this value was set at 0.0083.

Table 7.3-V, 7.3-VI, 7.3-VII, and 7.3-VIII present the results of pair-wise t-tests for information types, organisation types, storage technology types, and hierarchy of dimensions respectively. They list only the pair-wise tests that were NOT significant (p

values larger than 0.00139 for information types, 0.017 for organisation and storage types, and 0.0083 for the four dimensions). A graphic presentation of the results follows each table.

Table 7.3-V: The result of pair-wise t-tests for information types (listing only the pairs that were NOT significantly different)				
Paired samples	Dimension			
	Collection	Unauthorised Secondary Use	Improper Access	Errors
Financial + Transactional	2.56 (0.01)	2.23 (0.03)	2.46 (0.02)	2.96 (0.00)
Medical + Police	-2.75 (0.01)	-1.36 (0.18)	-1.95 (0.05)	2.85 (0.01)
Integrity + Police	0.29 (0.78)	-0.04 (0.97)	0.87 (0.39)	-----
Integrity + Ability	-2.00 (0.05)	0.07 (0.95)	2.30 (0.02)	1.80 (0.07)
Drug Testing + Ability	3.03 (0.00)	-0.58 (0.56)	-2.25 (0.03)	-----
Ability + Police	-1.32 (0.19)	0.00 (1.00)	1.75 (0.08)	-----
Drug testing + Police	1.71 (0.09)	-0.65 (0.52)	0.63 (0.53)	2.31 (0.02)
Medical + Ability Testing	2.05 (0.04)	1.54 (0.13)	-----	-----
Medical + Genetic	-0.35 (0.73)	-0.36 (0.72)	1.58 (0.12)	1.95 (0.05)
Integrity + Drug Testing	1.74 (0.08)	-0.58 (0.56)	-0.47 (0.64)	-3.11 (0.00)
Financial + Police	-----	2.71 (0.01)	2.89 (0.01)	-2.91 (0.00)
Financial + Medical	-----	1.80 (0.08)	2.01 (0.05)	0.10 (0.92)
Financial + Drug testing	-----	2.68 (0.01)	-----	0.27 (0.79)
Financial + Genetic	-----	1.43 (0.15)	2.78 (0.05)	2.08 (0.04)
Transactional + Police	-----	1.59 (0.11)	1.65 (0.10)	-----
Transactional + medical	-----	0.50 (0.62)	0.00(1.00)	-2.23 (0.03)
Transactional + integrity	-----	2.50 (0.01)	2.89 (0.01)	0.60 (0.55)
Transactional + Ability	-----	2.21 (0.03)	-----	1.98 (0.05)
Transactional + Drug testing	-----	1.35 (0.18)	2.60 (0.01)	-2.35 (0.02)
Transactional + Genetic	-----	0.15 (0.88)	1.30 (0.20)	-0.21 (0.83)
Police + Genetic	-----	-1.61 (0.11)	-0.57 (0.57)	-----
Ability testing + Genetic	-----	-1.77 (0.08)	2.44 (0.02)	-2.41 (0.02)
Integrity + Genetic	-----	-1.66 (0.10)	-1.44 (0.15)	-0.78 (0.44)
Integrity + Medical	-----	1.66 (0.10)	2.83 (0.05)	2.70 (0.01)
Drug Testing + Medical	-----	0.92 (0.36)	3.17 (0.00)	0.17 (0.87)
Drug Testing + Genetic	-----	-1.29 (0.20)	-1.42 (0.16)	2.07 (0.04)

Figure III: Ranking concern levels about collection of different record types. Note: The graph is not drawn to scale. The boxes illustrate significant difference. Information types sharing a box are NOT significantly different from each other.

Figure IV: Ranking concern levels about unauthorised secondary use of different record types. Note: The graph is not drawn to scale. The boxes illustrate significant difference. Information types sharing a box are NOT significantly different from each other.

Figure V: Ranking concern levels about Errors in different record types. Note: The graph is not drawn to scale. The boxes illustrate significant difference. Information types sharing a box are NOT significantly different from each other.

Figure VI: Ranking concern levels about improper access to different record types. Note: The graph is not drawn to scale. The boxes illustrate significant difference. Information types sharing a box are NOT significantly different from each other.

Pair-wise t-tests indicate that there are significant mean concern differences between various record types in all four dimensions of privacy. For the collection of information, transactional and financial records appear to be the most and the library records the least sensitive types of information. Significant mean concern difference is also noted between other record types in this dimension. For example, there is a significant mean concern difference between genetic records and integrity, drug testing and police records, but the mean concern difference between genetic records and ability testing and medical records is not significant.

For unauthorised secondary use dimension, the mean concern about financial records is significantly higher than mean concerns for integrity testing, ability testing, and library records. Mean concerns about unauthorised secondary use of all record types are significantly higher than that about library records. No mean concern difference is noted for other record types.

Similar pattern is also seen in the case of concerns about errors in and improper access to different record types. Concerns for library records are significantly lower than concerns for other record types in both dimensions of concern. Mean concerns about errors in financial, police, medical, and drug-testing records are significantly higher than that about transactional, integrity testing, ability testing, and library records. Genetic testing records also appear to elicit higher concerns about errors than ability and integrity testing and library records but lower concerns than police records.

Mean concerns about the improper access to financial records are significantly higher than integrity and ability testing records and library records. Moreover, mean concerns about the improper access to medical and transactional records are significantly

higher than that about ability testing and library records. As with other three dimensions, mean concerns about library records are found to be significantly lower than concerns about all other record types.

Table 7.3-VI lists the results of pair-wise tests for mean concerns various organisations and their handling of personal information. As indicated, only those pairs that resulted in non-significant results are listed.

Table 7.3-VI: The result of pair-wise t-tests for organisation types (listing only the pairs that were NOT significantly different)		
Paired Differences (Organisation Types)	t	Sig.
Non-profit (Collection) - Government (Collection)	0.00	0.10
Non-profit (USU) - Government (USU)	1.14	0.26
For-profit (Errors) - Non-profit (Errors)	2.00	0.05
For-profit (Improper Access) - Non-profit (Improper Access)	1.60	0.11
For-profit (Improper Access) - Government (Improper Access)	-2.09	0.04

Note: (all other pair-wise tests were significant (<0.017))

Figure VII: Ranking concern levels about various organisations' collection of personal information. The graph is not drawn to scale. The boxes illustrate significant difference. organisation types sharing a box are NOT significantly different from each other.

Figure VIII: Ranking concern levels about various organisations' unauthorised secondary use of "personal information." The graph is not drawn to scale. The boxes illustrate significant difference. Organisation types sharing a box are NOT significantly different from each other.

Figure IX: Ranking concern levels about various errors in personal information that organisations have in their possession. The graph is not drawn to scale. Organisation types sharing a box are NOT significantly different from each other.

Figure X: Ranking concern levels about improper accesses to "personal information" in various organisations. The graph is not drawn to scale. Organisation types sharing a box are NOT significantly different from each other.

As illustrated above, mean concerns about collection and unauthorised secondary use to personal information are significantly higher when respondents are prompted to think about for-profit organisations. Mean concerns about errors in personal information, however, are higher when respondents are prompted to think about government organisations. Mean concern about improper access to personal information is significantly higher for government organisations than for non-profit organisations. In this dimension, no significant mean concern difference is noted between for-profit organisations and the other two organisation types.

Table 7.3-VII lists the results of pair-wise tests for perceptions about the safety of different storage technologies.

Table 7.3-VII: results of pair-wise t-tests for perception of safety of storage technologies		
Paired Samples Test	t	Sig. (2-tailed)
Manual + Database	2.29	0.02
Manual + Smart Card	-0.16	0.87
Database + Smart Card	-2.79	0.01

Note: Only the middle pair-wised test was NOT significant (>0.017)

Figure XI: Ranking individual's perception of safety of personal information when different storage technologies are used to store them. The graph is not drawn to scale. Storage technology types sharing a box are NOT significantly different from each other.

The above illustration indicates that smart cards and manual storage are perceived to be significantly safer technologies than databases for storage of personal information.

Table 7.3-VIII lists the result of pair-wise t-tests for ranking of different dimensions of privacy. This table lists only the results for pairs that were found not to be significant.

Table 7.3-VIII: The results of pair-wise t-tests for the four dimensions of privacy (listing only the results for pairs that were not significantly different)			
RECORDS	Paired dimensions	t	Sig
Financial Records	Errors + Collection	2.827	0.005
Transactional Records	Errors + Collection	1.814	0.072
Police Records	Improper Access + Unauthorised Secondary Use	1.944	0.054
	Improper Access + Errors	-1.131	0.260
	Errors + Unauthorised Secondary Use	0.305	0.761
Library Records	Improper Access + Unauthorised Secondary Use	-1.961	0.052
Medical Records	Errors + Unauthorised Secondary Use	-2.295	0.023
Integrity Records	Improper Access + Unauthorised Secondary Use	1.107	0.270
Ability Testing Records	Improper Access + Unauthorised Secondary Use	0.000	1.000
Drug Testing Records	Improper Access + Unauthorised Secondary Use	1.060	0.291
	Errors + Unauthorised Secondary Use	-1.643	0.103
	Improper Access + Errors	-2.229	0.027
Genetic Information	Improper Access + Unauthorised Secondary Use	1.493	0.138
ORGANISATIONS			
For-profit Organisations	Improper Access + Unauthorised Secondary Use	1.026	0.307
	Errors + Collection	0.572	0.568
Non-profit Organisations	Improper Access + Unauthorised Secondary Use	2.542	0.012
Government organisations	Errors + Unauthorised Secondary Use	0.396	0.693

Note: all other pair-wised tests were significant (<0.0083)

Figure XII: Ranking of dimensions of concerns with respect to different information types. The graph is not drawn to scale. Dimensions sharing a box are NOT significantly different from each other.

Figure XIII: Ranking of dimensions of concern with respect to organisation types. The graph is not drawn to scale. Dimensions sharing a box are NOT significantly different from each other.

As illustrated above, mean concerns about improper access to information are significantly higher than those for unauthorised secondary use, errors and collection when respondents were prompted to think about financial records, transactional records and medical records. Mean concerns about improper access to information and unauthorised secondary use of information are significantly higher than those for errors in information and collection of information when respondents were prompted to think about genetic records, integrity and ability testing records, and library records. Moreover, mean concerns for collection of information are found to be the least important to respondents, except in the case of genetic records where they were the second lowest concerns and in the cases of financial and transactional records where they were as low as concerns for errors in information.

