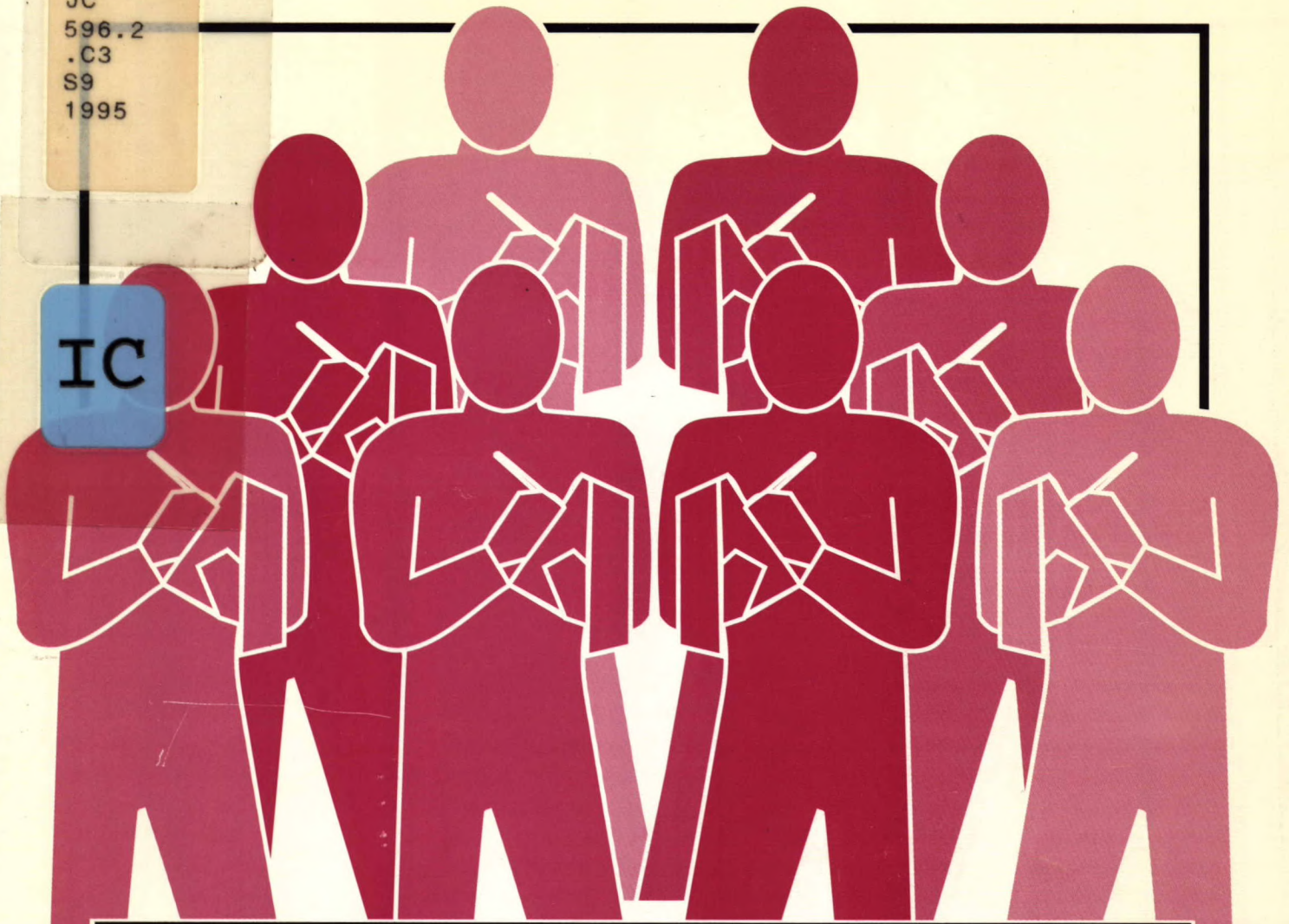


QUEEN
JC
596.2
.C3
S9
1995

IC



SURVEYING BOUNDARIES

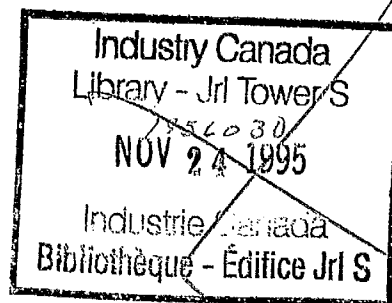
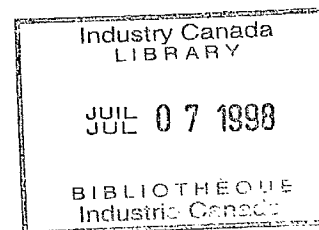
***Canadians
and their
Personal Information***

FNACQ • PIAC

SURVEYING BOUNDARIES:

Canadians and their Personal Information

September 1995



Public Interest Advocacy Centre

1 Nicholas Street
Suite 1204
Ottawa, Ontario
Canada K1N 7B7
(613) 562-4002



Fédération nationale des associations de consommateurs du Québec

1215 Visitation
Bureau 103
Montréal (Québec)
Canada H2L 3B5 2Y7
(514) 521 6820

PROJECT TEAM

Patrick Beauchamp, Ekos Research Associates Inc.
Lola Fabowalé, Public Interest Advocacy Centre
Susan Galley, Ekos Research Associates Inc.
Frank Graves, Ekos Research Associates Inc.
Bill Jeffery, Public Interest Advocacy Centre
Philippa Lawson, Public Interest Advocacy Centre
Pierrôt Péladeau, Progesta Inc.
Andrew Reddick, Public Interest Advocacy Centre
Marie Vallée, Fédération des Associations de Consommateurs du Québec

SPONSOR

This report and the survey on which it is based
were made possible by the generous financial assistance
of **Industry Canada**.

ACKNOWLEDGEMENTS

FNACQ and PIAC extend their appreciation to the following
individuals and organizations for their generous donations
of time and expertise:

Carman Baggaley, Price Waterhouse
Colin Bennett, University of Victoria
Ann Cavoukian, Assistant Privacy Commissioner/Ontario
Ekos Research Associates Inc.
David McKendry, Price Waterhouse
Rachel Roy, Industry Canada
Stephanie Perrin, Industry Canada
Progesta Inc.

and the 2,000 plus individuals who offered their time and thoughts to the survey team.

CANADIAN CATALOGUING IN PUBLICATION DATA

Fédération nationale des associations de consommateurs du Québec
& Public Interest Advocacy Centre
Surveying Boundaries: Canadians and their Personal Information

Issued also in French under the title:

Des Frontières à Définir : La Population Canadienne et les Renseignements Personnels

ISBN 1-895060-34-6

TABLE OF CONTENTS

FOREWORD	v
INTRODUCTION	vi
Background	vi
The Growing Importance of Personal Information Processing	vi
Previous Studies	viii
Study Objectives	ix
Methodology	ix
COMMENTARY by <i>Frank Graves, Ekos Research Associates Inc.</i>	x
EXECUTIVE SUMMARY OF SURVEY FINDINGS	xiv
 <u>SURVEY FINDINGS:</u>	
PUBLIC CONCERNS ABOUT PERSONAL INFORMATION PROTECTION	
Control and Consent	1
Focus of Concern	2
Concerns About Information Sharing by Institutions	3
Onus of Protection	3
Desire for More Information	4
 PERSONAL EXPERIENCES, PERCEPTIONS AND CONCERNS	
Experience	5
Invasiveness	7
Justification	8
Analysis	8
Situation-by-Situation Analysis:	10
Business Selling Personal Information to Third Parties	10
Sharing of Information Among Related Companies	11
Government Agency Selling Health Information to an Insurance Company	12
Charities Selling Donor Lists	13
Employers Taping Employees' Conversations	14
1-800 Caller Number Identification	16
Telemarketing	17
Businesses Monitoring Personal Information	18
Drug Testing by Employers	19
Employment Status and Bank Accounts	20
Phone Solicitation by Charities	21
Recipients Returning Calls Without Message Inviting Call-Back	22
Employment Canada and Revenue Canada sharing information about Unemployment Recipients	24
Revenue Canada Deducting Overdue Child Support Payments	24
Pharmacists Exchanging Information About Prescriptions	26

TELEPHONE COMMUNICATION PRIVACY

Call Display and Blocking 27
Other Telephone Services 28
Sources of Information 28
Attitudes 29

INDIVIDUAL ACTIONS

Awareness of Legislation and Programs 31
Individual Actions 34

REGULATORY PREFERENCES 36

APPENDICES

APPENDIX A

SAMPLING STRATEGY AND WEIGHTING PROCEDURES 38

APPENDIX B

SURVEY MARGINALS 40

FOREWORD

The Federation of Quebec Consumer Groups (FNACQ) and the Public Interest Advocacy Centre (PIAC) are non-profit organizations active on behalf of consumers in privacy issues. Each organization has been involved for a number of years in research and advocacy on privacy, through regulatory proceedings, publications and multi-stakeholder efforts aiming to improve privacy protection in Canada. In their work, FNACQ and PIAC found the dearth of empirical data - especially on the issue of informational privacy - to be a problem. Hence, this study, which was made possible through funding from Industry Canada.

Previous studies (Ekos, 1993; Equifax, 1993 and 1995) have examined Canadians' attitudes, experiences and concerns about privacy in general.¹ Each study laid an important foundation of knowledge in the area, and provided a baseline of the public attitudes around a broad concept of privacy. This study, *Surveying Boundaries*, deepens and extends previous research by inquiring into how Canadians feel about the collection, communication and use of their personal information, in particular.

Privacy issues involving the processing of personal information are better known under the term **protection of personal information**. This aspect of privacy is fast becoming a fundamental issue in a society in which social interaction is growing increasingly reliant upon, and structured by, information and communication technologies. Given the growing importance of policy concerns, it was felt that more focused empirical data was needed on this subject.

The following report presents the results of the first opinion poll conducted by consumer groups on the protection of personal information in Canada. Its publication brings important new information into the privacy debate.

In particular, the results of this survey provide a much clearer and deeper understanding of actual experiences and concerns of Canadians about the use by others of their personal information; about awareness of existing mechanisms designed to protect personal information; about individual initiatives to protect their interests; and about regulatory preferences. Each core issue was covered by a number of detailed questions. The survey also enriches an understanding of the public's values and perceptions about their privacy by assessing how justified they believe different types of information transactions are. Some of the findings question commonly accepted tenets regarding informational privacy. We believe that the results will be useful to researchers, stakeholders and decision-makers working in the privacy field.

¹ Ekos Research Associates Inc., *Privacy Revealed: The Canadian Privacy Survey*, Ottawa, Ekos, 1993; Louis Harris & Associates, Alan F. Westin, *The Equifax Canada Report on Consumers and Privacy in the Information Age*, Ville d'Anjou, Equifax Canada, 1993. Another study by Equifax Canada (Louis Harris & Associates, Alan F. Westin, *The Equifax Canada Report on Consumers and Privacy in the Information Age*, 1995) was published while this report was being prepared.

INTRODUCTION

1.1 Background

The growing importance of personal information processing

Today, more and more information about Canadians is being collected, stored, communicated and transformed into new information. This huge expansion of personal information processing¹ results from convergent developments: the growing importance of large public and private service industries (such as private and public services in the field of insurance and public utilities); the increased bureaucratization of other activities (including human resource management, health care and social services); innovations in information and communication technologies (including, computers, interactive communication media); and progress in the field of medical and social sciences (such as genetics, epidemiology, demographics, opinion polling). In fact, most experts agree that we have not yet witnessed the full span of these developments. Applications such as database marketing, automated transactions and decision making, interactive multimedia transactions, and predictive medicine, while still in their infancy, will undoubtedly increase the pressure to collect, store, share and transform personal information.

In itself, personal information may appear to be a by-product of normal business and governmental activities such as those mentioned above. Collection, storage, communication and transformation could be considered normal stages in the life of this valuable resource. However, no personal information is collected or produced without a purpose. The real significance of personal information processing lies in the fact that it feeds decisions that will affect individuals or groups in some way.² For instance, knowledge of an individual's medical history by a prospective employer could affect the employability of that individual. As well, aggregated personal information from demographic statistics and opinion polls can influence decision-making processes about social and political orientations.

Today, the individual is the subject of a large number of decisions based on information of a personal nature. Many of these decisions are of considerable importance: eg: admission to or graduation from educational programs; hiring and promotion; application for mortgage financing, insurance protection or financial assistance; and medical treatment. An even greater number of decisions are more benign, such as authorization for a credit card or a debit card transactions; being targeted for a sales pitch by businesses or charities; and being billed for consumption of goods and services or for contravention of parking by-laws. Whatever their consequences, a growing number of decisions are being made on the basis of information supplied pursuant to some personal information processing, which in most cases, is beyond the control of the people most directly affected by the decisions.

Control over personal information is at the core of the social and legal issue called *informational privacy* which can be summarized by the question: *Who controls what personal information to what end?* It refers to a fundamental conflict between the interests of many different stakeholders, who are usually divided into two groups: "data subjects" and "data users".