When respondents are prompted to think about different organisation types, mean concerns about the improper access to personal information are significantly higher than other concerns. In the case of for-profit and non-profit organisations mean concerns about improper access to and unauthorised secondary use of personal information are found to be significantly higher than collection of and errors in personal information. Collection is found to be the lowest concern when respondents think about government organisations and non-profit organisations and the lowest concern along with errors in personal information in the case of for-profit organisations.

8.0 Conclusions

As we are entering the new millennium, information privacy continues to be a grave concern of many people. Current laws and regulations inadequately address these concerns and fail to consider all nuances of privacy. Information privacy research will provide the information necessary for proactive management of sensitive information. Responsible organisations can utilise this type of research for ethical conduct in management of information to alleviate privacy concerns and to win consumer loyalty and trust.

The main thrust of this thesis was the exploration of dimensions and context sensitivity of information privacy concerns. The major conclusions relating to each of the research hypotheses are discussed below.

8.1 Conclusions Related to Group Differences

The first two hypotheses suggested that individuals of different age and education exhibit different levels of concern about information privacy. The results of this study, however, demonstrated that individuals in the study population were not significantly different based on age and education and with respect to study variables. Some explanation may be given for the similarity of students and faculty members with respect to information privacy concerns. Individuals in both groups are exposed to similar media for receiving information. Internet, daily newspapers, television, academic articles, course materials, and other sources provide both groups with similar information. Media

coverage is a moderating variable that was not examined in this study. Including this variable in the research model could provide a better understanding of group differences.

Although group differences could not be demonstrated in the study population, age and education should be considered when studying populations that include people from different levels of society. As indicated earlier, the experience with opinion polls suggests that age and education are important demographic variables that are worthy of consideration in this type of studies. Using individual grouping based on age (i.e., under 25 years of age, 26 to 34, 35 to 44, and so on) or education (i.e., based on number of years of schooling) may also provide future research with a better understanding of these variables.

8.2 Conclusions Related to Information Types

In this study, Information types were divided into two categories: personality information and performance information. Hypothesis 3a suggested that in the personality category of information, for all dimensions of concern, genetic records provoked more concerns than ability-testing and integrity-testing records. Although mean concerns were always higher for genetic records than for the other two, it was not possible to show statistical significance in all cases. Concerns about collection of genetic records were significantly higher than that for integrity-testing records. In addition, concerns about errors in, and improper access to genetic records were significantly higher than that for ability-testing records. No significant difference, however, was noted between concerns about the unauthorised secondary use of different personality type

records. Individuals' concerns in this dimension were equally high for all personality type records.

Hypothesis 3b proposed that in performance category of information, for all dimensions of concern, financial records followed by medical records and transactional records provoke the highest levels of concern. As with hypothesis 3a, this hypothesis was only partially supported. Individuals exhibited very high concerns for financial, transactional and medical records in all dimensions of concern; however, concerns about these record types were not found to be significantly higher than that for other records. For example, concerns about collection of financial and transactional records followed by concerns about collection of medical and police records were significantly higher than that for other record types in this category of information. Individuals also exhibited high levels of concern for unauthorised secondary use of financial, transactional, and medical records. However, these concerns were not significantly higher than concerns for drug-testing and police records.

Hypothesis four suggested that there might be higher concerns for performance than for the personality category of information. This hypothesis was also partially supported. It was not possible to significantly differentiate concerns about unauthorised secondary used of and improper access to genetic records from that about other types of records. In addition, library records always prompted the least amount of concern, which made it difficult to fully support this hypothesis.

When investigating concerns about information privacy, previous studies and opinion polls were found to ignore the variety in information types about which people are generally concerned. Different types of information were found lumped together as a

single item, referred to as "personal information." One objective of this research was to determine whether in fact people demonstrated different levels of concern, when they were prompted to think about different types of information. Based on earlier findings, hypotheses 3a, 3b, and 4 were used to test the context sensitivity of concerns with respect to information type. Despite high levels of concern for all record types leading to some difficulty in significantly differentiating these concerns, it was demonstrated that in fact individuals exhibit varying levels of concern when prompted to think about different types of information. It became evident, for example, that individuals are least concerned about the privacy of their library records than any other record types. In addition, individuals demonstrated significantly higher concerns for some types of records than others in every dimension of concern. A useful conclusion is that when examining concerns about information privacy, one should avoid using a general term such as "personal information" in information privacy studies. Using this term is likely to provide inaccurate results.

8.3 Conclusions Related to Organisation Types

Hypothesis five suggested that individuals exhibit varying levels of concern when they are prompted to think about different types of organisations handling various types of information. It suggested that for-profit organisations provoke the highest levels of concern, whereas non-profit organisations provoke the least amount of privacy concerns. Study results partially supported this hypothesis. Results indicated that the study population is very concerned about the collection of personal information by for-profit

organisations. It also indicated that they are highly concerned about the potential of unauthorised secondary use of the collected information by for-profit organisations. In these dimensions of privacy, however, no significant difference between non-profit and government organisations were noted. In errors and improper access dimensions of privacy concerns the hypothesis was not supported. Study population exhibited significantly higher concerns about governments than the other two types of organisations.

One explanation may be the following. Governments have been involved in information collection for many years. The fact that governments possess a large repository of personal information is well known by all citizens. Governments collect information for tax purposes, health care, employment benefits, and many justified or justifiable activities. In addition, people may be generally confident that governments do not transfer personal information to third parties. Individuals, however, exhibit most concerns when they are prompted to think about the potential for errors in their personal information that is at government's disposal. This is also true when individuals' attention is directed to the possibility of improper access to their personal information held by government organisations.

For-profit and non-profit organisations, on the other hand, are not universally recognised as keepers of personal information. For this reason, when prompted to think about for-profit organisations, individuals voice concerns about practices such as information collection and unauthorised exchange of personal information with third parties.

An important conclusion is that the level of concerns of individuals is in fact sensitive to organisation types about which they are prompted to think. This conclusion is in conformance with previous research that supported this context sensitivity.

8.4 Conclusions Related to Storage Technology Types

This thesis was also interested in perceived safety of information when different technologies were used for information storage. Hypothesis number 6 suggested that individuals exhibit various levels of concern about the safety of information stored using different technology types. The results indicted that databases are perceived as the least safe method of information storage.

Currently, databases are universally used to store information. One explanation for significantly lower perception of safety of databases may be their popularity. Databases are everywhere. Information is now being collected on millions of computer databases around the world. As a result, people are well aware or at least more cognisant of potential problems with databases and misuses of information that databases store. Smart cards, on the contrary, are still unknown to many. Most people have not used them and have limited information about them. Furthermore, potential problems with smart cards have not yet been publicly revealed. These may be some factors that contribute to significantly higher perception safety for this technology.

8.5 Conclusions Related to Concern Dimensions

Earlier cross-cultural research (Milberg, et al 1995) had indicated no significant difference in the relative importance or hierarchy of concerns across nationalities. This study had demonstrated that secondary use was the highest concern dimension in seven of nine countries (including Canada), followed by improper access, collection and errors respectively. As a follow-up to Milberg (1995), hypotheses 7 and 8 of this thesis expected to find a similar hierarchy of concern dimensions given that study population was prompted to think about different organisation or information types.

The results did not entirely support Milberg's cross-cultural study. In almost all cases collection of information was found to induce the least amount of concern. Concerns about the improper access to financial, transactional and medical records were found to be significantly higher than that for their unauthorised secondary. In addition, concerns about the improper access to information were found to be significantly higher than the secondary use of information when individuals were prompted to think about government organisations.

Failure to support earlier research can be contributed to the fact that Milberg et al., studied concerns about "personal information" as a general term. This insensitivity to context sensitivity of privacy concerns may have produced misleading results. When exposed to privacy concern questions, each respondent may respond based on a context that may be quite different than that for other respondents. The results of this study indicate that although a hierarchy of concern dimension is present, the ranking order is dependent on the context to which respondents are prompted to think about.

9.0 Research Benefits

Protecting the public's privacy is not only morally and socially responsible, but also financially profitable for organisations. Companies that engage in ethically proactive management of personal information will gain a competitive advantage over companies that handle sensitive information carelessly. This advantage is gained by way of winning consumers' trust and respect, which can be translated to customer loyalty and financial gains (Cavoukian and Tapscott, 95). Building consumers trust is also likely to entice a more accurate flow of information that could reduce marketing efforts and budgets (Cavoukian and Tapscott, 1995). Ethical handling of personal information will also lead to a reduction in litigation costs and a more flexible regulatory environment.

Employees and managers can also benefit from ethical handling of personal information. There have been reports of value conflicts when employees attempt to reconcile their own values with company values and policies with respect to privacy issues (Smith et al., 1996). Such ethical conflicts often result in a cognitive or emotional dissonance. Ethical practices relieve employee anxiety and increase confidence and trust in the organisation (Smith et al., 1996).

As a first step to proactive management of personal information, managers and executives can identify existing problems and take corrective actions to rectify problem areas. Exploring the theoretical linkages proposed in this research would pave the way for interpretative field studies that examine proactive management of sensitive information to protect the public's information privacy.

10.0 Research Limitations

This study suffers from a number of limitations. The four-dimension model of the construct reflects the majority views and perceptions of the respondents in a US study. Perceptions are dynamic and conditional and only reflect current thinking. They not only shift over time, but may also vary across different cultures. Since this study sought the views of a specific group of Canadian subjects, the instrument utilised may not have addressed the central dimensions of the construct and may have served as a limitation to the study.

The second limitation that may have influenced the outcome of the study is the omission of a number of variables including “personality factors,” “media coverage,” in the study model. These factors may act as moderating variables to influence the levels of concern.

Due to time and resource limitations constraints were imposed on the sampling procedures. Ideally, the author would have liked to target the Canadian population as a whole. However, taking a representative sample from this population was not possible at this level of research. Thus, the study was delimited to the university population.

The number of questions in the questionnaire was also a limiting factor. The questionnaire had to be shortened to encourage response. Despite all measures taken to increase response, non-response remains a limiting factor.

11.0 Bibliography

Altman, I., "Privacy: A conceptual analysis." In D.H. Carson (Ed.), *Man-environment interactions: Evaluations and applications* (Part II, Vol.6: S.T. Margulis, Vol. Ed.). Washington D.C.: Environmental Design Research Association, 1974, and in Stroudsburg, PA. : Dowden, Hutchinson, and Ross, 1975.

Annas, G. J., Leonard H. Glantz, and Patricia A. Roche, "Drafting the genetic privacy act: Science, policy, and practical considerations," *The Journal of Law, Medicine, and Ethics*, Vol. 23, 1995, pages 360-366.

Asch, David A., and Michael T. Mennuti, "Genetic Tests: Evolving Policy Questions," *IEEE Technology and Society Magazine*, winter 1996/1997, Pages 4-10.

Baker, J.A. "Personal Information and Privacy," In *proceedings of the First conference on computers, Freedom and Privacy*, J. Warren, J. Thorwaldson, and B. Koball (eds.), IEEE Computer Society Press, Los Alamitos, CA, 1991, Pages 42-45.

Bennett Colin, J., "Protecting privacy on the Canadian information highway: policy developments and regulatory options," *Canadian Journal of Information and Library Science* Vol. 21, No. 3/4, September-December 1996.

Berscheid, E. "Privacy: A hidden variable in experimental social psychology," *Journal of Social Issues*, Vol. 33, No. 3, 1977, pages 85-101.

Bible J. D. and D. A. McWhirter, "Privacy in the workplace: A guide for human resource managers," Quorum Books, 1990.

Billings, P. R., M. A. Kohn, Margaret de Cuevas, J. Beckwith, J. S. Alper, and M. R. Natowicz, "Discrimination as a consequence of genetic testing," *American Journal of Human Genetics*, Vol. 50, 1992, pages 476-482.

Bloustein, E., "Privacy as an aspect of human dignity: an answer to Dean Prosser'," *New York University Law Review* 39, 962-1007.

Brod, C., "Technostress." Addison-Wesley. Reading, MA, 1984.

Brown, William, S., "Technology, Workplace Privacy and Person-hood," *Journal of Business Ethics*, 1996, vol. 15, pages 1237-1248.

Burnham, David, "Data protection" in *Computers, Ethics, and Society* edited by M. D. Ermann, M. B. Williams, and C. Gutierrez, Oxford University Press, 1990.

- Burris, B. H., "Technocracy at work." University of New York Press, Albany, New York, 1993.
- Cavoukian, Ann, and Dan Tapscott, "Who Knows: Safeguarding Your Privacy in a Networked World," Random House of Canada, 1995.
- Cespedes, F. V., Smith, H. J., "Database marketing: New rules for policy and practice," Sloan Management Review, summer 1993, Pages 7-22.
- Clarke, R. A., "Information Technology and Dataveillance," Communications of the ACM, Vol. 31, No. 5, May 1988, pages 498-512.
- Cohen, J., "Statistical power analysis for the behavioural sciences." Revised Edition, Academic Press, New York, NY, 1977.
- Coombs, Robert, H. and Louis Jolyon, West "Drug Testing: Issues and options." Oxford University Press Inc., 1991.
- Cozby, P.C., "Self-disclosure: A literature Review," Psychological Bulletin, Vol. 79, No. 2, February 1973, pages 73-91.
- Culnan, Mary J. "How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use." MIS Quarterly, September 1993 pages 341-363.
- Cushman, Reid, "Information and Medical Ethics: Protecting Patient Privacy," IEEE Technology and Society Magazine. Fall 1996, pages 32-38
- Date, C. J., "An introduction to database systems." Fourth Edition, Addison-Wesley Publishing Company, Reading, MA, 1986.
- Davidson Tim, and Jeanette R. Davidson, "Cost containment, computers, and confidentiality." Clinical Social Work Journal, Vol. 23, No.4, winter 1995, Page 453.
- Davies, S. G., "Touching big brother: How biometric technology will fuse flesh and machine," Information Technology and People, Vol. 7, No. 4, 1994.
- DeJong, J., "Smart Marketing," Computer World, 7, February 1994, 113,117-118.
- Draper, Elaine, "Risky Business: Genetic testing and exclusionary practices in the hazardous workplace," Cambridge University Press, 1991.
- Duster, Troy, "Back door to eugenics." New York: Routledge, Chapman, and Hall, 1990.
- Ekos Research Associates, "Privacy revealed: the Canadian privacy survey." Ottawa: Ekos Research Associates, 1993.

Equifax, Inc., Harris, Louis, and Alan F. Westin "The Equifax Canada reports on consumers and privacy in the information age. Ville d'Anjou: Equifax Canada Inc., 1995.

Equifax, Inc., Harris-Equifax Consumer Privacy Survey, 1991. National opinion survey conducted by Equifax, Inc., L Harris and Associates, and Alan. F. Westin, 1991.

Equifax, Inc., "The Equifax report on consumers in the information age." National opinion survey conducted by Equifax, Inc., by L. Harris and Associates and A.F. Westin, 1990.

Ellul, J., "The Technological Society." Translated by John Wilkinson. Vintage Books, New York, 1964.

Ermann M. David, Williams, Mary B., and Claudia, Gutierrez, "Computers, Ethics, and Society." Oxford University Press, 1990.

Flaherty David, H. "Protecting privacy in surveillance societies," Chapel Hill: University of California Press, 1989.

FNACQ/PIAC (Fédération nationale des associations de consommateurs du Québec / Public Interest Advocacy Centre) "Surveying Boundaries: Canadians and their personal information" Ottawa and Montreal, 1995.

Fox Jeffrey L. "Will genetic tests and computers invade privacy?" Biotechnology Vol. 11, December 1993, page 1512.

Frawley W., G. Pieatetsky-Shapiro, and C. Matheus. "Knowledge Discovery in Databases: An Overview." AI Magazine, fall 1992, pages 213-228

Freedman W., "The right of privacy in the computer age." Quorum Books 1987.

Fromm, E., "The revolution of hope: Toward a humanised technology," Bantam Books, 1968.

Fusilier, Marcelline R., and Wayne D. Hoyer "Variables affecting perceptions of invasions of privacy in personnel selection situation," Journal of Applied Psychology, 1980, Vol. 65, No. 5, pages 623-626.

Gandy, Oscar H., Jr., "The Panoptic Sort: A political economy of personal information." Boulder: West view Press, 1993.

Ganster D. C., and ... "Information privacy in organisations: An examination of employee perceptions and attitudes," Proceedings of the 39th annual conference of the National Academy of Management, 1979, pages 262-266.

Goodwin, Cathy, "Privacy: Recognition of a consumer right," *Journal of Public Policy & Marketing*, 1991, 10 (1), pages 149-166.

Gostin Lawrence O., "Genetic Privacy." *The Journal of Law, Medicine and Ethics*, 1995, Vol. 23, pg. 320-330.

Grupe Fritz H., "Commercialising public information: A critical issue for Governmental IS professionals." *Information and Management*, Vol. 28, 1995, pages 229-241.

Harris, Louis, and Alan F. Westin, "The Equifax Canada reports on consumers and privacy in the information age. Ville d'Anjou: Equifax Canada, 1995.

HEW (U.S. Department of Health, Education, and Welfare), "Records, computers, and the rights of citizens: Report of the secretary's advisory committee on automated personal data systems." U.S. Government Printing Office, Washington, D.C., 1973.

Huberty, C. J., and J. D. Morris, "Multivariate analysis versus multiple univariate analyses," 1996.

Information Highway Advisory Council (IHAC). "Connection, community, and content: the challenge of the information highway." 1995. Ottawa: Minister of Supply and Services Canada.

Kelman C. Herbert, "Privacy and research with human beings." *The Journal of Social Issues*, Vol. 33, No. 3, 1977.

Kevles, Daniel J., "In the name of eugenics: Genetics and the uses of human heredity," New York: Alfred A Knopf, 1985.

Kling, Rob, Isaac Scherson and John Allen, "Massively parallel computing and information capitalism." In W, Daniel Hillis and James Bailey's, "A new era of computing, Cambridge, The MIT Press, 1992.

Kling, Rob, Mark S. Ackerman, and Jonathan P. Allen, "Information Entrepreneurialism, Information Technologies, and the Continuing Vulnerability of Privacy," Draft (4.4) for "Computerisation and Controversy: Value Conflicts and Social Choices. 2nd edition, academic press, 1995," <http://www.swiss.ai.mit...icics/kling-privacy.txt>, December 27, 1994.

Krier, J.E. and Ursin, E. "Pollution and Policy: A case study on California and Federal Experience with Motor Vehicle Air Pollution," 1940-1975. University of California Press, Berkeley, California, 1977.

Kusserow, Richard P., "The government needs computer matching to root out waste and fraud." *Communications of the ACM*, June 1984, Vol. 27, No. 6, pages 542-545.

Larson, Erick, "The Naked Consumer: How our private lives become public commodities," Henry Holt, New York, 1992.

Lauden, Kenneth, C., "Dossier society: Value choices in the design of National Information Systems," New York Columbia university press, 1986.

Laufer Robert S., and Maxine Wolfe. "Privacy as a concept and a social issue: A Multidimensional Developmental Theory." *Journal of Social Issues*, Vol. 33, No. 3, 1977, pages 22-41.

Levin, H. A., and F. Askin, " Privacy I the courts: Law and social reality," *The Journal of social Issues*, Vol. 33, No. 3, 1977, pages 138-153.

Linowes David F., "Privacy in America: Is your private life in the public eye?" University of Illinois Press 1989.

Linowes David F., "Your personal information has gone public." *Illinois Quarterly* (6) 2, pages 22-24.

Lipinski, Tomas A. "The economics of personal information: privacy and information in the consumer marketplace," *Canadian Journal of Information and Library Science*, 1996, Vol21 #3-4, page 86.

Louis Harris & Associates and Dr. Alan F. Westin, "The Equifax report on consumers in the information age (For Equifax Inc., 1990)." This poll was conducted between January 11 and February 11 and between April 20 and April 30, 1990.

Margulis, S. T. " Preface to Privacy" In D.H. Carson (Ed.), *Man-environment interactions: Evaluations and applications* (Part II, Vol.6: S.T. Margulis, Vol. Ed.). Washington D.C.: Environmental Design Research Association, 1974; and in Stroudsburg, P.A.: Dowden, Hutchinson, and Ross, 1975.