¹ While the term "personal information" was not defined for respondents, it is generally taken to mean any information about an individual which can be used to identify that individual, and includes name, address and telephone number among other data. By "personal information processing" we mean the full range of activities dealing with personal information, including collection, storage, communication, transformation and decision-making.

² Péladeau, P., "Esquisse d'une théorie juridique des procès d'information sur les personnes" (1989) *McGill Law Journal* 34:1952, discusses various representations of personal information processes.

Protection of personal information seeks a balance between the rights and duties of data subjects and those of data users. Mainstream informational privacy research defines these categories as follows:

DATA USERS = ORGANIZATIONS = NEED OF PERSONAL INFORMATION FOR DECISIONS/TRANSACTIONS

DATA SUBJECTS = INDIVIDUALS = NEED FOR PERSONAL INFORMATION PROTECTION

However, these equations do not always accurately depict relationships among the various stakeholders. The debate around telephone services derived from Automatic Number Identification technology (ANI) - of which Call Display is the best known application - provides an illustration of how roles and interests are not always as simple as these equations imply.

For example, because ANI technology is available to both companies and individual subscribers, both parties can be data subjects and data users. Companies can use ANI to gather personal information (i.e., name, phone number) for their purposes, such as marketing. Individuals can use Call Display to identify callers. While this provides greater control over incoming calls, it also creates potential privacy problems. For example, some individuals may not wish companies to collect and use this information. Or, where sensitive information or personal security is at stake (e.g., calling from a women's shelter, calls originating from a health care or social service professional), callers may have good reason for not wishing to divulge the telephone number from which they are calling.

The vision of an "information highway" anticipates individuals becoming both consumers *and* producers of information and transactional services. Consequently, the traditional concepts of "data subjects", "data users" and personal information protection must be replaced by more sophisticated models that better resemble the complicated web of social relations mediated by personal information.

An international consensus has emerged among experts and stakeholders about a minimal set of fair information principles.³ These principles can be summarized "succinctly in the aphorism that ***the right person should get the right information for the right purposes***".⁴ European countries have already opted for a legislative approach covering both the public and private sectors.

In North America, on the other hand, legislation is widely accepted as a sensible approach only with respect to governmental or public bodies encroaching on individual privacy. Strong disagreements emerge when the implementation debate turns toward the private sector. In the US, discussions are polarized between the proponents of pure self-regulation and those in favour of sectoral legislation. In Canada, the debate generally considers a spectrum of possible solutions, various combinations of approaches ranging from "mitigated self-regulation" (such as the *CSA Model Code for Protection of Personal Information (Q-830)* project), to legislation (such as Quebec's *Act respecting Protection of Personal Information in the Private Sector*⁵), with the federal Privacy Commissioner publicly recommending that federal privacy legislation be extended to cover both the public sector and the federally regulated private sector.⁶ Further complicating matters in Canada is the issue of constitutional division of powers as between the federal and provincial governments.

³ The best known version of these principles is the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 12, 1980).

⁴ Flaherty (1989) quoting Paul Sieghart at 380.

⁵ L.Q. 1993 c. 17.

⁶ Annual Report of the Privacy Commissioner of Canada, 1994-1995, p.6.

Previous studies

Previous opinion research has explored the attitudes of Canadians toward informational privacy to a limited extent. Two surveys were conducted in 1992, one sponsored by a groups of government and industry bodies,⁷ and the other by Equifax Canada, a leading collector and provider of personal information for consumer financial transactions.⁸ Equifax has since conducted a follow-up survey.⁹

The Ekos survey took a broad approach to privacy, combining personal information abuses together with other forms of privacy invasion such as those resulting from crime (eg: burglary, extortion or sexual assault), peeping Toms and eavesdropping, nuisances (such as door-to-door salespeople), and abuses of power by employers. As a result, Ekos concluded that there was a gap between the broad definition of privacy used by lay persons and the narrow one used by some experts to talk about the protection of personal information.¹⁰

The Equifax surveys examined informational privacy more closely, and noted rising levels of concern, including 70% (64% in 1992) of respondents agreeing with the statement that "Consumers have lost all control over how personal information about them is circulated and used by companies".¹¹

However, evidence from both consumer associations and information-intensive organizations suggests that the average individual does not spontaneously construe the result of poor or unfair informational practices as an "invasion of privacy", or even as a privacy-related issue. More detailed analysis was needed to obtain information on public opinion and experiences related to personal information practices in particular. As Ekos noted in its report, "Clearly, concern about relinquishing personal information cannot be adequately explained in a unidimensional model. It is the interaction of the setting, the purpose, the initiator and the type of information which determines acceptability in the real world".¹²

Moreover, past research has not settled the question of how Canadians would like personal information protection to be addressed. Equifax (1993) found that a significant majority (66%) of respondents considered privacy to be a fundamental right that should be enshrined in the *Canadian Charter of Rights and Freedoms*. At the same time, Equifax respondents were quite distrustful of public institutions.

The Ekos study identified a preference for governmental response to misuse of personal information over industry self-regulation. In fact, the Ekos study showed that 83% of respondents preferred a strong legislative response by government that applied to both the public and private sectors. The Ekos study also concluded that there is no clear consensus, let alone public agenda, for what must be done. Canadians do not show a clear preference between a partnership model of Government working with business and a purely legislative response.¹³ The Ekos study also noted that Canadians see themselves as individuals having a strong responsibility in shaping their levels of

⁷ Ekos Research Associates Inc., *Privacy Revealed: The Canadian Privacy Survey* (conducted October/November 1992, published 1993).

⁸ Louis Harris & Associates and Dr. Alan Westin, *The Equifax Canada Report on Consumers and Privacy in the Information Age* (1993).

⁹ Louis Harris & Associates and Dr. Alan Westin, *The Equifax Canada Report on Consumers and Privacy in the Information Age* (conducted August/September 1994, published 1995).

¹⁰ Ekos, p.41.

¹¹ Equifax (1995), p.17.

¹² Ekos, p.21.

¹³ Ekos, p.46.

personal privacy.¹⁴ But that study did not provide for options that would include the general public, or their representative organizations, in solution design processes.

1.2 Study Objectives

The core issues examined in this study are:

1. What is the awareness, experience and level of concern among members of the public with regard to a variety of situations dealing with personal information?
2. Which personal information practices are considered by the public to be privacy-invasive, and which are nevertheless considered to be justified?
3. What actions are currently being taken by Canadians to protect their interests in relation to the use of their personal information?
4. How aware are Canadians about available tools and existing efforts to protect their personal information?
5. What are Canadians' policy preferences for managing the protection of personal information?
6. How would the above questions be answered with particular reference to telephone Call Management Services?

1.3 Methodology

The Public Interest Advocacy Centre (PIAC) and the Fédération nationale des associations de consommateurs du Québec (FNACQ) developed the questionnaire for this survey, drafts of which were circulated for comment among experts and government officials who share an interest in the protection of personal information.

The revised questionnaire was then administered by phone to a sample of 20 residents in Ottawa (in English) and Montréal (in French), who were then invited to an English and a French focus group, respectively. Besides facilitating refinement of the draft questionnaire, the focus groups also permitted an examination of the qualitative aspects of public opinion about personal information practices.

Five additional telephone pre-test surveys were administered across Canada to further refine the questionnaire prior to the final administration of the survey.

The final questionnaire was administered by phone to a total of 2,053 Canadians during November and December 1994.

To minimize non-response bias, a shorter form of the questionnaire was administered in the last week of the survey to a random sample of 150 people who had refused to answer the longer questionnaire. No statistically significant difference from the results of the main sample was identified.

The survey was conducted from a centralized computer-assisted telephone interviewing facility during November and December 1994. The sample yielded a 95 per cent confidence interval at +/- 2.16 per cent.

¹⁴ Ekos, p.47.

PRIVACY REVEALED — REVISITED:

**A Commentary by
Frank Graves, Ekos Research Associates Inc.**

Introduction

The new privacy survey conducted by FNACQ and PIAC provides an important and timely contribution to the ongoing debate about privacy in Canadian society. In particular, the study refines and sharpens our focus on the topic of *informational privacy*. The study confirms much of the earlier research conducted in the 1992 National Privacy Survey. It also provides a more elaborate picture of Canadians' experiences and concerns within the more delimited domain of personal informational privacy. FNACQ and PIAC have asked us to provide an interpretative essay to accompany this new report.

The purposes of this companion essay are threefold:

- i. to provide an interpretative discussion of selected highlights of the new survey results — particularly in terms of how they deepen or challenge the earlier conclusions of the 1992 study;
- ii. to report on the results of some independent multivariate analyses examining the role of experience in conditioning responses to privacy concerns; and
- iii. to relate the main survey conclusions to the role of government and present some new evidence drawn from our original *Rethinking Government* project on the relative priority, expectations and preferred divisions of roles and responsibilities in the area of privacy concerns.

It should be noted at the outset that public perceptions of privacy issues are generated through an uneasy mixture of values, interests, knowledge and experiences. The neat analytical distinctions of the research or policy analyst are extremely difficult to impose in the shifting realm of public perceptions of privacy. Our comments will reflect the complexities and vagaries of the way privacy concerns play out in the real world.

Levels of Concern and Experience

The new survey reaffirms the fact that Canadians remain seriously concerned about threats to personal privacy. It also demonstrates that the level of direct experience of privacy intrusions in the area of personal information is substantial. Earlier research had argued that for many Canadians it was the vicarious or theoretical possibility of insidious, hidden invasions which produced highest levels of concern. This new survey clearly documents that many informational privacy abuses are in fact fairly pervasive, and indeed noticed by individuals. On the other hand it is quite clear that the level of experience is inversely correlated with the seriousness of the invasion. In other words, *relatively* trivial invasions (e.g., "victims" of telemarketing) are ubiquitous, but more threatening forms of privacy invasions, such as governments selling your health history to an insurance company or an employer taping your telephone conversations, are relatively rare.

The survey shows that the two most *common* forms of experienced invasions — uninvited telemarketing and uninvited requests for charitable donations are also rated as *serious by only a minority* of those experiencing them. The survey also shows that the two *most seriously rated invasions* — governments selling your personal health information and your employer taping your (work calls) are the *least frequently experienced* (four and six per cent). Clearly, it remains the case that the most insidious and threatening forms of privacy invasions tend to be relatively rarely experienced. We continue to note that these invasions may occur unbeknownst to the victim. We also note that the vagaries of survey methodologies does not preclude the possibility that the actual experience of these more serious invasions may well be lower than four and six per cent.

Beyond the simple observation that the most serious problems are least experienced, we were asked to conduct a more careful statistical examination of the role of experience in affecting perceptions of invasiveness and seriousness. In other words how do the responses of those who claim to have actually experienced a particular event compare to the responses of those who say they never have? In order to isolate the influences of experience on perceptions of seriousness and invasiveness we conducted detailed multivariate analyses controlling for a broad range of other factors which we also know influence perceptions of seriousness (e.g., demographics, social class variables, etc.). The detailed statistical analyses, which utilize logistic regression techniques, are appended to this report.

The central conclusion is that direct experience actually *reduces* the probability that one will find a given privacy scenario threatening. Out of 15 separate situations tested there was a negative relationship between prior experience and the likelihood of perceiving the situation as an invasion in 14 cases. The same is true in the case of how prior experience relates to ratings of the seriousness of a privacy intrusion. In about half of these events the effects remained statistically significant in the multivariate analysis. The only example of a significant positive effect (i.e., experience heightening concern) was in the case of the government deducting child support payments from tax refunds. It may not be surprising that those evading child support would find the actual experience of having their income tax tapped more alarming than the theoretical principle. On the other hand, few members of the general public summon much sympathy for the use of invasive techniques in *this* situation (above ten per cent consider it serious).

From Absolute to Situational Principles

This underlines the confirmation of the 1992 Ekos research that the acceptability of an event or practice is a complex product of: rationale/ benefit; knowledge and familiarity; transparency; consent/ control and trust. It is safe to say that *there are no absolute privacy principles*. There is, however, a clear logic underlying the public's application of these different factors to determining the acceptability of various practices in the real world. As this new study argues, the factors of control/consent and benefit/ rationale are typically the most important. The same practice (e.g., uninformed exchange of health information) can produce profoundly different levels of concern depending on its purpose. It is generally viewed as acceptable and even desirable for pharmacists to share data to avoid health risks to their customers. Respondents don't agree, however, that this same type of information sharing is acceptable to help insurance companies improve their risk assessment for underwriting purposes.

Returning to the role of experience it is important to note that this survey advances our understanding of the complex interactive role of experience in conditioning response to privacy-related practices. The most serious problems are least experienced. Perhaps less obviously, the act of experiencing a given practice appears to diminish concerns. The effect is not huge and it does not eliminate concern.