Martin, Elaine R., In Review of "Protecting privacy in computerised medical information" by U.S. Congress, office of technology assessment, Washington D.C., (1993). *Government Information Quarterly*, 1995, Vol. 12, No. 1, page 132.

Mason, R. O. "Four ethical issues of the information age," *MIS Quarterly* Vol. 10, No. 1, March 1986, Pages 4-12.

McKusick, V.A., and J. S. Amberger, "The morbid anatomy of the Human Genome: Chromosomal location of mutations causing diseases." *Journal of medical genetics*, 1993, 30:1-26.

Milberg, S. J., Burke, S. J., Smith, H. J., and E. A. Kallman, "Values, personal information privacy concerns, and regulatory approaches," *Communications of the ACM*, Vol. 38, No. 12, December 1995, pages 65-74.

Miller, A. "Computers and privacy," in *Ethics and the Management of Computer Technology*, W. M. Hoffman, and J. M. Moore (eds.), Oelgeschlager, Gunn, and Hain Publishers Inc., Cambridge, MA, 1982.

Morgan, J.P. "Problems of mass urine screening for misused drugs," *Journal of Psychoactive Drugs*, 1984, 16(4), pages 305-317.

Morris, S., J., Cooper, D., Bomba, L. Brankovic, M. Miller, and F. Pacheco, "Australian healthcare: A smart card for a clever country," *International Journal of Bio-medical Computing*, Vol. 40, 1995, pages 101-105.

Nock, S. L., "The costs of privacy: Surveillance and reputation in America," Aldeline De Gruyter, Hawthorne, NY, 1993.

O'Brien David M., "Privacy, law, and public policy." New York Praeger 1979 page vii.

O'Conner Kevin, "Privacy and Profiling. Information Paper No.2. Privacy Commissioner, Human Rights Australia."
<http://www.austlii.edu.au/au/other/hreoc/privacy/profil2.htm>

Oleck Howard L., "Non-profit corporations, organisations, and associations." Third Edition, Prentice-Hall Inc., 1974.

PPSC (Privacy Protection Study Commission), "Personal privacy in an information society: report of the Privacy Protection Study Commission," U.S. Government Printing Office, Washington, D. C., 1977.

Privacy Commissioner of Canada, 1997. Annual report, 1996-1997. Ottawa: Canada Communications Group.

Privacy Commissioner of Canada, 1996. Annual report, 1995-1996. Ottawa: Canada Communications Group.

Privacy Commissioner of Canada (Phillips), 1995. Annual report, 1994-1995. Ottawa: Canada Communications Group.

Privacy Commissioner of Canada, 1994. Annual report, 1993-1994. Ottawa: Canada Communications Group.

Regan, Priscilla M. "Legislating Privacy: Technology, Social values, and Public Policy." The University of North Carolina Press. 1995.

Reily W. D., "Big Brother," *Datamation*, January 15, 1996, page 22.

Rosenbaum, B. L. "Attitude toward invasion of privacy in the personnel selection process and job applicant demographic and personality correlates." *Journal of Applied Psychology*, 1973, Vol. 58, Pages 333-338.

Rosenberg Richard, S. "Social impact of computers: Privacy and freedom of information," Academic Press Inc., 1992.

Ruebhausen, O. M., and Brim, O. G., Jr. "Privacy and behavioural research." *Columbia Law Review*, 1965, 1184-1211.

Rotenberg, M., in a review of "The right to privacy" by Ellen Alderman and Caroline Kennedy, NY (1995). *Government Information Quarterly*, Vol. 13, No. 2, 1996, Pages 11-12.

Schoechle, Timothy D. "Privacy on the information superhighway: Will my house still be my castle?" *Telecommunication Policy*, 1995, Vol. 19. 6, pages 435-452.

Schultz, E. E., "Open Secrets: Medical data gathered by firms can prove less than confidential." *The Wall Street Journal*, May 18, 1994, pages 1-5.

Shattuck, John, "Computer matching is a serious threat to individual rights." *Communications of the ACM*, June 1984, Vol. 27, No. 6, pages 538-541.

Shils, E.B., "Privacy: Its constitution and vicissitudes." *Law and Contemporary problems*, 1966, 31, 281-306.

Simon, H.A., "What computers mean for man and society," *Science* 195, March 18, 1977, pages 1186-1191.

Singer, E., N. A. Mathiowetz, and M. P. Couper, "The impact of privacy and confidentiality concerns on survey participation: The case of the 1990 U.S. census," *Public Opinion Quarterly*, Vol. 57, pages 465-482, 1993.

Smith, Jeff "Privacy policies and practices: Inside the organisational Maze," *Communications of the ACM*, December 1993, Vol. 36, No. 12, pages 105-123.

Smith, Jeff "Managing Privacy: Information technology and corporate America," Chapel Hill and London: The university of North Carolina Press, 1994.

Smith, H. Jeff, Milberg Sandra J., and Sandra J. Burke, "Information Privacy: Measuring individuals, concerns about organisational practices," *MIS Quarterly*, June 1996, Pages 167-196.

Stopher Peter, R., and Arnim, H., Meyburg, "Survey sampling and multivariate analysis for social scientists and engineers." Lexington Books. 1979.

Stone, E. F., Gardner, D. G., Gueutal, H. G., and McClure, S. "A field experiment comparing information-privacy values, beliefs and attitudes across several types of organisations," *Journal of Applied Psychology* (68:3), August 1983, pages 459-468.

Stone, D. L., "Relationship between introversion/extroversion, values regarding control over information, and perceptions of invasion of privacy," *Perceptual and Motor Skills*, Vol. 62, No. 2, April 1986, pages 371-376.

Stone, E. F., and Stone, D. L. "Privacy in organizations: Theoretical issues, Research findings, and protection mechanisms," in *Research in Personal and Human Resources Management*, Vol. 8, K.M. Rowland and G.R. Ferris (eds.), JAI Press, Inc., Greenwich, CT, 1990, Pages 349-411.

Straub, D. W. And Collins, R. W. "Key information liability issues facing managers: software piracy, proprietary databases, and individual rights to privacy," *MIS Quarterly*, Vol. 14, No. 2, 1990, Pages 143-156.

Thompson Steven, K., "Sampling." John Wiley and Sons, Inc., New York, 1992.

Tolchinsky, P. D., McCuddy M. K., Adams, J., Ganster, D. C., Woodman, R. W., and H. L. Fromkin, "Employee perceptions of invasion of privacy: A field experiment," *Journal of Applied Psychology* (66:3), June 1981, pages 308-313.

Toothaker, L. E., "Multiple Comparisons for Researchers," Sage Publications, 1991.

Tryfos, Peter, "Sampling methods for applied research: Texts and cases." John Wiley and Sons, Inc., New York, 1996.

Uncles Allison, "Harris backs drug testing at nuclear plants. Union no longer adamantly opposed to mandatory checks on members." *Ottawa Citizen*, Thursday Aug 21, 1997, pages A1-A2.

Warren, C., and Barbara Laslett, "Privacy and secrecy: A conceptual comparison," *Journal of Social Issues*, Vol. 33, No. 3, 1977.

Warren S., and Brandeis L., ... *Harvard Law Review* 1890.

Watson Richard T., "Data Management: An organisational Perspective." John Wiley and Sons Inc., 1996.

Westin, A. "Privacy and Freedom." New York: Atheneum, 1967.

Westin, A. F., and M. A., Baker, "Databanks in a free society," Quadrangle Books, New York, 1972.

Westin, A. F., "Consumer privacy issues in the nineties," in the Equifax Report on consumers in the information age, Equifax Inc., Atlanta, GA, 1990, pages XVIII-XXVIII.

Westin, A. F. and Arthur R. Miller, "The assault on privacy: Computers, Data Banks, and Dossiers," Ann Arbor: University of Michigan Press, 1971.

Willis, H. W., "The new faces of privacy," Information Society, 1993, pp 195.

Woodman, R. W., Ganster, D. C., Adams, J., McCuddy, M. K., Tolchinsky, P. D., and H. Fromkin, "A survey of employee perceptions of information privacy in Organisations," Academy of Management Journal (25:3), October, 1982, pp. 647-663.

12.0 Appendices

12.1 Appendix A: Performance Information

i) Financial Records

Financial records may include all information about one's finances. Bank account balances, household incomes, debts, credit card balances and payments, and mortgages are some of the information that may exist in one's financial records. Credit bureaux usually have the updated account of most individuals' finances. They usually have credit histories – recorded as on time, occasionally late, consistently late – income, mortgages, liens, and bankruptcies along with personally identifying information. The majority of people, particularly the people who live in North America, consider their financial information to be very sensitive and refuse or hesitate to disclose it upon request (Smith, 1993).

ii) Transactional Records

Transactional records or “Transactional Information” (Burnham, 1983) include all records generated using personally identifiable means of purchase – credit cards, cheques, Bankcards, etc. – or other electronic transactions that leave a digital footprint. This category of information is automatically collected and stored in databases and can be retrieved on command. Its potential to reveal information about a person's interests, attitudes, habits, tastes, and whereabouts makes it an important tool that serves various corporate and government purposes.

As a cost reduction tool, for example, the analysis of transactional information enables organisations to reduce costs and increases profits through target marketing and data base marketing. Based on the assumption that "people are what they purchase," by

studying one's purchasing patterns, it may be possible to identify one's habits and preferences. Targeting selectively, based on one's past buying habits, will increase business by targeting solid leads and avoiding wasteful advertising to poor prospects (DeJong, 1994).

As a surveillance tool, transactional records enable governmental organisations to track suspicious movements of criminals. In addition, these records are useful in the courts of law as evidence for, for example, placing a criminal at the scene of a crime. Using these records it may also be possible to track the activities of corporations and ethnic or economic groups. Moreover, because of the universal reach of transactional information, it is possible to globally monitor the activities of individuals, groups or corporations.

iii) Police Records

Police records consist of records of arrests, convictions, warrants, bails, paroles, court judgements, driving accidents, motor vehicle registrations, and information about any other type of interactions with the police. The major concern about police records arises from poor security that permits unauthorised or improper access to these records. Moreover, the incompleteness or incorrectness of police records may be problematic, as it may or may not, for example, properly reflect the outcome of one's arrest to indicate exoneration or guilt (Burnham, 83). This could be troublesome, particularly to those vindicated of a crime. Police records may also be misused in making stereotypic or discriminatory decisions about individuals based on arbitrary criteria. An example is the text and photo database of California's Orange County sheriff's department, which was constructed in 1994 to help crush the growing trend of ethnic violence. This database

included the names of many teenagers of Hispanic or Asian descent who wore a particular type of clothing, known to be the colours of an infamous gang, which was in fashion at the time, to school (Kling, 94). More alarming is the use of criminal records for employment purposes. Ermann (1990) reported “in New York the use of criminal records by law enforcement agencies has declined in recent years, while its use by private employers has gone up.” Using an experiment by Richard Schwartz and Jerome Skolnick as evidence, Ermann argued, “Some employers assume that any kind of record, no matter what the offence, no matter what the outcome, is a powerful mark against the individual.” The experiment, carried out in the 1960s, had attempted to measure this type of bias in employment situations. The investigators had found that thirty six percent of employers were willing to offer jobs to those with no records. Twenty four percent of the employers were ready to hire those who had been acquitted and had a letter from the judge, and twelve percent of employers accepted to hire individuals who had been acquitted but had no letter. In contrast, only four percent of employers were willing to hire individuals who had been convicted of a crime (Quoted in Ermann, 1990). The evidence suggests that the impact of criminal records is powerful, even if the individual in question is acquitted.

iv) Library Records

Library records are personal records stored in public, university, or other libraries. These records, in addition to personally identifiable demographics, contain information on the reading habits of individuals. In other words, they contain the names of books and other items that individuals borrow from a library.

The major concern with respect to library records relates to secretive government practices. For instance, in the United States, organisations of librarians, authors, and civil

libertarians have indicated their concerns about the practices of the Federal Bureau of Investigation (FBI). FBI in a so called “Library Awareness Program” actively looked into what types of books people are reading, who the readers are, and even with whom the readers are associating. This program was directed at the public libraries to collect information on “seemingly suspicious requests by readers to reveal the names of people who may be helping soviet agents to obtain information” (New York times, 1988 quoted in Rosenberg, 1992).

v) Medical Records

Medical technologies and medical information systems have made astonishing leaps over the past two decades. Although a large administrative part of the medical information systems remains paper intensive, advances in computer technology have now made possible the total shift from paper to a more efficient computerised record keeping health care system (Cushman, 1996; Martin, 1995). As part of this trend, hospitals, drug companies and other users of medical records collect and store a large number of records in their databases (Cushman, 1996). And with every technology that is introduced for the computerisation of health care systems – be it in the name of “efficiency” or “providing better services to customers”– organisations collect more medical records in their databases (Cushman, 1996; Cavoukian and Tapscott, 1995).

Medical records are extremely intimate and personal. In addition to diagnostic and testing information about patients, they contain personally sensitive information such as medical, family, financial, and employment histories, marital status, disabilities, drug and alcohol related experiences, psychological and mental status, recreational habits, and even sexual orientations of patients (Regan, 1995; Cushman, 1996). Although the

computerisation of these records simplifies and improves the efficiency of information collection, it also adds new dimensions to the potential for invasion of privacy. It brings personal risks through increased unauthorised or improper access, and increased number of errors in medical information stored in databases (Cushman, 1996). The adverse consequences of this phenomenon can be devastating for individuals. Once in the public domain, one's personal information may affect that person's ability to obtain or to maintain employment, insurance, education, or housing. It may cause humiliation, expulsion, discrimination, or unjust incrimination.

Physicians have acknowledged the sanctity of medical records for centuries. In fact, the "need to know" basis has played a major role in the protection of information, from disclosure to unauthorised third parties, for hundreds of years. This respect is evident from the Hippocratic oath, upon which today's codes of ethics are founded. "...What I see or hear in the course of treatment or even outside of the treatment in regard of the life of men, which no account one must spread about, I will keep to myself such things shameful to be spoken about" (Hippocratic oath quoted in <http://www.hipocreatic2.html>).

However, the amount of information and types of information that the third parties receive are no longer restricted. All medical files have become "open secrets" (Schultz, 1994) that are easily seen by insurance companies and others alike (Davidson and Davidson, 1995). "...In order to be reimbursed and have visits approved, psychotherapists may be required to report to insurance companies such details as how often their clients masturbate and whether they still drink too much or are thinking about suicide" (Schultz, 1994 – quoted in Davidson and Davidson, 1995).

It is unnerving to find that, aside from one's physician, as many as 75 unintended people have access to one's medical information (Linowes, 1989). A 1977 position statement by The American Records Association listed 12 broad categories of those with access to medical information (Regan, 1995). This list, termed the "social users of medical information," included public health agencies, medical and social researchers, employers, social welfare staff, insurance companies, governmental organisations, educational institutions, law enforcement agencies, credit investigation agencies, and the media (Regan, 1995). During government audits patients' medical records may be exposed to an even greater number of individuals, which include inspectors, members of review committees and lawyers to name a few (Cavoukian and Tapscott, 1995).

Direct marketers are yet another group of people that may gain access to medical information (Cavoukian and Tapscott, 1995). This group, however, gains access mainly through personally volunteered information (Regan, 1995). Some may even resort to illegal means of obtaining information when legitimate routes are not readily available. In his article "your personal information has gone public," David Linowes (1993) reports a private investigation agency as training their agents to impersonate physicians to acquire information. He also reports nurses who were paid as informants to leak out information. The illegal means of obtaining medical information claim a 99% success rate as the agency boasts (Linowes, 1993).

Furthermore, organisations that collect and store medical records are constantly pressured by external sources to share them (Smith, 1994). For example, the management of an organisation providing life or medical coverage for its employees may obtain information from the insuring company and, intentionally or unintentionally, use it to

discriminate against some employees. Those who test positive for a transmittable disease such as AIDS, for example, would be easy targets for discrimination. Smith quotes an employer as having said, “ I am going to fire everyone of those sons of b... (SOBs)” (Smith, 1994).

Insurance companies routinely receive and store massive amounts of information as part of their daily business practice. Information transfer in this industry has become so common and ubiquitous that privacy violation is sanctioned as the norm (Davidson and Davidson, 1995). The files of “The medical Information Bureau” (MIB)¹ contain medical records of over 12 million people (Cavoukian and Tapscott, 1995; Linowes, 1989). Member companies disclose all significant information, regardless of means by which it is obtained, and retrieve information as the need arises (Linowes, 1989). Although MIB has certain rules for the use of this information, there are no enforceable means of controlling the consequences for the individual (Linowes, 1989). Moreover, these files, undoubtedly prone to errors, may be used over and over again, spreading and possibly aggravating the errors with every transmission. More alarming is that, even if one became aware of the errors in one’s own file, it would be very difficult, if not impossible, to have the erroneous information corrected or removed through personal requests (Cavoukian and Tapscott, 1995).

Contrary to common beliefs, there are practically no medical privacy laws in Canada to protect individuals against privacy invasions (Cavoukian and Tapscott, 1995). Unlike some major sectors of commerce that fall within the federal jurisdiction – Such as telecommunications, transportation, and banking – health care is provincially regulated.

Thus, most provincially regulated records – such as hospital records – or records in the unregulated private sector – such as records in physicians’ offices or in laboratories – are out of the federal jurisdiction (Cavoukian and Tapscott, 1995). In the absence of the universal “medical privacy laws,” general privacy laws are incapable of protecting medical records. Moreover, the public seems to provide information and sign “consent forms” without considering the consequences of this action. This leaves individuals legally unprotected, with no control over dissemination of their medical information.

¹ A Massachusetts based organization that serves as a repository for information to be exchanged by insurance companies for the basic purpose of detecting and deterring insurance fraud. About 800 U.S. and Canadian insurance companies rely on MIB files as a source of information (Cavoukian and Tapscott, 1995; Linowes, 1989).

vi) Drug Testing Records:

Despite centuries of attempts to halt the use of habit-forming drugs, there are always new generations of drugs that emerge in different forms or appearances (Coombs and West, 1991). Subsequent to advances in techniques for the isolation, purification, and synthesis of habit-forming compounds, the evolution of technology has made possible the detection of minute quantities of drugs in biological beings. “Drug-testing,” the societies’ recent attempt to stifle the nagging problem of drug abuse, employs one of a number of techniques to detect traces of illicit drugs in one’s blood stream, urine, or breath. The decision to choose the method depends on the required speed, sensitivity, specificity, and the type of drug detection, as well as the extent of physical intrusion that is conceivable (Coombs and West, 1991).

Specific drug-testing programs have so far affected the military, the amateur athletic sports, the hospitals, the prisons, and more recently the work place, implicating both the current and the prospective employees (Coombs and West, 1991). In Ontario, drug testing in nuclear plants has recently been encouraged by Mike Harris, the premier of Ontario. This is notwithstanding an earlier decision by the federal court, which called the “tribunals-approved” mandatory drug-testing policy for all new employees of the Toronto Dominion bank, discriminatory (Uncles, 1997). His statement has now opened the door to mandatory drug testing in Ontario.

Despite society’s disapproval of drug abuse, the question of using tests to detect drug usage elicits ethical and moral dilemmas. The proponents of drug testing strongly believe that vigorous measures are long overdue to eliminate the drug problem. They believe that this is the best solution to arrive at a drug free society; and in fact, drug

testing has been successful to some extent. The opponents, on the other hand, are concerned about the invasion of the individuals' privacy. They also view drug tests as "dehumanising and degrading" (Coombs and West, 1991). In the case of workplace, concerns and controversies over drug testing revolve around a number of issues. First is the lack of a proven correlation between a positive test for a drug and the human behaviour. In fact, some authors believe that "the real justification for drug screening is the identification of deviant, rather than dysfunctional behaviour"(Morgan, 1984). In addition, these tests may be used to predict the "moral behaviour of individuals" (Morgan, 1984). Second is the drug tests' limitation to differentiate a drug user from a drug abuser (Coombs and West, 1991). As the detection powers of current techniques increase, it becomes more difficult to determine a cut-off point to distinguish the users from the abusers. Also, as protective measures, drug tests fail to identify those who, despite passing the drug test, are unfit to work. An example would be people who suffer from fatigue. Finally, it not only invades individuals' physical privacy, but also opens the door to discrimination and the potential invasion of individuals' information privacy. As the individuals' testing information is collected and stored in organisations' databases, regardless of the accuracy of results, potential stakeholders may access and use this information, in a different context, against them.