Why would experience reduce concern? Once again it may be useful to utilize a *risk perception* framework to understand this. Perception of risk is typically magnified in the absence of experience. This is why smoking is seen as less threatening than living near a nuclear power plant — despite reverse “objective” or statistical risks. In the case of privacy concerns it may be that as people experience, and manage to cope with, these situations their fears are lessened. It is also interesting to note that another key element of risk perception theory involves “locus of control” — whether the individual feels personal control. This connects clearly to the study findings on informed consent — that the less control individuals feel they have over the uses of personal information, the more concern they have.

The Role of Social Class

How does social class intervene in these relationships? In our past research we argued it was an important variable for understanding privacy concerns. This survey provides a basis for examining its connection to more detailed instances of informational privacy problems. We argued that actual experience of many privacy intrusions was higher amongst the more affluent members of society. For the economically insecure the actual experiences were lower but the sense of threat from vague yet threatening invasions was higher.

The current study argues that “the weight of personal information processes in the lives of individuals actually grows according to their dependence on public and private bureaucracies”. It goes on to claim that the current survey supports this hypothesis. Our re-analysis of the data leaves us sceptical of this claim. In examining the domain of experience across the range of practices/scenarios tested we generally find that those individuals who are more comfortable and secure are *more* likely to experience the intrusions tested. The relationship between experience and social class is typically either positive or insignificant.

Another important finding is that there is a strong connection between access to new technology and social class. More affluent and educated Canadians are more likely to own and understand new information technologies (e.g., computers) and commercial services designed to manage invasions. Most Canadians approve of the use of call management technology to manage privacy concerns. There is an escalating ecology of predator-prey technology for gatekeeping and managing personal and electronic access in western society. The growth of the information highway is redefining the boundaries of community and privacy in a new information age. Basic controls and access are increasingly determined through the use of technology and knowledge which are systematically less available to members of economically insecure classes of society.

It is also the case that the application of invasive practices has far less benefit in the insecure portions of society. Whereas the nuisances of telemarketing and recombinant data linkages for reselling are not welcome, there are aggregate benefits for the economically secure (for example: consumer choice, greater profits and commercial activity, reduced costs for governments). These benefits are less likely to be enjoyed by the economically distressed. In fact, applications for the insecure are more likely to include surveillance and control to reduce employer or government costs. For these Canadians, sharing of personal information is also more likely to result in an unwelcome outcome — e.g., credit or employment denial. Our point is not to argue about the ethics of these phenomena — although this broader debate should be vigorously pursued as these trends accelerate. Rather we wish to underline the major differences in the experience, meaning and implications of privacy concerns across social class.

The Broad Societal Context: Expectations of Government

We can also examine this question of the role of experience-familiarity at the highly aggregated level of society as a whole. This leads to a discussion of the changing context for privacy concerns in society and the role of the state, the individual and business in dealing with privacy issues.

We have been tracking Canadians' attitudes to privacy as government priority since 1992. Recently we have been examining privacy concerns in the context of shifting expectations of government. We can link our broader research to some of the more specific conclusions drawn from this new survey.

First of all, we find that the *overall* priority assigned to privacy has declined somewhat since 1993. It remains a moderately important priority of the same broad order of importance as national unity, consumer protection and housing. It is a substantially lower concern than top priorities like jobs and debt.

Part of the decline in priority is a reflection of general erosion in government priorities conditioned by declining expectations and confidence in government and acute economic anxieties about public finances. The decline in privacy concerns, although modest, is steeper than in other areas. This may well reflect growing familiarity/ experience with the expression of privacy practices in the new information era. This may be a macro, societal expression of the diminution of risk with increased familiarity hypothesis. Clearly the incidence of informational invasions tested in the study has risen dramatically since 1992 (several key examples were not even evident in the market place in 1992).

Some Evidence on Role of Government

Does this mean that Canadians are now comfortable with relying on their own resources or trusting the good faith of other organizations to respect their privacy concerns? Clearly the answer is no. The majority of Canadians see privacy as a moderate to important priority for government. Most are unaware of current privacy programs/ legislation and the majority are unhappy with the current system for protecting privacy concern of individual citizens (only 33 per cent rate satisfaction with the current system).

Our *Rethinking Government '95* material also shows that 64 per cent of Canadians feel government should be *primarily* responsible for protecting citizens from privacy intrusions (35 per cent federal, 21 per cent provincial). Only six per cent pick "businesses". This links with past research to reconfirm Canadians' unease with business self-regulation. Citizens are not looking for a heavy-handed or expensive government involvement. Canadians reveal a pragmatic balance of concern and tolerance in most of these areas. It is, however, important to note that 77 per cent would like the federal government to either increase or maintain its involvement in this area. Canadians are also looking for personal involvement in this area and are receptive to the concept of strategic partnerships amongst business, government and individuals. This is, however, one of those areas where Canadians see the problems as too difficult to manage on their own and they look to government to provide a sense of protection and security regarding the overall public interest.

Respondents Who Experienced a Situation Compared to Those Who Did Not: Percent Stating Situation is an Invasion of Privacy

	Ever experienced the stated situation			Logistic Regression	
	No	Yes	Sig.	Coff.	Sig
Consider a government agency sells a database which includes your health history to an insurance company. ¹	91.3	70.2	0.000	-1.7072	0.000
Consider providing information about your employment status in order to open a bank account to be a privacy invasion	63.0	32.7	0.000	-1.1838	0.000
Consider pharmacists across the province can exchange information by computer about your prescriptions to ensure that the medications you are receiving are compatible to be a privacy invasion	16.7	4.7	0.000	-1.021	0.003
Consider a business you deal with monitors the information it has on you and then tries to promote new services to you to be a privacy invasion	57.0	39.5	0.000	-0.6006	0.000
Consider a prospective employer insists that you take a drug test to be a privacy invasion	49.1	34.5	0.009	-0.4926	0.079
Consider a business you deal with provides personal information about you to a related company, without your consent to be a privacy invasion	91.9	87.8	0.003	-0.4362	0.032
Consider Revenue Canada deducts an amount a court has ordered a delinquent parents to pay for child support from her or his income tax refund to be privacy invasion	22.0	30.9	0.082	0.3455	0.336
Consider receiving an uninvited telephone calls from someone selling a product of service to be a privacy invasion	64.6	61.1	0.488	-0.3397	0.243
Consider calling a 1-800 number and your telephone number is automatically registered for marketing purpose by the business you called to be a privacy invasion	76.3	71.2	0.034	-0.3360	0.032

1. The following example is intended to clarify this table. Among the respondents who had not experienced government selling a database to an insurance company, 91.3 per cent indicated this situation was an invasion of privacy while only 70.2 per cent of individuals who experienced this stated it was an invasion of privacy. The coefficient for the logistic regression model (which controls for differences in background characteristics) was negative and significant, confirming that individuals who experienced the situation were less likely to indicate this type of situation was an invasion of privacy.

	Ever experienced the stated situation			Logistic Regression	
	No	Yes	Sig.	Coff.	Sig
Consider a charity to which you donated money sells its list of donors to another charity to be a privacy invasion	78.6	85.8	0.010	0.3258	0.047
Consider a business you deal with sells personal information it has about you to others without your consent to be a privacy invasion	95.7	94.7	0.376	-0.3214	0.271
Consider your employer tapes your telephone conversations at work to determine if you are doing personal business during work hour to be a privacy invasion	82.2	74.1	0.015	-0.2976	0.283
Consider Employment Canada and Revenue Canada share information about you to ensure that you are not cheating on their unemployment insurance to be a privacy invasion	26.0	29.3	0.365	0.2390	0.307
Consider someone returns a telephone call even though the caller did not leave a message to be a privacy invasion	31.8	27.6	0.033	-0.0187	0.886
Consider receiving an uninvited telephone calls from a charity seeking a donation to be a privacy invasion	40.7	42.3	0.602	-0.0034	0.984

Respondents Who Experienced a Situation Compared to Those Who Did Not: Average Rating of Seriousness of the Privacy Invasion

Rating of the seriousness of the following situations:	Ever experienced the stated situation			Linear regression	
	No	Yes	Sig.	Coff.	Sig
Consider a government agency sells a database which includes your health history to an insurance company. ¹	5.763	4.620	0.000	-1.3708	0.000
Consider providing information about your employment status in order to open a bank account to be a privacy invasion	3.642	2.290	0.000	-1.1831	0.000
Consider Revenue Canada deducts an amount a court has ordered a delinquent parents to pay for child support from her or his income tax refund to be privacy invasion	1.905	2.662	0.001	0.7729	0.007
Consider a prospective employer insists that you take a drug test to be a privacy invasion	3.210	2.580	0.024	-0.7647	0.024
Consider a business you deal with monitors the information it has on you and then tries to promote new services to you to be a privacy invasion	3.424	2.580	0.000	-0.6673	0.000
Consider your employer tapes your telephone conversations at work to determine if you are doing personal business during work hour to be a privacy invasion	5.261	4.664	0.002	-0.6450	0.008
Consider pharmacists across the province can exchange information by computer about your prescriptions to ensure that the medications you are receiving are compatible to be a privacy invasion	1.672	1.205	0.000	-0.3944	0.002
Consider a business you deal with provides personal information about you to a related company, without your consent to be a privacy invasion	5.420	5.037	0.000	-0.2836	0.014
Consider Employment Canada and Revenue Canada share information about you to ensure that you are not cheating on their unemployment insurance to be a privacy invasion	2.114	2.320	0.237	0.2791	0.195

1. The following explanation is intended to clarify the information in this table. Respondents who had not experienced the government selling a database to an insurance company, on average, rated this situation as a more serious privacy invasion (5.76) than respondents who had experienced this type of situation (4.62). The regression coefficient confirms that respondents who experienced this type of situation had lower ratings of the seriousness of the privacy invasion than those who did not, in fact the rating was 1.37 lower, controlling for differences in background characteristics.

Rating of the seriousness of the following situations:	Ever experienced the stated situation			Linear regression	
	No	Yes	Sig.	Coff.	Sig
Consider a charity to which you donated money sells its list of donors to another charity to be a privacy invasion	4.450	4.790	0.000	0.2195	0.077
Consider calling a 1-800 number and your telephone number is automatically registered for marketing purpose by the business you called to be a privacy invasion	4.296	4.124	0.171	-0.1355	0.3829
Consider a business you deal with sells personal information it has about you to others without your consent to be a privacy invasion	5.94	5.820	0.136	-0.1043	0.291
Consider receiving an uninvited telephone calls from someone selling a product of service to be a privacy invasion	3.547	3.514	0.893	-0.0724	0.032
Consider receiving an uninvited telephone calls from a charity seeking a donation to be a privacy invasion	2.510	2.540	0.797	-0.0685	0.6727
Consider someone returns a telephone call even though the caller did not leave a message to be a privacy invasion	2.180	2.060	0.127	0.0004	0.969

EXECUTIVE SUMMARY OF SURVEY FINDINGS

This report presents the results of the first opinion poll conducted by consumer groups on the protection of personal information in Canada. Its publication brings important new information into the privacy debate. In particular, the results of this survey provide a much clearer and deeper understanding of actual experiences and concerns of Canadians about the use by others of their personal information; about awareness of existing mechanisms designed to protect personal information; about individual initiatives to protect their interests; and about regulatory preferences. The survey also enriches an understanding of the public's values and perceptions about their privacy by assessing how justified they believe different types of information transactions are.

Control over personal information is at the core of the social and legal issue called *informational privacy* which can be summarized by the question: *Who controls what personal information to what end?* It refers to a fundamental conflict between the interests of many different stakeholders, who are usually divided into two groups: "data subjects" and "data users", but who are not always so easily categorized, as our results show. The vision of an "information highway" anticipates individuals becoming both consumers *and* producers of information and transactional services. Consequently, the traditional concepts of "data subjects", "data users" and personal information protection must be replaced by more sophisticated models that better resemble the complicated web of social relations within which personal information flows.

The core issues examined in this study are:

1. What is the awareness, experience and level of concern among members of the public with regard to a variety of situations dealing with personal information, and with respect to informational privacy generally?
2. Which personal information practices are considered by the public to be privacy-invasive, and which are nevertheless considered to be justified?
3. How aware are Canadians about available tools and existing efforts to protect their personal information?
4. What actions are currently being taken by Canadians to protect their interests in relation to the use of their personal information?
5. What are Canadians' policy preferences for managing the protection of personal information?

Key findings are summarized below:

Public concerns about personal information protection

- *Concerns of Canadians over collection and use of their personal information are high; individuals sense an erosion of control over their personal information.*

Seventy-six percent (76%) of Canadians feel that they have less control over their personal information than they did ten years ago. This compares to 60% of Canadians who agreed in 1992 that they had less personal privacy in their daily lives than they did ten years ago.

- *Canadians are particularly concerned about the sharing of personal information between different organizations, especially private firms.*

While 70% would be at least moderately concerned about sharing between government bodies, 90% would be at least moderately concerned about sharing among private firms, or

between government and private firms.

- *Canadians demand knowledge about and control over the uses to which their personal information may be put.*

Canadians want to be informed about collection processes and about the uses to which their personal information may be put (95%). They insist that their permission be sought and given before any such information is passed on to another organization (94%). They want to understand how new technology can affect their personal privacy (86%).