12.2 Appendix B: Personality Information

i) Integrity (Honesty) and Polygraph Testing Records:

These records contain information that is collected using integrity tests or Polygraphs. Polygraphs are based on the scientific theory that a liar's fear of being detected provokes certain bodily responses including changes in blood pressure, pulse, respiration and perspiration. Thus by measuring these changes it is possible to determine whether the person is telling the truth. Other inventions include a CD-ROM lie detector called the "Truster"¹, which measures the frequency of voice vibrations, and a computer program called HARM² Inventory (Holden Applicant Reliability Measures) test, which measures response time to a series of 100 work-related questions. Integrity tests are a non-intrusive form of polygraphs, which consist of interviews and questionnaires. The purpose of integrity tests is to measure one's level of honesty, by asking honesty related questions, about attitudes towards honesty and admission to past dishonest behaviours (Regan, 1995). The logic for integrity tests, in particular in the employment context, is that the attitudes of individuals, toward employment misconduct such as theft, are good predictors of their future behaviours (Regan, 1995).

The main difficulty with these types of tests is the amount of judgement necessary on the part of the examiner. The experience and skills of the examiner, as well as the examiners' subjective perception of the examinee may be quite influential in the final decision (Bible and McWhirter, 1990). Another problem is the assumption underlying these tests that "there is a predictable causal relationship between lying, certain

¹ This test, which was developed in Israel, is based on the claim that "lying reduces the blood supply to the larynx, causing the voice to flutter (Citizen, Feb.1998).

emotional, physical, attitudinal states, and future behaviour. The lack of scientific correlation for this relationship undermines the conclusions of such tests (Bible and McWhirter, 1990). As these tests are usually aimed at new recruits for employment, the most immediate damage is the individuals' inability to acquire a job for which they may be well suited.

ii) Ability Testing Records:

The ability tests were originally formulated during the Second World War, when the United States government was faced with the problem of assigning millions of people to war related jobs. The aim of ability tests was originally to "measure basic intelligence and physical agility" of individuals (Bible and McWhirter, 1990). These tests have since been transformed into a battery of different types of aptitude tests, which evaluate individuals' intelligence or psychological traits.

Intelligence tests can usually be done through paper and pencil tests that require individuals to answer a series of multiple choice, or true or false questions.). An example of the intelligence test is the intelligent quotient (IQ) test. Psychological tests, on the other hand, in addition to paper and pencil form, can be done through interviews with psychologists, following which the psychologists submit their opinions about the examinees (Bible and McWhirter, 1990). One example of the paper and pencil psychological tests is the Minnesota Multi-Phasic Personality Inventory Test (MMPI). This test is widely used in the context of employment (Bible and McWhirter, 1990).

These tests suffer from lack of test validity. Intelligence tests, for example, purport to measure intelligence, but it is difficult to establish what intelligence really is. Is

² This test, which was developed by Mr. Ronald Holden of Queen's university and funded by the Imperial Oil Ltd., claims a 65-85 percent accuracy rate. HARM Inventory test "could be legally used in Ontario to

intelligence one specific trait for which one can look or there are a variety of biological and environmental variables that play a part in developing a person's intelligence?

Dissemination of information about individuals' ability testing may prevent many, who are negatively or erroneously labelled, from obtaining jobs or higher education. In this sense, people may be concerned about organisations' handling of this type of information.

iii) Genetic Records:

Human genes, the carriers of hereditary information from one generation to the next, carry instructions that determine the growth patterns, the physical appearances, and as recently suggested the behaviours of individuals. There are estimated 100,000 Deoxyribonucleic Acid (DNA) based genes in the human genome, which make up the humans' 23 pairs of chromosomes within each single cell. The collection of information in this complex structure, which ensures variety and uniqueness of individuals, is what scientists refer to as the genetic records.

Genetic technology has now advanced to the point that it can unravel the mysteries of the human genome by decoding the genetic records. The Human Genome project, an auspicious 15-year project jointly directed by the United States' National Institute of Health and the Department of Energy, for example, delivers the promise to determine the location and chemical sequence of all genes in the human genome by the year 2003. Genetic records have the potential to greatly benefit the human kind by clarifying the etiology and the pathophysiology of disease. Genetic records can confirm the diagnosis of a disease; determine the presence or absence of a gene, a group of genes, or a specific gene marker or markers. This information indicates that the individual is at

increased or decreased risk of developing a disease or an illness, as a result of having inherited a gene, or that the individual is a carrier of a gene. Consequently, genetic records has the prospect to empower medicine and science to prevent or mitigate human suffering through genetic testing, genetic and reproductive counselling, and treatment of disease (Gostin, 1995). Currently, there are certain pre-symptomatic tests that, through a simple analysis of a small tissue or blood sample, can identify genetic susceptibility to at least 350 different, highly catastrophic “monogenic” or “polygenic” genetic diseases (Regan, 1995; Nock, 1993).

Many have also begun to look for genetic causation in a wide range of physical and behavioural disorders. The recent years, in particular, have witnessed a trend in searching for intrinsic genetic explanations for undesirable social behaviours (Draper, 1991). Criminal conduct, addiction, aggression, obsessive-compulsive behaviours, mental illness, and alcoholism (Duster, 1990) exemplify infamous behaviours that are increasingly viewed as inherited, rather than the outcome of moral integrity, self-discipline, or social circumstances (Nock, 1993; Draper, 1991). For example, a gene on chromosome 11, which codes for a dopamine receptor on brain cells, has been linked to some cases of heroin addiction (Glausiusz, 1998). This abnormally long gene is present in the genome of not only drug addicts, but also others who exhibit “novelty-seeking behaviour” (Glausiusz, 1998).

The term genetic record, in the context of this thesis, means “any information about an identifiable individual that results from three types of analyses. First is from the analysis of an individual’s DNA. Second is from the analysis of the DNA of a person to whom the individual is related. And finally, it is the information that results from the

status of the individual in a pedigree or family history that has been developed or analysed for a particular hereditary condition” (Annas, et al., 1995). Genetic records are the most intimate information about a person. It is the information by which it is possible to uniquely identify a person, and all the attributes of that person, amongst millions of people. In terms of the quality and the quantity, genetic records are more comprehensive than any other type of information about an individual. This type of information not only provides knowledge about the present physical and psychological status of an individual, but also paints a picture of the individual’s future physical, psychological and behavioural standing. It can be thought of as “a coded probabilistic future diary,” which describes a part of a person’s unique future (Annas, et al., 1995).

A growing group of organisations, in both the private and the public sectors, currently collect, store, use and transfer vast amount of personally identifiable genetic records in their databases. The National Institute of Health (NIH), and the National Health and Nutrition Examination Survey (NHANES), exemplify organisations that actively collect genetic records. NHANES, for example, has already collected comprehensive genetic data in patient-identifiable form on over 40,000 Americans (Gostin, 1995). Furthermore, a number of countries have proposed to introduce, in the near future, the automation of health data and plan, using conceptual and technological innovations such as the “patient-based longitudinal clinical records” (Gostin, 1995). Patient-based longitudinal clinical records include genetic testing, unique identifiers, which can link genetic, records to specific individuals, and genetic databases for clinical, research and public health purposes (Gostin, 1995). Following the introduction of these technologies, the next logical step would be to screen the whole population of

individuals, and to collect and store in special databases the genetic records of the entire population.

As scientists map³ more of the human genome, they develop more sophisticated genetic tests to examine individuals' genetic characteristics. The Medical Section Committee of the American Council of Life Insurance (ACLI) on genetic testing provides a definition for genetic tests. This definition states that genetic tests are "laboratory tests that are used to determine the presence or absence of abnormal or defective genes and/or chromosomes, directly measuring such abnormalities or defects, as opposed to indirect manifestations of genetic disorders" (Quoted in Regan, 1995). There are two major types of genetic tests, *genetic screening*, and *genetic monitoring* (Draper⁴, 1991). Genetic screening enables scientists to examine individuals' genetic make-up for hereditary characteristics that make them susceptible to diseases (Nock, 1993; Linowes, 1989). Genetic screening is, particularly, effective in identifying *heterozygous carriers*⁵ (Draper, 1991). Emphysema, chronic bronchitis, heart attacks, or haemolytic reactions exemplify some of the disorders that genetic testing can prognosticate (Draper, 1991; Nock, 1993; Linowes, 1989). The second type of genetic testing, the genetic monitoring, is the periodical examination of individuals to evaluate changes in their genetic material. These changes include chromosomal damage caused by exposure to radiation and chemicals (Nock, 1993).

Although, collecting genetic records will be highly beneficial for health care decisions with respect to prevention, treatment, diet, lifestyle, and reproductive planning,

³ Mapping refers to the identification of every gene on every chromosome.

⁴ Draper names *Tests for teratogenic risk* as the third type of genetic testing. As far as this study is concerned genetic monitoring encompasses this type of genetic testing.

⁵ Heterozygous carriers are those who carry a single gene that may cause higher risk of developing disorders, when exposed to certain chemicals or certain environmental conditions (Draper, 1991).

it may serve other less desirable purposes. It has the prospect to empower those in possession of this information, or those with access to it, to tap into the most private attributes of the individuals and their families, and to invade their “Genetic Privacy”, or in other words the privacy of their genetic records (Gostin, 1995). Furthermore, scientific attempts to interpret individuals ‘past actions, anticipate individuals’ future performances and differentiate individuals, on the basis of race, intelligence, “genotypic abnormality,” or behaviours, can entice a host of “social inequalities” including elitism, and genetic discrimination⁶ (Gostin, 1995; Nock, 1993; Billings, et al., 1992; Draper, 1991). A 1992 study, to obtain statistically significant information about the extent of genetic discrimination in the United States, has shown that many social institutions regard genetic conditions as serious, disabling, and even lethal (Billings, et al., 1992). People seem to have a misconception about the abnormality of genotypes. Contrary to common understanding, individuals with genotypic abnormality – the “asymptomatic ill” – leads healthy lives, have medically controllable conditions, or only suffer from mild forms of the genetic condition (Billings, et al., 1992). These misconceptions have inevitably created situations where individuals are unjustly discriminated against. This type of discrimination limits access to jobs, acquisition of medical or life insurance, higher education, or adoption of children by the affected individuals (Billings, et al., 1992). One can find numerous real life examples in “Dangerous Diagnostics.” This is a book by Marsha Saxton (1989), which describes situations where discrimination has led to denial of medical, or life insurance, employment, and a range of other social vulnerabilities.

⁶ Genetic discrimination refers to discrimination against an individual or a family based solely on an apparent or perceived genetic variation from the “normal” human genotype (Billings, et al., 1992).

The experience with the HIV-related information, which in some aspects parallels the genetic records, also provides many examples for individuals' stigmatisation, discrimination, and victimisation that may result from information leakage or disclosure. As with the genetic records, HIV-related information can foresee one's future, while not necessarily offering a particular cure or the hope of a cure. At the same time, the public feels concerned about both types of information as they identify the carriers of a communicable life threatening illness (Parmet, 1995).

In the case of genetic records disclosures, as with the HIV-related information, the problems with insurance, employment, and social acceptance subsist. For example, insurance companies may refuse an insurance application on the basis of predisposition or susceptibility of a subject to an illness. Conversely, any individual who is aware of her likely bleak genetic future can attempt to obtain insurance for economic gain. By identifying, and eliminating from the workplace, the "carriers" of predisposing genetic abnormalities, employers may be able to avoid certain future costs that such employees may potentially impose on the organisation. Public schools may be able to use genetic records, as a measure of the students' ability to learn, to select candidates, or to use it as a part of their educational credentials. Courts of law may be able to appeal to genetic records evaluations about genetic deviance of convicts to assess the potential dangers of releasing a convict back into the society. There is also the danger of implementation of some form of eugenics, since different genetic characteristics occur with different frequencies in racial and ethnic populations.

There are a number of issues that augment the potential problems associated with the breach of individuals' genetic privacy and other social problems associated with

dissemination of individuals' genetic records to unintended parties. Great weight that the public perception places on the genetic findings, uncertainty, unreliability, and inaccuracy of genetic tests, and unavailability of cures for many of the diagnosed illnesses exemplify such issues (Gostin, 1995). The Human Genome Project, for example, exaggerates the importance of genes. Genetic testing, in contrast to common perceptions, is incapable of predicting the presence or absence of a disease or a condition. What it is capable of is the determination of predisposition to a disease or a condition (Asch, et al., 1997; Regan, 1995). Besides, genetic tests do not consider environmental factors, which are important, in particular, at the time when the environment is deteriorating. Nor do they consider individual genetic variations and the affects of economic and social misfortune or blessing. Thus, genetic testing interpretations, in particular when looking for genes responsible for mental illnesses, could be wrong or misleading. For example, an abnormality in chromosome 11 is notorious for causing manic depression. The abnormality, however, produces the illness in only 60-70% of individuals who carry the responsible gene. This is not true for the remaining 30-40% of individuals who never develop this disease (Nock, 1993). Therefore, by looking at the abnormality of a gene, one cannot unequivocally guaranty the occurrence of the illness. Studies of this sort reflect the probability of disease in a population of individuals and may be irrelevant when applied to specific individuals (Nock, 1993).

In making predictions or decisions about individuals' genetic status, it is important to consider the validity and reliability of the tests that provide the genetic records. Furthermore, to obtain reliable genetic records, to confidently predict individuals' future genetic status, it is necessary to overcome a number of obstacles.

These include the absence of genetic markers in most disorders, the cryptic biological mechanisms underlying some illnesses, the ambiguous modes of disease inheritance, and the doubtful location of genes responsible for certain diseases (Draper, 1991).

While current genetic tests may be unreliable predictors of individuals' fates, future improvements are likely. Increased diversity and availability of genetic tests, fashioned to meet different medical or research needs, is likely to increase concerns about the above mentioned social implications of genetic records (Asch, et al., 1997; Fox, 1993).

An increasing number of employers are using genetic tests as the criteria for hiring or discharging employees (Draper, 1991). In 1982 a survey by the United States' Office of Technology Assessment (OTA)⁷ reported 19 major companies as having previously used genetic screening of employees to detect their susceptibility to disease if exposed to high levels of toxins (Linowes, 1989). This study found that out of 366 respondents 8 companies used genetic testing, and 59 admitted using them in the past and indicated plans for the future use of genetic tests (Regan, 95). A follow up report in 1989 indicated 13% of the fortune 500 companies admitting to present or past use of some type of genetic testing. Later in 1991, however, a task force sponsored by the ACLI and the Health Insurance Association (HIAA) reported that genetic testing was not yet in use in the insurance industry and nor was it about to be adopted. This task force presented a number of reasons why they thought genetic testing might never find use in the insurance industry (Smith, 94).

⁷ OTA is a bipartisan agency that serves United States congress.

Despite the increase in the use of genetic testing by different industries, the public seems to remain indifferent about the implications of this practice. A 1995 Harris poll reported that only 27 percent of Americans have read or heard about genetic tests. This poll reported that 68 percent of those questioned said that they would be “very likely,” or “somewhat likely to undergo these tests, even for diseases for which a cure has not been found. Most surprisingly 56 percent “found it either “very” or “some what” acceptable to develop government computerised data banks with samples taken from all new-borns and their names attached to the samples” (Roche, et al., 1995).

Considering the malice that may result from the accumulating volumes of genetic records, the increase in usage of genetic tests, and the public’s unawareness about potential dangers of genetic tests and information they generate, it is important to afford some measures to protect the privacy of individuals’ genetic records.

12.3 Appendix C: Sample Cover Letter

Dear respondent:

I am currently conducting a study regarding information privacy. This study intends to assess individuals' concerns regarding the information privacy practices of different organisations.

The attached questionnaire, which will take approximately 10-15 minutes to complete, will assess your concerns about the information privacy practices of organisations with respect to 1) information type, 2) organisation type, and 3) technology type.

I would appreciate your completing of this questionnaire and returning it to Dr. Uma Kumar of the School of Business, using the university's internal mail. Your responses will remain completely anonymous. The results of the survey will be made available to you on request.

Thank you for taking the time to help with this survey.

Sincerely,

Roosbeh Ghiami

M.M.S Student
Carleton University
Ottawa, Ontario

12.4: Appendix D: Smith's instrument & instrument Validation model

Smith's instrument development and validation process (Adopted from Bagozzi, 1980; Bearden, et al., 1993; Churchill, 1979; and Straub, 1989 and illustrated in Smith, et al., 1996).

The instrument developed by Smith et al., 1996

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, **agree** or **disagree** with each statement by circling the appropriate number. *

- A. It usually bothers me when companies ask me for my personal information.
- B. All the personal information in computer databases should be double-checked for accuracy - no matter how much it costs.
- C. Companies should not use personal information for any purpose unless it has been authorised by the individuals who provided the information.
- D. Companies should devote more time and effort to preventing unauthorised access to personal information.
- E. When companies ask me for personal information, I sometimes think twice before providing it.
- F. Companies should take more steps to make sure that the personal information in their files is accurate.
- G. When people give personal information to a company for some reason, the company should never use the information for any other reason.
- H. Companies should have better procedures to correct errors in personal information.
- I. Computer databases that contain personal information should be protected from unauthorised access - no matter how much it costs.
- J. It bothers me to give personal information to so many companies.
- K. Companies should never sell the personal information in their databases to other companies.
- L. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
- M. Companies should never share personal information with other companies unless it has been authorised by the individuals who provided the information.
- N. Companies should take more steps to make sure that unauthorised people can not access personal information in their computers.
- O. I'm concerned that companies are collecting too much personal information about me.

Items A, E, J, and O comprise the "collection" sub-scale; Items B, F, H and L comprise the "Errors" sub-scale; items C, G, K, and M comprise the "unauthorised secondary use" sub-scale, and items D, I, N

* Each of the items is followed by a seven-point likert scale anchored by "Strongly disagree (1) and "Strongly agree" (7).

12.5 Appendix E: Research Questionnaire

Carleton University School of Business

A study of Information Privacy

- This survey is designed to investigate the levels of concern of individuals about the information privacy practices of various organisations. Your participation in this survey will aid our understanding of the factors affecting these concerns. There is no right or wrong answer. Rather, your opinion will provide valuable insight.
- All information given in this survey will be kept in the strictest confidence and will only be presented in aggregate form in the research results.
- Please answer all questions and return the questionnaire in the enclosed envelope as soon as possible.
- If you have any questions about this survey, please contact Roozbeh Ghiami at: 595-9180, E-mail rgmg@sympatico.ca or Professor Uma Kumar at the School of Business, at 520-2600, extension 4463, E-mail ukumar@ccs.carleton.ca.
- If you would like a summary of the results of this study sent to you, please indicate this in the space provided at the end of the questionnaire.

Thank you for your assistance in this research

Roozbeh Ghiami, B.Sc. (Hon),
M.M.S. Student,
School of Business
Carleton University
Ottawa, Ontario

Information Privacy

In today's society organisations need to collect information, about citizens with whom they engage in business activities. Similarly, people disclose information about themselves to many different organisations in order to receive services or products. This information disclosure may be through application forms, income tax returns, or as a result of applications for jobs or an insurance coverage, for example. Regardless of the method by which the information is collected, organisations store it in their storage files for future use. This survey seeks to investigate your concerns about what happens to this information once it has been collected. Below are examples of each type of information on which we would like to get your opinion.

- **Financial Records:**
 - Household income
 - Bank accounts information
 - Debts, and mortgages
 - Credit card balances and payment history
- **Transactional Records:**
 - Credit card or debit card purchases
 - Cheque Payments
- **Police Records:**
 - Driving records
 - Motor vehicle registration information
 - Arrests, convictions, criminal records, bails, paroles, and court judgements
- **Library Records:**
 - Record of books previously read
 - Late or timely return of books
- **Medical Records:**
 - Diagnostic and testing information
 - Psychiatric and mental status
 - General health status
 - Disabilities
- **Integrity or polygraph testing Records:**
 - Lie-detection testing records
 - Pre-employment or other employment-related honesty or integrity tests
- **Ability testing records:**
 - IQ testing, or other intelligence or personality testing records
 - School admission aptitude testing records: GMAT, LSAT, MCAT, GRE
- **Drug Testing Records:**
 - Records of pre-employment or other employment-related testing for alcohol or drug abuse
- **Genetic Records:**
 - Records of any information obtained by DNA analysis for hereditary information-gathering purposes, or as a pre-employment requirement

The questionnaire contains five sections. Please answer all questions. It should take approximately 15 minutes to complete the questionnaire.