- *Technological changes should not place a greater burden on individuals to protect their personal information.*

Canadians feel strongly that technological change should not place a greater burden (financial or otherwise) on them, as individuals, to protect their personal information (82%). However, they are concerned enough about their privacy that they are willing to go out of their way to protect their personal information in order to keep up with technology (67%).

Personal experiences, perceptions and concerns

- *Most Canadians have experienced violations of widely-accepted principles of protection of personal information.*

Ninety-five percent (95%) have experienced unsolicited calls from telemarketers, and 85% from charities. There can be little doubt that personal information is being widely collected and traded without the knowledge or consent of data subjects, contrary to principles of informational privacy.

- *The more directly respondents are affected by an information process, the more certain they will be of their experience. People exhibit high levels of uncertainty with respect to their experience of less easily detectable practices.*

Thirty-seven percent (37%) of Canadians are unsure about whether their telephone number has been recorded by a business through its 1-800 service. Twenty-eight percent (28%) are uncertain of whether their personal information has been sold by one business to another without their consent, and 26% are not sure about whether a charity they give to trades its donor list with other charities.

- *There is a direct relation between perceptions of the invasiveness of personal information practices and opinions as to their justification.*

Opinions as to justification of specific practices closely match perceptions of invasiveness. Non-justification ratings are usually a few percentage points lower than invasiveness ratings (whether or not invasive); where the majority found the practice invasive, a majority also found it unjustified. The only anomalies were employer drug testing, for which non-justification results were 18% higher than invasiveness ratings, and "blind call-backs", which 2% more respondents found to be unjustified than did invasive.

- *Opinions as to the invasiveness and justification of personal information practices are closely linked with appreciation of, and likelihood of experiencing, their consequences. Hence, these opinions are often biased according to socio-economic factors such as income, education and age.*
- *Perceptions of invasiveness and justification of specific information management practices simultaneously involve many interacting factors including privacy.*

Factors which appear to influence perceptions of invasiveness and justification include: the social or personal benefit arising from the transaction; the degree of consent, control and

awareness respondents have over the transaction or process; the type of information (sensitive or general); and the level of trust or perception of legitimacy of the institution involved.

Awareness and action

- *Canadians are largely unaware of legislation and programs protecting the privacy of their personal information.*

Three quarters (73%) of Canadians are unaware of any law or government program protecting personal information, and only 17% can actually cite an example. Only 14% of respondents knew about any private business initiatives protecting personal information, and fewer than one in twenty could actually cite an example.

- *Canadians display low levels of awareness about where they can go for recourse when their personal information is abused.*

Few people request to see their personal information which is in the possession of businesses or institutions (ranging from 1% for records held by landlords to 18% for medical records). Requests to see personal information were denied to roughly 12% of respondents who made them. Approximately one fifth of respondents who obtained access to their personal file detected errors in it.

Telephone communication privacy

- *Both Call Display and Call Display Blocking are seen as desirable services by Canadians. Canadians want Call Display blocking functions to be universally available, easy to operate, and free of charge, both on a "per call" and a "per line" basis.*

Eighty-three percent (83%) of Canadians consider Call Display to be a desirable service, while 40% think that it invades privacy. Seventy-four percent (74%) think that they should have access to call display blocking (and 73% think they should not have to pay for it), while 47% think that blocking is not a good idea.

- *Attitudes of Canadians about Call Display and the blocking function appear to be driven by a desire to maximize the benefits of the technology in respect of both control of incoming calls and control of outgoing information.*

Regulatory preferences

- *Canadians lack confidence in private sector self-regulation.*

When asked to choose among three options, only 7% of Canadians choose industry self-regulation over government regulation or public involvement.

- *Canadians distrust both private business and government in dealing with the protection of personal information; public involvement is essential.*

When asked to choose among three regulatory options, a large majority (69%) choose that option which involves the public, and does not rely entirely on either government or private business.

- *Canadians think that governments should treat this issue as a priority.*

Eighty-seven percent (87%) of Canadians think that government should treat protection of personal information as a priority, but should not collect more taxes for this purpose.

PUBLIC CONCERNS ABOUT PERSONAL INFORMATION PROTECTION

- **Concerns of Canadians over uses of personal information continue to grow.**
- **Individuals sense an erosion of control over their personal information.**
- **Canadians are very concerned about the sharing of personal information between organizations**
- **Concerns are as much about the collection and circulation of personal information, as they are about decisions made on the basis of such information.**
- **Canadians demand knowledge about and control over the uses to which their personal information may be put.**
- **Technological changes should not place a greater burden on individuals to protect their personal information.**

CONTROL AND CONSENT	AGREE	DISAGREE
Less control over personal information than ten years ago	X (76%)	
Should be informed of why personal information is being collected and how it may be used	X (95%)	
Need not inform person in advance when information about him/her is collected		X (80%)
Personal information should not be passed on to another organization without permission	X (94%)	
Don't mind companies using personal information as long as person knows about it and can stop it	X (79%)	

A large majority of respondents felt that they had less control over their personal information than they had ten years ago. Ekos asked a similar question in 1992,¹ to which 60% of respondents agreed. However, Ekos' question was about privacy in general, not control over personal information in particular.² Hence, two factors could be at play here: concerns about privacy in general may be increasing, and/or Canadians feel less control over their personal information than over other aspects of privacy. The former hypothesis is supported by the results of a recent survey by Equifax, however, recent work by Ekos (*Rethinking Government*, 1995) suggests that while concern over privacy in general has remained high, it may in fact have decreased slightly.

Canadians almost unanimously (95%) want to be informed of how personal information collected about them will be used, and insist (94%) that their permission should be obtained before an organization can pass this information on to another. These findings mirror those reported in the Ekos survey, in which 92% of Canadians demanded that they should be notified in advance when information about them was being collected.³ They are further confirmed by responses to a inversely-worded

¹ The question read: "I feel that I have less personal privacy in my daily life than I did 10 years ago."

² Ekos 1992 p. 6.

³ Ekos, 1992, pp.56-57.

question on the same issue, which read as follows: "I **don't** think it is **necessary** to notify me in advance when information about me is collected" (emphasis added). A large majority *disagreed* with the statement, despite the fact that it was phrased in a way designed to elicit responses indicating acceptance of covert data collection.

The statement "I don't mind companies using information about me as long as I know about it and can stop it" was also asked by Ekos in 1992. Responses to the same question in this survey were similar, showing a slight increase in agreement (from 71% to 79%), with strong agreement rising from 62% to 67%. Québécois (85%) were particularly adamant in their support for forewarning and control over information collection. This result could reflect the fact that Québécois, unlike other Canadians, are governed now by legislation restricting use of personal information in the private sector, and therefore may feel more at ease with companies using their information.

FOCUS OF CONCERN	AGREE	DISAGREE
Concerned about decisions affecting the individual, made on basis of personal information collected (English)	X (79%)	
Less concerned with collection and circulation of information than with resulting decisions (French)	47%	37%

The survey included a question designed to distinguish between concerns over collection and circulation of personal information on one hand, and concerns about the *resulting decisions* affecting individuals, on the other hand. Unfortunately, the question received a faulty translation, such that the English and French versions differed.

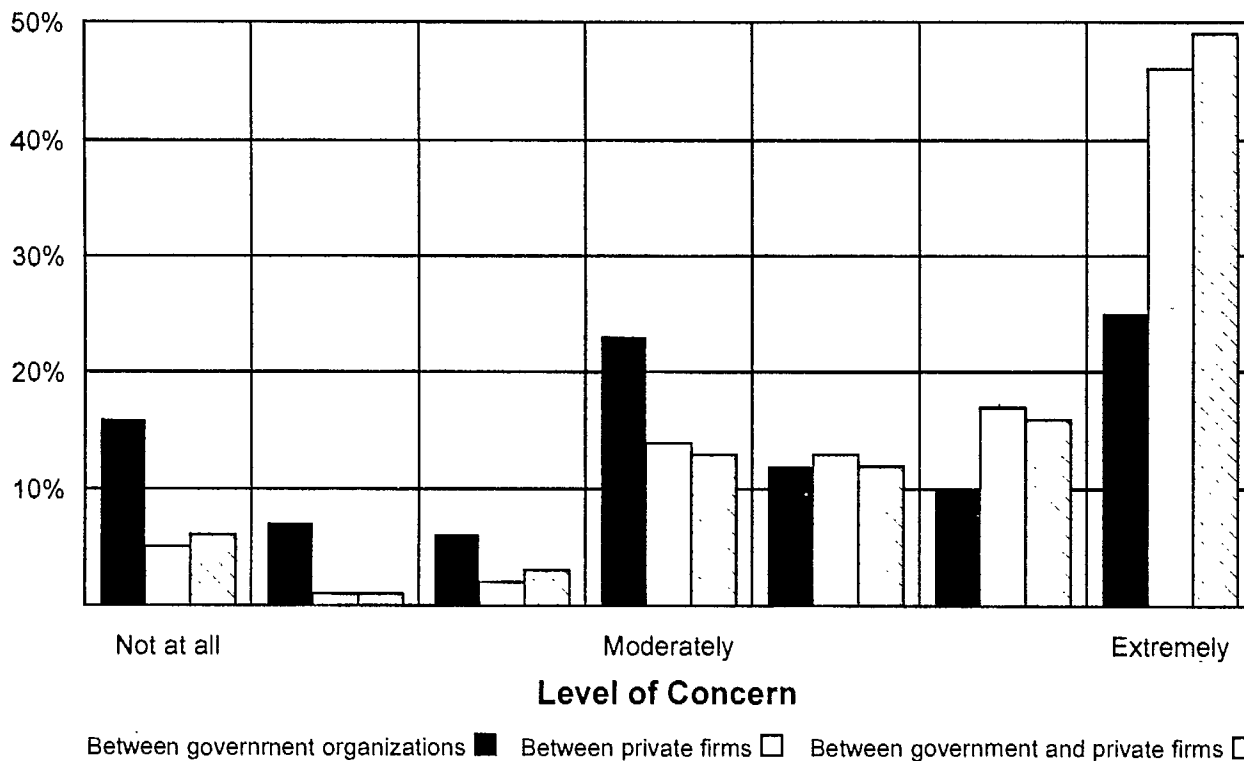
Anglophones were asked about their concerns respecting decisions affecting them which are based on their personal information. A large majority agreed with the statement that: "the collection and circulation of my information aside, I am concerned about decisions taken on that information, which affect me".

Francophones were asked if they were *less* concerned with collection and circulation of information *than* with resulting decisions. Thirty-seven percent (37%) disagreed, thirteen percent (13%) answered "neither" and forty-seven percent (47%) agreed with the statement. Thus, Francophones appear to be almost equally divided between, on one hand, those who are more concerned about decisions than about collection and circulation and, on the other hand, those who are equally or more concerned about collection and circulation.

Both versions of the question suggest that a large majority of Canadians are concerned about *final uses* of personal information collected and communicated about them.

Interestingly, concerns about *decisions* (rather than information collection itself) were much higher among respondents with the highest incomes (over \$75,000 household income: 71%) and among those having University education (67%). It may be the case that better educated Canadians and high income earners have more familiarity with personal information processes and a more acute awareness of the stakes involved in personal decision-making than do other respondents.

Concerns Over Information Sharing by Type of Institution



Overall, respondents expressed a high degree of concern about the sharing of information between two bodies or institutions. Nine out of ten would be at least moderately concerned if government departments and private firms, or if two or more private firms, shared information about them, while seven out of ten would be at least moderately concerned about sharing between two or more government organizations.

Levels of concern are clearly higher when private firms are involved. This difference could reflect less trust in private organizations than in government institutions.⁴ Government may be viewed as a safe, legitimate organization, whose integrity requires such information exchanges. Exchanges between government and private firms are likely to involve a commercial aspect, and may therefore be more suspect in peoples' minds than are exchanges strictly within government.

Despite the abstract nature of the questions, there is evidence that respondents also considered the probable consequences of sharing. In all three cases, older respondents were significantly more likely to report extreme concern, perhaps reflecting greater experience and therefore awareness of possible consequences. Greater dependance on government bureaucracies coincided with greater concern about information sharing between government organizations (Women 27% vs. men 21%; less educated 30% vs. more educated 17%; lower income 26% vs. highest income 17%). Higher income households appear to be more concerned (52%) than average (44%) about sharing among private firms, perhaps reflecting the fact that these were also the most likely households to be targeted for marketing or charity purposes.

⁴ There is support for this hypothesis in results about specific instances and regulatory preferences. Ekos (1993:20-21) found that Canadians had higher levels of concern with private companies than with government, employers or professionals such as physicians. Less concern was asserted with institutions that had greater authority or legitimacy.