Thank you for your assistance

Section I

This section examines your past experiences and attitudes towards information privacy. Please check the appropriate box in question 1 and 2. In question 3 indicate the extent to which you agree or disagree with each statement by simply circling the appropriate number. One (1) denotes strongly disagree and seven (7) denotes strongly agree with the statement.

1. Have you personally been the victim of what you felt was an improper invasion of privacy?	<u>YES</u>	<u>NO</u>
--	------------	-----------

2. Have you heard or read during the last year about the use and potential of misuse of personal information?	<u>YES</u>	<u>NO</u>
---	------------	-----------

	Strongly Disagree				Neutral			Strongly Agree
3. Circle the number that most closely applies to you:								
3a. In general, I am very trusting when it comes to providing my personal information to others.	1	2	3	4	5	6	7	
3b. I readily accept social values, and practices about information privacy issues.	1	2	3	4	5	6	7	

Section II

This section examines how concerned you are about the information privacy practices of organisations. Please indicate the extent to which you agree or disagree with each statement by simply circling the appropriate number. One (1) denotes strongly disagree and seven (7) denotes strongly agree with the statement.

	Strongly Disagree					Neutral			Strongly Agree
4. It usually bothers me if I am asked to <i>disclose</i> my:									
a. financial records	1	2	3	4	5	6	7		
b. Transactional records	1	2	3	4	5	6	7		
c. Police records	1	2	3	4	5	6	7		
d. Library records	1	2	3	4	5	6	7		
e. Medical records	1	2	3	4	5	6	7		
f. Integrity and polygraph testing records	1	2	3	4	5	6	7		
g. Ability testing records	1	2	3	4	5	6	7		
h. Drug testing records	1	2	3	4	5	6	7		
i. Genetic information	1	2	3	4	5	6	7		

	Strongly Disagree		Neutral		Strongly Agree		
5. If asked for, I would think twice before <i>disclosing</i> my:							
a. financial records	1	2	3	4	5	6	7
b. Transactional records	1	2	3	4	5	6	7
c. Police records	1	2	3	4	5	6	7
d. Library records	1	2	3	4	5	6	7
e. Medical records	1	2	3	4	5	6	7
f. Integrity and polygraph testing records	1	2	3	4	5	6	7
g. Ability testing records	1	2	3	4	5	6	7
h. Drug testing records	1	2	3	4	5	6	7
i. Genetic information	1	2	3	4	5	6	7

	Strongly Disagree			Neutral		Strongly Agree	
6. I am concerned that organisations are <i>collecting</i> too much of my:							
a. financial records	1	2	3	4	5	6	7
b. Transactional records	1	2	3	4	5	6	7
c. Police records	1	2	3	4	5	6	7
d. Library records	1	2	3	4	5	6	7
e. Medical records	1	2	3	4	5	6	7
f. Integrity and polygraph testing records	1	2	3	4	5	6	7
g. Ability testing records	1	2	3	4	5	6	7
h. Drug testing records	1	2	3	4	5	6	7
i. Genetic information	1	2	3	4	5	6	7

	Strongly Disagree		Neutral		Strongly Agree		
7. Regardless of the cost, organisations should ensure the <i>accuracy</i> of my:							
a. financial records	1	2	3	4	5	6	7
b. Transactional records	1	2	3	4	5	6	7
c. Police records	1	2	3	4	5	6	7
d. Library records	1	2	3	4	5	6	7
e. Medical records	1	2	3	4	5	6	7
f. Integrity and polygraph testing records	1	2	3	4	5	6	7
g. Ability testing records	1	2	3	4	5	6	7
h. Drug testing records	1	2	3	4	5	6	7
i. Genetic information	1	2	3	4	5	6	7

	Strongly Disagree			Neutral			Strongly Agree
8. The following, when disclosed to an organisation for one purpose, should never be used by that organisation for any <i>other purposes</i>:							
a. financial records	1	2	3	4	5	6	7
b. Transactional records	1	2	3	4	5	6	7
c. Police records	1	2	3	4	5	6	7
d. Library records	1	2	3	4	5	6	7
e. Medical records	1	2	3	4	5	6	7
f. Integrity and polygraph testing records	1	2	3	4	5	6	7
g. Ability testing records	1	2	3	4	5	6	7
h. Drug testing records	1	2	3	4	5	6	7
i. Genetic information	1	2	3	4	5	6	7

	Strongly Disagree			Neutral			Strongly Agree
9. Organisations should never <i>share or sell</i> the following to other organisations, unless authorised:							
a. financial records	1	2	3	4	5	6	7
b. Transactional records	1	2	3	4	5	6	7
c. Police records	1	2	3	4	5	6	7
d. Library records	1	2	3	4	5	6	7
e. Medical records	1	2	3	4	5	6	7
f. Integrity and polygraph testing records	1	2	3	4	5	6	7
g. Ability testing records	1	2	3	4	5	6	7
h. Drug testing records	1	2	3	4	5	6	7
i. Genetic information	1	2	3	4	5	6	7

	Strongly Disagree			Neutral			Strongly Agree
10. Regardless of the cost, information systems that store the following should be protected from unauthorised <i>access</i>:							
a. financial records	1	2	3	4	5	6	7
b. Transactional records	1	2	3	4	5	6	7
c. Police records	1	2	3	4	5	6	7
d. Library records	1	2	3	4	5	6	7
e. Medical records	1	2	3	4	5	6	7
f. Integrity and polygraph testing records	1	2	3	4	5	6	7
g. Ability testing records	1	2	3	4	5	6	7
h. Drug testing records	1	2	3	4	5	6	7
i. Genetic information	1	2	3	4	5	6	7

Section III

This section examines how concerned you are about the information privacy practices of organisations by measuring your levels of concern based on the type of organisation, which is handling the information. This section of the questionnaire refers to three types of organisations:

- **Governments Organisations:** Examples: Revenue Canada, or Health and Welfare Canada.
- **Non Profit Organisations:** Examples: Red Cross, Oxfam Canada, or Carleton University.
- **For- profit Organisations:** Examples: Royal Bank, Bell Canada, Met-Life or Wal-Mart.

Please indicate the extent to which you agree or disagree with each statement by simply circling the appropriate number. One (1) denotes strongly disagree and seven (7) denotes strongly agree with the statement.

	Strongly Disagree		Neutral		Strongly Agree	
11. It usually bothers me to <i>disclose</i> my personal information to:						
a. For-profit organisations	1	2	3	4	5	6 7
b. Non-profit organisations	1	2	3	4	5	6 7
c. Government organisations	1	2	3	4	5	6 7

	Strongly Disagree		Neutral		Strongly Agree	
12. I think twice before <i>disclosing</i> my personal information to:						
a. For-profit organisations	1	2	3	4	5	6 7
b. Non-profit organisations	1	2	3	4	5	6 7
c. Government organisations	1	2	3	4	5	6 7

	Strongly Disagree		Neutral		Strongly Agree	
13. I am concerned that too much personal information is being <i>collected</i> by:						
a. <u>For-profit organisations</u>	1	2	3	4	5	6 7
b. <u>Non-profit organisations</u>	1	2	3	4	5	6 7
c. <u>Government organisations</u>	1	2	3	4	5	6 7

	Strongly Disagree		Neutral		Strongly Agree	
14. Regardless of the cost, personal information held by the following should be double checked for <i>accuracy</i>:						
a. For-profit organisations	1	2	3	4	5	6 7
b. Non-profit organisations	1	2	3	4	5	6 7
c. Government organisations	1	2	3	4	5	6 7

	Strongly Disagree		Neutral		Strongly Agree		
15. The following should never use personal information, given to them for one purpose, for any <i>other</i> purposes:							
a. For-profit organisations	1	2	3	4	5	6	7
b. Non-profit organisations	1	2	3	4	5	6	7
c. Government organisations	1	2	3	4	5	6	7

	Strongly Disagree		Neutral		Strongly Agree		
16. The following should never <i>share or sell</i> personal information in their files to other organisations, unless authorised:							
a. For-profit organisations	1	2	3	4	5	6	7
b. Non-profit organisations	1	2	3	4	5	6	7
c. Government organisations	1	2	3	4	5	6	7

	Strongly Disagree		Neutral		Strongly Agree		
17. Regardless of the cost, the following should protect their information systems against unauthorised access:							
a. For-profit organisations	1	2	3	4	5	6	7
b. Non-profit organisations	1	2	3	4	5	6	7
c. Government organisations	1	2	3	4	5	6	7

Section IV

This section examines how concerned you are about the information privacy practices of organisations by measuring your levels of concern, based on the type of technology used for storing the personal information. Please indicate the extent to which you agree or disagree with each statement by simply circling the appropriate number. One (1) denotes strongly disagree and seven (7) denotes strongly agree with the statement.

and seven (7) denotes strongly agree with the statement.

	Strongly Disagree			Neutral			Strongly Agree
18. My personal information is safe when it is stored:							
a. <u>by manual filing</u> (in filing cabinets on paper copies)	1	2	3	4	5	6	7
b. <u>in databases</u> (on computer files)	1	2	3	4	5	6	7
c. <u>on Smart Cards</u> (Small cards, the size of credit cards, with a computer chip. Small cards are carried by the persons providing the information. Organisations can access the relevant information on the cards, only when they are providing a service to the individual. A central database serves as information backup if cards are lost or stolen).	1	2	3	4	5	6	7

Information Privacy Questionnaire

Section V

This section collects some personal information, which will be needed for a complete analysis of your responses. It helps the proper classification of your responses. Please note that all responses are strictly confidential. Please check the appropriate box.

1. How old were you on your last birthday? _____ years of age

2. Check the appropriate level education that you have completed and got credit for:

High school Diploma ☐ Technical College ☐

University: First Year ☐ Second year ☐ Third year ☐

Bachelor's Degree ☐ Master's degree ☐ Ph.D. ☐

3. What is your sex? Male ☐ Female ☐

4. For how many courses are you officially registered? _____ Courses

5. What is your major field of study? _____

Your participation in this survey is very much appreciated