ONUS OF PROTECTION	AGREE	DISAGREE
Should not have to make a special effort to protect personal information, regardless of technological change	X (82%)	
Don't mind making a special effort to protect personal information, in order to keep up with technological change	X (67%)	
Should not have to pay more to protect personal privacy in order to keep up with technological developments	X (81%)	
Don't mind paying more to protect personal privacy in order to keep up with technological developments		X (56%)

The survey also asked respondents who should bear the onus of ensuring that personal information is appropriately protected. A large majority of Canadians agreed that they should not have to make a special effort to protect the privacy of their personal information, regardless of technological change. Interestingly, agreement increased with income, from 78% among those having the lowest incomes to 88% among those drawing the highest incomes.

When phrased inversely, the question still elicited agreement from most respondents (67%), indicating the importance attached to privacy of this information by most people. People value the privacy of their personal information enough that they are willing to make special efforts to protect it. Nevertheless, they feel strongly that such special efforts on their part should not be required.

When asked: "I should not have to pay more to protect privacy of my personal information under any circumstances", respondents overwhelmingly agreed (81%), consistently with their opinions above. Meanwhile, a majority of 56% disagreed with the statement "I do not mind having to pay more to protect my personal privacy to keep up with technological developments." Again, it would appear that people are *willing* to pay more in order to maintain their privacy, but that they do not think such costs *should* be forced on them. Residents of the Maritimes (New-Brunswick: 66%; Prince Edward Island/Nova Scotia: 62%) were most reluctant to shell out extra money to protect their privacy in the information age. Otherwise, responses to this question were fairly uniform among regions and socio-economic groups.

DESIRE FOR MORE INFORMATION	AGREE	DISAGREE
Would find it useful to have more information on how new technologies might affect personal privacy	X (86%)	

A high proportion of respondents would find it useful to have information about how new technologies might affect their personal privacy. This preference was somewhat less forcefully expressed by seniors (79%), but was otherwise fairly uniform among regional and socio-economic groupings.

PERSONAL EXPERIENCES, PERCEPTIONS AND CONCERNS

- Most Canadians have experienced violations of widely-accepted principles of protection of personal information.
- The more directly respondents are affected by an information process, the more certain they will be of their experience.
- There is a direct link between perceptions of the invasiveness of personal information practices and opinions as to their justification.
- Opinions as to the invasiveness and justification of personal information practices:
 - are closely linked with appreciation of their consequences;
 - involve many interacting factors, of which privacy is just one;
 - are influenced by the likelihood that the particular information practice will affect them;
 - and
 - are often biased according to socio-economic factors such as income, education and age.

• *Experience*

Previous surveys on privacy conducted by Equifax and Ekos concluded that despite high levels of concern about privacy and protection of personal information, very few respondents actually reported direct experience with abuses of personal information.¹ Accordingly, both studies concluded that concerns about use of personal information were less a product of experience than of fear or distrust of institutions.

The results of this survey, however, show that a large proportion of Canadians *have* experienced situations that they consider to be privacy-invasive dealings with their personal information, and which constitute violations of one or more widely-accepted principles of protection of personal information.²

¹ The most recent Equifax survey (1995) did ask about personal experience with disclosure of medical information in particular. It found that 18% of Canadians have experienced improper disclosure of their medical information. Yet, this did not change Equifax's conclusion that distrust continues to be a major factor in level of concern.

² One widely accepted codification of these principles is the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 12, 1980). These principles include the following:

-that personal data should not be collected, disclosed or used without the knowledge and consent of the data subject except where inappropriate (consent/control); and

-that organizations should make readily available to individuals specific information about their policies and practices relating to their handling of personal information (openness).

Exhibit 1

	Invasion Yes	Very Serious Yes ³	Justified No	Experienced Yes ⁴
Business Sells Information	95	75 (71)	86	26
Business Shares Information	90	62 (56)	81	25
Government Sells Health Data	90	77 (64)	81	4
Charity Sells List of Names	81	51 (41)	76	39
Employer Tapes Phone Calls	80	75 (60)	69	6
Marketing Using 1-800 Data	74	48 (36)	69	18
Uninvited Calls (business)	61	44 (27)	55	95
Business Monitors Data to Sell	48	43 (21)	46	50
Employer Drug Testing	46	54 (25)	64	3
Employment Status for Banks	43	42 (18)	36	64
Uninvited Charity Calls	42	32 (13)	33	85
Call Return - No Message	30	35 (11)	32	53
Sharing to Prevent UIC Cheats	26	49 (13)	18	7
Child Support Deductions	21	46 (10)	15	3
Pharmacists Exchange Data	15	43 (6)	11	13

The principles of consent/control by data subjects and openness by data users, in particular, appear not to have been fully respected in number of situations, including telemarketing (95% have experienced) and charity solicitations (85% have experienced). Direct marketing and fundraising activities currently rely on the trading of personal information databases, most of which have been compiled and traded without the knowledge or consent of the individuals concerned.

Personal information processes⁵ are often difficult to detect by individuals. The easiest to detect involve either direct participation of the individual at some stage (for example, knowingly providing information), or a direct link between the use of the information collected and a resulting action or decision affecting the individual (for example, solicitation calls or mail received soon after use of a list of subscribers). In contrast, other processes can occur without any direct participation or without producing any visible clues about the origin of the information (for example, processing calling numbers collected through automatic number identification technology). Hence, the high levels of uncertainty and low levels of reported experience with respect to the more covert forms of personal information processing.

³ Percentages are of those responding "yes" to the question "Is this an invasion of your privacy?". Percentages in brackets are of total respondents.

"Very serious" = 6 and 7 on a scale of 7, where 1 = "not at all serious", 4 = "moderately serious", and 7 = "extremely serious".

⁴ Includes uncertain "yes" answers ("Yes, I think so").

⁵ The term "personal information processes" refers to the range of activities involved in collection, storage, communication, and transformation of personal information, as well as decision-making based on personal information.

The following is a list of the less detectable scenarios for which actual experience was difficult to determine. The percentages describe levels of uncertain answers ("Yes, I think so" and "No, I do not think so", plus non respondents).

- * Businesses automatically register incoming 1-800 calls for marketing purposes (37%)
- * Businesses sell personal information to third parties without consent of the information subjects (28%)
- * Charities sell donor lists (26%)
- * Businesses share information with related companies without consent of customers or clients (24%)
- * Government agencies sell health information to insurance companies (21%)
- * Businesses monitor personal information for marketing purposes (15%)
- * Employment Canada and Revenue Canada share information about U.I. recipients (10%)
- * Pharmacists share clients' prescription information to ensure compatible medication, without advising clients (10%)

Factors that influence an individual's awareness about personal information protection include: education, knowledge of programs or legislation protecting personal information, and age (middle age adults are more sophisticated in this area than are youths or seniors). Those respondents who were more aware of personal information processes were also more likely to be uncertain of their experiences, while less aware respondent were more certain.

• *Invasiveness*

As discussed earlier, these survey results indicate that Canadians are as much concerned about final uses of personal information as they are about its collection and circulation. Responses to questions about specific instances confirm this: the appreciation of respondents about the relative invasiveness of specific personal information practices is linked with their appreciation of potential consequences.

For instance, circulation of health information from governmental agencies to insurance companies was viewed as a seriously invasive practice (Invasive: 90%). In contrast, the possibility of computer-supported circulation of prescription information among pharmacists to ensure compatibility of multiple medications was perceived to be substantially less invasive (Invasive 15%), and those who found it invasive tended to consider it to be only a moderately serious invasion. The two instances dealt with circulation of sensitive health information, but the one which can be linked with possible negative consequences (insurance) was viewed as highly invasive, while the one linked to a clear benefit (pharmaceutical prescriptions) was not viewed as so invasive.

Canadians appear to assess each specific instance in a pragmatic way. If the conditions of a specific situation are modified (positive or negative consequences, more or less control of individual over the practice, etc.), opinions will likely change. For example, if we had presented mandatory circulation of prescription information between pharmacists, had not mentioned the purpose of medication compatibility, or had mentioned another purpose (such as government control over the costs of free prescriptions for the elderly), the result would likely have been different.

• *Justification*

The collection and use of personal information is controversial, not only with respect to its invasiveness, but also with respect to its justification. Hence, for each situation, respondents were asked not only whether they considered the practice to be invasive, but also whether it was justified.⁶ Non-justification ratings closely matched invasiveness ratings in most scenarios (lower in all but two cases: employer drug testing and blind call-backs), reaffirming findings of previous surveys that informed consent, control and awareness are important dimensions of the privacy issue.

Only in three instances was the "not invasive" rate higher than the "justified" rate by more than 5% (government departments sharing information to prevent cheating, employer monitoring of employee calls, employer drug testing), and in each of these cases, acceptability of the behaviour sought to be controlled would appear to be a factor.

In addition, the "potential benefit" factor seems to be at play: three practices which could be viewed as directly beneficial to data subjects (pharmaceutical information) or indirectly to respondents as taxpayers (U.I. and child support), were least likely to be defined as invasive, and most likely to be considered justified.

• *Analysis*

Canadians clearly do not think of protection of personal information in absolute or abstract terms. They are sensitive to the purpose of information practice, to the interests of likely beneficiaries of it and to the social and personal consequences. For example, 42% of Canadians viewed calls from charities as invasive (22% as seriously so), whereas 61% viewed calls from telemarketers as invasive (38% seriously so). The two instances dealt with the same intrusion: uninvited phone solicitation. But it is likely that one was considered much less invasive than the other because of the type of party making the call (charity or business) and because of the purpose of solicitation (helping fellow humans or making profits).

In its conclusion, Ekos suggested five inter-related hypotheses to explain public privacy concerns: knowledge and familiarity; transparency; consent, control and regulation; rationale/benefit; and legitimacy/trust. While these hypotheses are consistent with the findings of this survey, interactions between them may be more complex than earlier thought. For example, knowledge and familiarity are certainly integrally related with level of concern, but high familiarity does not necessarily bring less concern. In many instances, the effect is completely the opposite, as the results of this survey about uninvited phone solicitations indicate.

As discussed below, issues of **control** (Does the individual give consent to, or have control over, the process?) and of **benefit/adverse effect** (What is the probability of being adversely affected by a decision or action made on the basis of the information collected?) have unequivocal impacts on levels of concern. This leads us to conclude that these two issues are key ones affecting public perceptions of personal information processes.

⁶ The 1995 Equifax report also looked at trade-offs: under what circumstances the gathering and use of personal information is acceptable to Canadians.

Other factors include:

- Is the information subjectively sensitive?
- Is the practice covert or open?
- Is the party using the information behaving in an ethical manner?
- What is the level of surveillance or external control imposed?
- How acceptable is the behaviour sought to be controlled?
- What is the probability of an individual actually experiencing the situation?
- How trustworthy or legitimate is the institution?
- How widespread is the practice?
- How important is the resulting decision or action?

The "probability of being affected" factor reveals itself along many socio-demographic lines. The most noticeable cleavage is social class. An ironic illustration of the privacy "perception gap" among social classes is illustrated by the Ekos' analysis of its survey results. Invasive instances were identified from the experience of those Ekos defined as the "more privileged and powerful members of society": telemarketing, charitable solicitation, scanning of cellular phone conversations, following the personal lives of public figures. The report quite accurately indicated that less well-heeled individuals were less likely to be subjected to such privacy invasions, but then concluded that "for the less powerful and less privileged classes of society, privacy threats are seen as vague yet threatening."⁷

Yet, other researchers in the area of informational privacy have arrived at a different conclusion: the weight of personal information processes in the lives of individuals actually grows according to their dependence on public and private bureaucracies.⁸ The results of this survey confirm this latter hypothesis.

In any case, attitudes toward what constitutes a privacy invasion, and how serious it is, often differ according to social class. This "perception gap" can have practical significance. Top executives, personal information system designers, data protection coordinators, privacy commissioners and judges are generally members of a social group whose personal perceptions and concerns about privacy and data protection are structured by their privileged position in society. More importantly, their perception and concerns are often at odds with the perceptions and concerns of the people affected by their decisions. In order to avoid class biases in policy-making, decision-makers must be rigorous in their scrutiny of practices and sensitive to the perspectives of data subjects, when deciding, as in the above examples, about the appropriateness of information management practices.

On the other hand, our survey results suggest that division of the Canadian population into typologies, as done by previous opinion research on privacy, has little predictive value, especially at the level of specific practices. This is likely because social and economic relations among stakeholders are numerous and varied - indeed, the same individuals are often personal information *subjects* in some contexts, and personal information *users* in others. In brief, the significantly different interests, concerns and values of individuals, which greatly affect their attitudes toward personal information processes, are not easily categorized.

⁷ Ekos pp.44-45.

⁸ André Vitalis, *Informatique, pouvoir et libertés*, Paris, Economica, 1981.

SITUATION BY SITUATION ANALYSIS

Findings related to the fifteen scenarios presented to respondents are provided below, in diminishing order of invasiveness, as perceived by respondents.

■ BUSINESS SELLS PERSONAL INFORMATION TO THIRD PARTIES

• *Experience*

One quarter of Canadians reported a business they dealt with selling personal information about them to others without authorization. But only 19% were *certain* they had experienced this. In fact, 26% were uncertain in their answers about this experience ("Yes, I think so", or "No, I don't think so" qualify as uncertain).

Levels of reported experience were consistent across the different regions of Canada, with residents of B.C., Saskatchewan and Ontario most familiar with this practice.

Because selling personal information is driven by a quest for lucrative markets, it is not surprising that experience was higher among high income respondents than low income respondents: while only 18% of low income respondents were certain of having such experiences (14% were fairly sure), this rate increased to 36% for highest income respondents (29% being fairly sure of experiencing it). Perception of experience also grew with education from 18% (14% sure) to 36% (29% sure) for highly educated respondents.

Those who were aware of protection of personal information programs were also much more likely to report experiences (37% with 30% fairly certain) than those who were not aware of the programs (22% with 16% fairly certain).

• *Invasiveness*

Businesses selling personal information without consent is viewed, almost unanimously (95%), as an invasion of privacy.

This practice was considered to be a very serious invasion of privacy by 75% of respondents defining it as invasive, of whom 57% described it as extremely serious. Twenty-one percent (21%) of respondents viewed it as a moderately serious intrusion, while only 3% viewed it as *not* very serious.

There was considerable consistency among geographic and socio-economic categories about the seriousness of these practices. The only significant variation occurred with age: a higher proportion of older respondents considered the invasion to be "extremely serious" (from 43% for the youngest to 66% for the oldest).

• *Justification*

A large majority (86%) of all respondents considered the sale of personal information by businesses to be unjustified. The higher the income and level of education, the more likely respondents were to find the practice unjustified. (These respondents were also more likely to have experienced the practice.) While there was some variance by age and income, all groups felt very strongly that this practice was unjustified (from 79% of those with least income to 91% of those in the highest income category; and from 82% of the least educated to 91% of the most educated).

Although employment status did not appear to explain much variance in opinion on this issue, self-employed persons were less likely to condemn the practice: only 75% found the practice unjustified, compared to 86% of the entire sample.

• *Analysis*

Canadians almost unanimously find this practice to be an invasion of privacy, and a serious one. They do not consider it to be justified. Indeed, of all the situations posited, this one elicited the highest levels of concern. Such a result likely reflects the lack of control that individuals feel over use by businesses of their personal information - not only do they have no way of monitoring or stopping the practice, they simply do not know the extent to which their personal information is used by private firms. Clearly, informed consent is a key issue: the *status quo*, in which companies engage in the trading of personal information without informing information subjects, is not considered acceptable by Canadians.

Given that businesses often collect and trade personal information without the knowledge of the data subjects, the low level of reported experience of this practice is not surprising. High levels of uncertainty simply reflect the covert nature of this practice, evidence of which is usually indirect at best (eg: increased direct marketing).

These results compare interestingly with those for the same practice engaged in by charities: while 71% of all respondents found business trading to be a very serious invasion, only 41% found charity trading equally serious. Responses were closer, however, on the issue of justification: 76% found personal information trading by charities to be unjustified, vs. 87% with respect to trading by businesses. The largest divergence in opinion seems to be on the seriousness of the invasion, as opposed to the nature of it.

■ SHARING OF INFORMATION AMONG RELATED COMPANIES

• *Experience*

One quarter of respondents thought that they had experienced a business with which they had dealings sharing personal information about them with an affiliate, without their consent (22% were uncertain).

Respondents from British Columbia (31%), Saskatchewan (30%) and Ontario (29%) more often reported having had such experiences, with one third being not completely certain. Those from Quebec and the Maritimes tended to report a level of experience below the average.

There was some variance based on income and education. Lower income (23%) and less educated (21%) respondents reported lower levels of experience than did higher income (34%) and better educated (23%) respondents. Respondents who claimed to have an awareness of personal information protection programs (36%) also claimed to have experienced these types of transactions more often than did others (22%). However, as in other situations, higher levels of reported experience included a higher proportion of uncertain answers.

• *Invasiveness*

Businesses sharing personal information with related companies without the consent of information subjects was viewed as an invasion of privacy by 90% of respondents. There was little variance according to socio-economic variables.

This practice ranked high on the list of privacy invasions, with 56% of respondents considering it a very serious invasion, 30% viewing it as moderately serious, and only 5% as not very serious. Concerns were fairly evenly felt by all groups, although women were more concerned than men (66% vs. 46% finding it very serious), and seniors were more concerned than young adults (69% vs. 56%).

Interestingly, computer owners were more moderate in their concerns than were non-owners (57% vs. 66% finding it a very serious invasion). Like men and university graduates, computer

owners seem make a distinction between *selling* personal information to a *third party* (a much more serious invasion of privacy) and *sharing* personal information among *related companies*, both without consent.

• **Justification**

Even if many Canadians view unauthorized sharing of personal information with affiliated companies as *less* invasive than unauthorized sale to third parties, the fact remains that four-out-of-five Canadians (81%) described the sharing of personal information between related companies without consent as unjustified. This was consistent across different regions of Canada. There was some variation by gender and income, with more women than men finding the practice unjustified (84% vs. 78%), and more high income earners than low income households finding it unjustified (81% vs. 74%).

• **Analysis**

The sharing of personal information among business affiliates is viewed as a serious invasion of privacy by the vast majority of Canadians. Indeed, levels of concern about this practice were not much lower than those expressed over the selling of personal information to third parties without consent.

As with selling to third parties, high levels of concern likely reflect the lack of knowledge and control felt by individuals over what happens to their personal information. Failure by companies to obtain consent before passing on such information to affiliates is clearly unacceptable to Canadians.

■ **GOVERNMENT AGENCY SELLING HEALTH INFORMATION TO AN INSURANCE COMPANY**

While this practice may not yet actually occur, some provinces have been studying the possibility of selling statistical health information databases (not information that identifies individuals) to the private sector, as a means of generating revenue to offset the costs of computerizing health care records.

• **Experience**

Respondents were almost unanimous (95%) in reporting that they had not experienced a government agency selling a database which included their health history to an insurance company. 19% were uncertain, with the highest level of uncertainty (27%) among the \$45,000 to \$59,000 income group, among British Columbians (25%) and Albertans (24%), as well as among university graduates (26%).

• **Invasiveness**

Ninety percent (90%) of respondents defined the sale of health information as an invasion of privacy, which makes this scenario as invasive as the sharing of information among related companies without consent, and second only to businesses selling personal information to third parties. Definition as invasive was consistently high across age groups and education levels (87% - 94% range), although young adults tended to be a little less inclined (79%) to find it invasive.

This scenario attracted the highest level of concern (mean invasiveness rating: 6.23 on a scale of 7) of all fifteen scenarios presented. Sixty-one percent (61%) of those who found it invasive considered the invasion as extremely serious, (77% very serious), only 21% as moderately serious, and very few (3%) described it as not very serious.

Concern was high among all respondents. However, the older the respondent, the more likely they were to be concerned by the idea (extremely serious response rates grew from 30% for younger

adults to 51% for seniors).

Concern also varied with education: 32% of higher educated respondents found the practice "extremely serious", versus 46% of those with high school or less. More education thus brought a more moderate qualification of invasiveness, even if these respondents were more likely to define the situation as invasive.

• *Justification*

Consistent with their definition of this as an extremely invasive practice, respondents described this scenario as the second least justified intrusion (along with businesses sharing information among affiliates) - second only to businesses selling information without consent. Eighty-one percent (81%) considered the sale of health information to insurance companies to be unjustified.

Francophones (21%) were more likely than average (17%) to find it justified. Justification rates dropped with higher education (from 22% to 11%), higher age (from 30% to 13%) and higher income (from 23% to 10%). Consistent with attitudes toward other practices, computer owners were almost half as likely as non-owners to view this practice as justified (13% vs. 22%).

• *Analysis*

Disclosure of sensitive personal information by governments to private firms raises strong concerns on the part of Canadians. To the extent that the information disclosed does not identify the individual to whom it relates, concerns will likely diminish. However, responses to this unqualified question suggest caution on the part of governments in their treatment of such personally sensitive data as health records.

Canadians clearly find such exchanges of data unjustified. This result contrasts with attitudes toward the sharing of sensitive information between government agencies, where the purpose is perceived as socially beneficial (see "Revenue Canada Deducts Overdue Child Support Payments" and "Employment Canada and Revenue Canada Share Information about U.I."). 81% found the exchange between government and private industry to be unjustified, while only 15%-18% found the internal government exchanges to be unjustified. Even though most members of the public might stand to benefit (through lower insurance premiums) from the provision of such information to insurance companies, any such perceived benefit appears to be outweighed by privacy concerns.

■ CHARITIES SELL DONOR LISTS

• *Experience*

A majority of respondents (60%, including 47% responding with certainty) reported having not experienced the selling of donor lists by charities.

Twenty-four percent (24%) of respondents were uncertain in their answers. This is to be expected, since charities do not always advise donors of donor list circulation (either through sale or sharing). In the absence of such disclosure, donors can only infer that this has taken place from available clues (eg: by noticing an identical error in the address labels affixed to mail received from two seemingly unrelated charities). Nevertheless, 39% of respondents (including 28% definite) reported having noticed an exchange of lists.

Reported experience of the practice grew with age, from 23% to 48%; as well as with income, from 22% to 54%. But uncertainty shows the same trend, growing from 7% to 36% with age, and from 18% to 30% with income.

Experience also varies along cultural and geographic lines, with Newfoundlanders (77%), Québécois (72%), francophones (71%) and Allophones (62%) being much more likely than other

Canadians to report that they did not experience this situation. Allophones apart, these respondents are also much more certain in their answers.

• *Invasiveness*

Eighty-one percent (81%) of respondents thought that selling a list of donors, even to another charity, is an invasion of privacy. Those who were more likely to be subjected to this practice were also more likely to define it as invasive: 88% of the high income group and 86% of university graduates characterized this particular exchange as invasive.

A bare majority (51%) of those who described selling donor lists as invasive thought that it was a very serious invasion of privacy. Thirty-four percent (34%) considered it an extremely serious invasion, 39% a moderately serious invasion, and only 10% considered it to be not very serious. Seniors and Québécois were more likely to describe this practice as a serious invasion of privacy. Indeed, almost half of seniors surveyed held the opinion that it is an extremely serious intrusion.

• *Justification*

The fact that the purpose of information circulation in this particular example was charitable did not make the practice more acceptable in the eyes of respondents: 76% still thought that it was unjustified.

Perceived justification for selling donor lists decreased as income grew, from 25% among lowest income respondents to 15% among the highest income respondents. Culture, or at least linguistic culture, may also play a role in determining attitudes toward the justification of selling/exchanging donor lists: 31% of Allophone respondents believed that such practices were justified, compared with 25% of Francophones and only 20% of Anglophones.

• *Analysis*

The difference in perceptions of invasiveness between two interrelated practices (being contacted by a charity on one hand, and the charity circulating personal information on the other) suggests that, in addition to such factors as the level of trust in an institution, and perceived benefits from allowing one's personal information to be used, a third important factor is the amount of *control* individuals have over the use of their information. In those examples where the information transaction and intrusion was open and transparent, and respondents had some degree of control over the process, they were much more comfortable about the activity. (For example, a little less than one half of respondents considered a direct appeal from a charity to be invasive, while a majority (64%) considered such calls to be justified.) In addition to transparency, consent, and control, the personal and social benefits provided by charities also likely influenced respondents views.

While public attitudes toward direct appeals by charities are mixed, the proportion of respondents who considered the selling of lists by charities to be invasive (81%) suggests that informed consent is an important dimension of information transactions *regardless* of how benevolent the body conducting the transactions.

■ EMPLOYERS TAPING EMPLOYEE CONVERSATIONS

• *Experience*

Few Canadians (6%) reported having experienced their telephone conversations being taped by their employers. Moreover, respondents demonstrated very little uncertainty in their responses to this question (2%), probably because this practice, when it occurs, is either part of stated company policy or becomes common knowledge by way of rumours.

Maritimers had little or definitely no experience of such a situation, while Ontarians (9%) reported experiencing it most often.

• *Invasiveness*

Eighty percent (80%) of Canadians defined taping of employees telephone conversation as an invasion of privacy.

There is some regional variation: 87% of Manitobans and 84% of Québécois characterized it as invasive while only 77% of Alberta residents described it as such. Ontarians, the most likely provincial residents to report working in such a situation, were also the most likely to construe it as a very serious invasion (80% of those who found it invasive considered the invasion to be very serious), while residents of Prince Edward Island/Nova Scotia (54%) who had virtually never experienced such work environments were divided on how serious this was.

Young adults (86%) were much more likely to view the practice as invasive than were seniors (70%). University graduates (85%) also felt it to be more invasive than did those with no more than high school education (80%).

Seventy-five percent (75%) of respondents who viewed this situation as invasive described it as a very serious invasion, with 60% describing it as extremely serious, 21% as moderately serious and only 3% as not very serious. This was considered one of the most *seriously* invasive scenarios of the fifteen presented to respondents; it was exceeded in this respect only by businesses selling or sharing personal information, and by government agencies selling personal health information to insurance companies.

• *Justification*

Seven-out-of-ten Canadians (69%) consider the taping of employee telephone conversations by employers to be unjustified.

Employment status has some influence on attitudes toward justification of the practice: unemployed respondents were a little less likely than average to define it as unjustified (66%), while self-employed and seasonal workers were, understandably, more uncertain (non-responses: 12%-15%) and less likely to consider it unjustified (51%). Interestingly, professionals (76%) and senior managers (73%) were among the most likely to describe it as unjustified.

The more educated the respondent, the more likely they were to find the practice unjustified (from 65% of least educated to 74% for most educated).

• *Analysis*

Surveillance of employees through monitoring of telephone conversations was included in this question for comparative purposes - to observe relative perceptions of invasiveness as between direct surveillance and personal information processing. Considered to be one of the more invasive of the fifteen scenarios posited, this one ranked fifth as an invasive practice, after the unauthorized trading of personal information by businesses, government and charities, and third in terms of seriousness of the invasion.

While such surveillance may seem more intrusive than information practices which only affect the individual indirectly, and which are in common use throughout Canada, it is interesting to note that Canadians find the trading of their personal information by others without their consent to be an even greater concern than direct surveillance by employers.

■ 1-800 CALLER NUMBER IDENTIFICATION

• *Experience*

Only 18% of Canadians recognized that when they call a 1-800 number, their own calling number may be automatically registered by the called business for marketing purposes.

Thirty six per cent (36%) of respondents were uncertain about this practice. This level of uncertainty is not surprising, given the lack of any readily available evidence of such registration when individuals make their calls.

Those living in Ontario and the West (Saskatchewan 59%, Alberta 42%, Ontario 40%, and British Columbia 39%) exhibited the highest levels of uncertainty, as did those with higher incomes and education: uncertainty grew with income (from 28% to 62%), education (from 30% to 46%), and age (from 28% to 46% for middle age adults).

• *Invasiveness*

Although most Canadians have difficulty detecting the use of automatic number registration of 1-800 calls, they are clear about their opinions of it: three-out-of-four (74%) considered the practice to be an invasion of privacy.

Older respondents were more likely to find this practice invasive (77% for seniors vs. 65% for young adults), as did those with higher incomes (77% for highest income vs. 69% for lowest income). Finally, Anglophones (75%) tended to find it more invasive than did Francophones (68%).

Almost half (48%) of those who defined 1-800 subscribers' use of automatic number identification (ANI) technology as invasive viewed it as a very serious invasion of privacy. Indeed, one third (32%) of those respondents defined it as an extremely serious invasion, while 42% considered it moderately serious, and 9% not very serious.

Again, the older the respondent, the more likely the invasion will be construed as very serious (rates grew from 32% for youngest to 60% for seniors). Conversely, the more educated the respondent, the less likely they were to view the invasion as very serious (rates dropping from 52% to 42% with education).

Computer owners were also more inclined to define this situation as an invasion of privacy. However, they were less inclined than non-owners to describe it as a very serious invasion (43% vs. 53%).

• *Justification*

Seven-out-of-ten (69%) of Canadians found that there was no justification for automatic registration of calling numbers to a 1-800 service for marketing purposes. Compared with views as to the invasiveness of this practice, there was more consistency among respondents that this practice is not justified. For example, while younger respondents were less inclined to view this practice as an invasion than were older adults, about two thirds of both groups felt that it was unjustified.

• *Analysis*

These answers contrast with views held about "blind call-backs" (see below) which are made possible by the use of similar technology. Blind call-backs were seen as an invasion of privacy by only 30% of respondents, while almost 70% found ANI use by businesses (1-800 numbers) to be unjustified. But these results are consistent with opinions respecting telemarketing and unauthorized circulation of personal information by businesses. It appears that use of ANI by *individual subscribers* is not nearly as much of a problem as is non-declared use of the same technology by businesses.

Interestingly, younger, more educated and computer-owning individuals are more moderate in their assessment of the seriousness of what they nevertheless consider an ethical abuse and a breach of privacy. Results in other scenarios in this study also tend to show that younger respondents are more accommodating of business use of consumer information, and that more educated respondents are more nuanced in their assessment of the invasiveness of a given situation.

■ TELEMARKETING

Telephone solicitation is accomplished by directing sales calls to individuals or households targeted according to their consumption habits, socio-demographic profiles or geographic locations.

• *Experience*

Ninety-five percent (95%) of respondents reported having received uninvited telephone calls from someone selling a product or service. The majority of those not reporting such calls live in the Atlantic Region.

Individuals living in households with annual incomes less than \$15,000, Newfoundlanders and young adults were slightly less likely than average to receive these types of calls. Respondents with annual incomes over \$45,000 were a little more likely than average to report having received telemarketing solicitations. Those figures appear consistent with known telemarketing practices which tend to target particular market segments based on income and geographic location.

• *Invasiveness*

Although telemarketing solicitation is a common experience for Canadians, their perception of it as an intrusion varies greatly. Overall, a majority of Canadians (61%) share the opinion that uninvited calls from sellers are an invasion of their privacy.

However, those living in Atlantic Canada and Quebec were generally evenly divided (50%) on whether these types of calls were invasive. In the rest of Canada, and in particular Alberta (66%), respondents were more likely to feel that such calls are invasive. There also appears to be a direct correlation between age and feelings of invasion due to telemarketing calls: 56% of young adults feel invaded by such calls, but that figure jumps to 73% for seniors (age 65+).

Of the 61% who found telemarketing to be invasive, 40% considered the invasion to be moderately serious, 45% very serious, and 15% not very serious.

• *Justification*

A slim majority of Canadians (55%) did not consider this practice justified. It was only in Atlantic Canada that a majority considered it justified (PEI/NS: 55%; NB: 54%; Nfld: 48%). Strongest opposition came from Manitobans (70%) and British Columbians (59%). By age, seniors (65%) felt most strongly that telemarketing is unjustified.

• *Analysis*

Evidently, Canadians are divided into two groups: a bare majority which does not welcome unsolicited calls from telemarketers, and a large minority which accepts them without complaint. This divergence reflects the dual nature of telemarketing - as both an annoyance and a potential convenience or source of information. It may also reflect the amount of telemarketing to which each respondent was subject - the more calls one receives, the more likely one is to find the practice annoying.

With 61% reporting it as an invasion, and almost half of those considering it to be a very serious invasion, telemarketing must be recognized as a privacy problem. Compared with other potentially invasive scenarios, however, telemarketing falls in the middle in terms of relative concern: 27% of all

respondents found it to be a very serious invasion of privacy, vs. 71% for businesses selling personal information to others, or 6% for pharmacists exchanging data on customers. The more moderate level of concern about telemarketing may reflect greater control on the part of recipients (through answering machines, for example), and/or perceived benefits to those who purchase goods or services as a result of the call.

To the extent that telemarketers target individuals whose profiles indicate potential interest in the product of service being marketed, recipients may find the calls more acceptable. It should be noted, however, that while individuals *as consumers* may prefer targeted to untargeted telemarketing, *as data subjects* they are very concerned about the kind of information trading that is necessary for businesses to engage in targeted marketing (see most invasive scenarios, discussed above).

■ BUSINESSES MONITOR PERSONAL INFORMATION

• *Experience*

Canadians appear divided on their awareness and perceptions about businesses monitoring personal information for the purposes of target marketing goods and services to their clientele. Forty-four percent (44%) of respondents reported having definitely experienced this situation, while six percent (6%) stated that they thought they had done so.

A majority of residents of Newfoundland (55%)¹, New Brunswick (54%), and Quebec (52%) reported that they had never noticed such monitoring. In contrast, a majority of British Columbians (54%) and Albertans (53%) responded that they had observed businesses monitoring personal information for marketing purposes.

Awareness varies significantly with age, income, education, and computer ownership. Fifty-seven percent (57%) of the most educated respondents reported experiencing this situation, versus only 35% of the least educated. While fifty-three percent (53%) of computer owners claimed to have seen such monitoring practices, only 34% of non-owners did. Not surprisingly, 58% of persons claiming an awareness of personal information protection programs reported having seen businesses monitoring personal information for marketing purposes, versus only 41% of those who were unfamiliar with such programs. Finally, only 36% of young adults and 28% of seniors reported ever having experienced this practice, compared to 49%-52% of those aged 25-54.

• *Invasiveness*

Canadians are as divided in their opinions about the invasiveness of this practice (48%) as they are about having experienced it. (It should be noted that this question posited a company collecting information for its own subsequent marketing purposes.)

Socio-economic factors seem to influence attitudes to this practice. For example, 55% of less educated respondents viewed the practice as invasive, compared with 39% of the more educated. Similarly, 50% of lower income respondents, versus 37% of higher income respondents, defined monitoring as invasive. And, 55% of respondents who did not own a computer, versus 42% of computer owners, perceived monitoring to be invasive. The results suggest the presence of the following paradox: respondents who are least likely to be the target of business monitoring are most inclined to construe it as an invasion of privacy.

Sense of invasion was less common among those aware of programs protecting personal information (40%), versus those who were unaware (51%). Perception as invasive also grew significantly with age, from the youngest respondents (38%) to the oldest (67%). It may be that this trend reflects

¹ Figures exclude uncertain "yes" or "no" answers.

a greater degree of acceptance of a consumption-oriented society among younger people, as seems to be the case regarding other marketing techniques. Opinions about other personal information practices, however, are much more evenly distributed.

The majority (46%) of those who described monitoring as invasive viewed it as a very serious invasion of privacy (31% as extremely serious, 39% as moderately serious, and 14% as not serious).

Level of concern varied substantially according to socio-economic classification, along the same lines as did respondents' definition of the practices as invasive, namely according to gender, education, age, and ownership of a computer. Interestingly, however, concerns were fairly evenly distributed across income categories, indicating that if income is a factor in deciding whether the practice is invasive, it ceases to be a factor in judging degrees of invasiveness.

• *Justification*

Exactly half of respondents (50%) considered the practice justified. As in other cases, those who reported with certainty having experienced such business monitoring were, in fact, the most likely to consider it justified.

• *Analysis*

In this case, personal information is not collected directly from the individual, but rather is generated from transactional records. The information-gathering process involved here tends therefore to be hidden from consumers. This explains the high percentage of uncertain responses² regarding experience: 14%, with Manitobans (21%) and seniors (23%) displaying the most uncertainty.

As with some other practices, it appears that ignorance or lack of experience can lead to greater concern on the part of consumers. Nevertheless, perceptions of invasiveness are considerable even among the least concerned. While certainly not the most offensive practice among those presented to respondents, this one deserves attention by businesses engaging in it.

■ DRUG TESTING BY EMPLOYERS

• *Experience*

Only 3% of respondents reported having been asked to take a drug test by a prospective employer. These results are consistent with the fact that very few employers actually use drug testing. Those who reported having the experience tended to come from Alberta (5%), Québec (5%), Ontario (4%) and British Columbia (4%).

• *Invasiveness*

Canadians are divided in their assessment of workplace drug testing as a privacy invasion: 46% defined it as invasive, while 50% did not.

Newfoundlanders (58%) and Québécois (55%) mainly defined the situation as invasive, while New Brunswickers (62%), Albertans (58%) and British Columbians (54%) mainly saw it as non-invasive. As well, the older the respondent, the less likely they were to view the practice as invasive (rates dropping from 56% to 36% from youngest to oldest respondents).

Those who think drug testing in the workplace is invasive, generally viewed it as very serious: 44% defined it as a very serious invasion (36% as extremely serious); 37% as a moderately serious invasion; and 6% as not very serious.

² Uncertain responses include "Yes, I think so", "No, I don't think so", as well as non-respondents.

• **Justification**

Sixty-four percent (64%) of Canadians found drug testing as a prerequisite for employment to be a justified intrusion. There tended to be little variation in responses based on socio-economic variables, other than that more seniors found the practice to be justified, as compared to young adults (74% vs. 61%).

• **Analysis**

Opinions are sharply divided on both the invasiveness and the justification for drug testing. It is possible that some respondents construed "drug testing" as testing for illegal drugs (as opposed to legal drugs such as alcohol, pharmaceuticals or tobacco). This criminal dimension would bring a strong moral connotation to the issue, possibly explaining why there is division in perception of this issue even among unionized workers.³

■ **EMPLOYMENT STATUS AND BANK ACCOUNTS**

• **Experience**

Sixty-four percent of Canadians (64%) reported having been required to provide information about employment status in order to open a bank account.

Québécois and Albertans were asked most frequently (71% in each province), while only about half (49%) of Newfoundlanders were queried about employment status in applications. Only 41% of seniors indicated that they were asked to provide such information, while just over half (53%) of young adults (aged 18 to 24) reported being required to supply employment status information.

While it might have been expected that lower income people would be queried more often on this issue, such does not appear to be the case: lower income respondents reported having been required to provide employment information to the bank *less often* than did higher income respondents (rates increasing with income from 51% to 78%). Two factors may be at play here: persons with higher household income are more likely to have opened several accounts in different institutions, only some of which may demand to know such information. Also, individuals with higher household income are more likely to have applied for credit services (for example, mortgages, lines of credit, or loans) at the same time they opened an account.

• **Invasiveness**

A majority (56%) of Canadians viewed this request by a bank as non-invasive.

Québécois, who were also more likely to have reported being asked about employment status, were less likely to view this question as invasive (63% felt it was *not* invasive). Conversely, Newfoundlanders, who were the least likely of all provincial residents to report being asked for this information, were the most likely to define it as invasive (50% thought it was invasive). Similarly, those with higher education, while more likely to have experienced such an inquiry, were less likely to consider it invasive ("invasive" rates dropped with education, from 46% to 38%). The same applies with regard to income (rates dropped as income grew, from 54% to 35%).

Respondents who described the bank's inquiry about employment status as an invasion of privacy generally viewed it as a fairly serious violation: 46% of respondents who felt the question was invasive described it as moderately serious, 42% as very serious, and 12% as not very serious.

³ This finding is based on private communications with a Canadian Labour Congress representative.

• *Justification*

Sixty-two percent (62%) of Canadians find justified the collection of employment status information in bank account applications. Some regional differences are apparent: 70% of Québécois, 71% of New Brunswickers, and 68% of Saskatchewan residents believed the practice to be justified, while only 51% of Newfoundlanders did.

Analysis of respondents' household incomes reveals that the rate of defining such practices as "unjustified" is lowest (28%) among the highest household income respondents and highest (46%) among the lowest income respondents.

• *Analysis*

Not surprisingly, perceptions of the invasiveness and justification of such information collection by banks appear to be linked to employment and social status. In particular, views are closely correlated with perceived potential threat and with discomfort related to the disclosure of employment status.

The results can also be linked with the level of comfort people have in revealing their employment status. The more precarious one's employment status, the more likely this information could eventually bring a negative decision from the financial institution. Not surprisingly, unemployed respondents were more inclined to view such practices as invasive (47%) than were employed respondents (41%). This trend is even clearer when looking at responses according to nature of employment:

Is having to provide information about employment status in order to open a bank account an invasion of privacy?

Status	Yes	No	DK/NR
Self-employed	28%	64%	8%
Full-time	40%	60%	0%
Part-time	44%	54%	2%
Seasonal	49%	34%	17%
Other	55%	45%	0%

There is a clear link between the probability that information on employment status could lead to an adverse decision affecting the respondent, and the perceived invasiveness of the practice. The "Other" category includes students and seniors (who reported that they were not asked this information as often as others) as well as various categories of unemployed people. Yet, this category was most likely to find the practice invasive. Less secure economic groups may well fear that information on employment status could be used for some adverse decision affecting them.

■ **PHONE SOLICITATION BY CHARITIES**

• *Experience*

Eighty-five percent (85%) of Canadians reported having received uninvited telephone calls from a charity seeking a donation. The higher the income, the more likely respondents were to have received such a call (75% in the lowest income group to 96% in the highest). This practice also seems to have developed differently across the country. With levels of 75% for Québécois and 79% for Newfoundlanders, it appears that people in certain regions are less likely to receive phone calls from charities. Residents of Manitoba (93%) and Saskatchewan (92%) are the most likely provincial

residents to have received these sorts of calls.

• *Invasiveness*

Only 42% of Canadians find charity telephone solicitations to be a privacy invasion. This result varies by region: 71% of Newfoundlanders and 67% of Prince Edward Island/Nova Scotia respondents did not consider calls from charities to be invasive, while 45% of Manitobans and 44% of Ontarians did consider such calls to be invasive. As with telemarketing, this difference may be linked to variances in the amount of such calling, since level of annoyance is bound to increase with the amount of calls received.

Sense of invasiveness (whether or not the practice is invasive) increases with income (from 36% to 51%) and with age from young adults (29%) to seniors (53%). Tolerance, as well, seems to diminish with age: while only 10% of young adults found the practice to be an extremely serious invasion, 36% of seniors did so.

However, of those who found the practice to be invasive, higher income individuals generally viewed the invasion created by charity telephone solicitations as less serious than did lower income respondents (8% vs. 28% reporting "extremely serious"). The same trend was evident with increases in educational attainment: 29% of less educated respondents reported the practice as an extremely serious invasion, versus 13% of highly educated respondents.

• *Justification*

Sixty-four percent (64%) of Canadians considered calls from charities to be justified. Residents of Prince Edward Island/Nova Scotia (71%) and Alberta (70%) showed higher than average acceptance of telephone fund-raising efforts, and Manitobans (37%) the least.

• *Analysis*

Canadians perceive phone calls from charities as substantially less invasive than calls from telemarketers (42% vs. 61%). Of those who found them invasive, charity calls are less likely to be considered serious invasions of privacy than are commercial calls (32% vs. 45%).

The relatively low level of concern about charity fundraising through telephone calls is likely partially explained by the obvious social benefits these organizations provide in respondent's communities. However, such tolerance is not as evident with respect to the exchanging or selling of address lists by charities, a practice which is considered as invasive by 80% of Canadians, as noted above. Such trading of personal information is common among charities, and may well be used to derive lists for telephone solicitation. Charities should take note of these results, and should ensure that their donors are provided, at the very least, with an opportunity to opt out of any list trading.

■ RECIPIENTS RETURN CALL WITHOUT MESSAGE INVITING CALL-BACK

• *Experience*

A majority of Canadians (53%) declared having experienced someone returning their telephone call even though they did not leave a message. Such "blind call-backs" are likely to be triggered by the Call Display or Call Return function, but other factors, such as mere coincidence or recognition by one member of the called household of the caller's voice, could also be the cause of this situation.

Sixty-four percent (64%) of New Brunswick residents and 62% of Québec and Saskatchewan residents reported being surprised by at least one of these "blind call-backs." Respondents residing in those three provinces were more likely than all their other provincial counterparts to receive such calls.

Moreover, younger respondents were much more likely to have had the "blind call-back" experience than were seniors (64% vs. 35%). This phenomenon likely reflects more extensive use of Call Management Service, and of the telephone generally, on the part of younger respondents (see section of this report on Calling Number Display).

• *Invasiveness*

Sixty-eight percent (68%) of Canadians do *not* view "blind call-backs" as invasions of their privacy. On closer inspection of the answers, it appears that there are other factors influencing one's perception of blind call-backs. The majority of physicians (58%) and social workers/counsellors (52%) viewed such calls as invasive, while communications specialists (38%), accountants (37%), volunteers (37%), and those working in arts and entertainment (37%) appeared to be less offended by them.

Thirty-one percent (31%) of women responding to our survey regarded these types of call-backs as invasive, compared to 25% of men. There is also a small difference between unemployed respondents (of whom 34% characterized such calls as invasive) and employed respondents (27%).

Sense of vulnerability may also play a role in the assessment of the "returned calls" phenomenon. For example, perceptions vary greatly with age: only 18% of youngest respondents (ages 18-24) considered such calls to be invasive, compared to 43% of oldest respondents (ages 65+). Variations are also apparent between residents of small communities (where one is more likely to be known by his or her neighbours) and large urban centres (24% vs. 36%, respectively, find "blind call-backs" invasive).

Nearly half of all respondents (48%) who described "blind call-backs" as invasive characterized the invasion as moderately serious, while 35% called it very serious, and 16% described it as not very serious.

• *Justification*

Almost two-thirds (64%) of respondents view such an incident as justified. Differences related to gender, age and employment with respect to the perceived invasiveness of "blind call-backs" significantly diminish when dealing with perceived justification. This is explained by the fact that some among those who did not consider those incidents as invasive did not view it either as justified. For instance, only 25% of men perceived "blind call-backs" as invasive, but 31% found it unjustified. The same occurred with the youngest respondents: only 18% defined the practice invasive, but 24% considered it to be unjustified.

• *Analysis*

"Blind call-backs", unlike telephone solicitation, do not involve the processing of personal information. They are prompted by a call (often a wrong number) by the individual concerned, and are returned in many cases out of curiosity. For those who disapprove of them, they are an annoyance more than anything else. It is therefore interesting to compare perceptions of invasiveness as between this and other practices which are part of a larger information-processing scheme.

Blind call-backs rank low on the list of scenarios presented to respondents in terms of invasiveness. It may be that many of these respondents understood such return calls to come from someone already known to the original caller - both persons had previously and voluntarily exchanged telephone numbers. In such cases, it is less likely that a return call would be construed as invasive. On the other hand, the lower concern expressed about this practice may simply reflect its limited potential repercussions; the issue for some respondents may be more about lack of tact and good manners from the person returning the call, than it is about protection of one's own privacy.

■ EMPLOYMENT CANADA AND REVENUE CANADA SHARING INFORMATION ABOUT U.I.

• *Experience*

Seven percent (7%) of Canadians were fairly certain that they had experienced a situation in which Employment Canada and Revenue Canada shared information about them to ensure that they were not cheating on their unemployment insurance benefits.

• *Invasiveness*

Only one-out-of-four (26%) respondents defined this practice as an invasion of privacy. Respondents most likely to be affected by this practice were most likely to define it as invasive: perception of invasion was highest among the lowest income respondents (35% for less than \$15,000 annually), unemployed respondents (30%), as well as among the least educated (29%). Attitudes about invasiveness also varied by age: seniors tended to define this practice as invasive more than adults 25-34 years old (32% vs. 19%).

Among those who defined the practice as invasive, almost half (49%) viewed it as a very serious invasion (extremely serious: 35%); 39% as moderately serious; and 11% as not very serious.

Middle aged respondents (aged 35-44, 45-54) were more concerned (extremely serious: 43% and 46%) than youngest adults (extremely serious: 15%), while less educated respondents expressed greater concern than others (extremely serious: 39%).

• *Justification*

Four-out-of-five (79%) of Canadians found the sharing of information between Employment Canada and Revenue Canada to be justified.

• *Analysis*

The fact that this circulation of information is strictly between two federal government agencies, that it is limited to information about sources of income and, more importantly, that the question mentioned that the purpose is to detect fraud, were likely important factors considered by respondents.

■ REVENUE CANADA DEDUCTS OVERDUE CHILD SUPPORT PAYMENTS

• *Experience*

Only a small percentage (3%) of Canadians reported having experienced Revenue Canada deducting overdue child support payments from income tax refunds. More Newfoundlanders (6%) and Albertans (5%) reported experiencing the practice than did other Canadians.⁴

• *Invasiveness*

Less than one quarter of respondents (21%) viewed this practice as an invasion of privacy. Regional differences were evident: Ontarians (16%) were the least likely to view this situation as invasive, while Québécois (31%) and New Brunswickers (28%) were somewhat more likely than average to define it as invasive. Not only were New Brunswick residents among the most likely

⁴ Many respondents may have confused this practice with court-ordered deductions from salaries by employers (which do not involve the intervention of Revenue Canada).

to define the practice invasive, but two-thirds (67%) of New Brunswickers who thought so defined it an *extremely serious* invasion.⁵

Perception of invasiveness tended to diminish as education and income levels grew (from 26% for the least educated to 17% for the most educated; from 27% for those with incomes under \$15,000 to 15% for respondents in the \$60,000-\$74,000 range). Unemployed respondents (26%) were more likely to perceive invasiveness than were employed respondents (20%), and tradepersons (25%) were more likely than professionals (15%) to consider this practice invasive.

Gender also appears to be a factor: 19% of women defined it as invasive compared to 25% of men. As well, professional categories in which women are heavily represented tended not to see this practice as invasive (nurses 10%, teachers 13%). Interestingly, gender disappeared as a factor in assessments of the *degree* of invasiveness. Lower education and income, however, corresponded to greater levels of concern: 52% of least educated respondents vs, 31% of most educated found it to be very serious.

Among the 21% of respondents who perceived Revenue Canada's deduction of overdue child support payments from tax refunds as invasive, 46% found it to be very serious, 39% as moderately serious and 14% as not very serious at all. Translated into overall results, however, only 10% of respondents considered this practice to be a very serious invasion of privacy.

• *Justification*

Eighty-one percent (81%) of Canadians found this exchange of personal information to be justified.

There were, however, noticeable provincial differences: residents of Prince Edward Island/ Nova Scotia (88%), Ontario (87%) and Manitoba (85%) were more likely to view it as justified than were New Brunswickers (72%) or Québécois (76%). Allophones (69%) were much less likely to perceive the practice as justified than were Anglophones (84%) or Francophones (77%).

The 10% gap in opinions according to education and income remained in respect of justification: more educated and higher income respondents were more inclined to see the practices as justified (from 76% to 86% in both cases). A large gap also appeared between seasonal (66%), part-time and self-employed (75%), and full-time employed respondents (85%).

• *Analysis*

Attitudes toward this scenario reflect a strong pragmatic approach taken by Canadians to the use of their personal information by government. Not surprisingly, men (who tend to be payors of child support) perceive the practice as invasive more often than do women (who tend to be the recipients of child support), although the gap is not as large as one might expect. Those with lower income and social status tend to be more protective than others of their income, and less supportive of policies allowing for automatic deduction of child support debts from amounts owed to them.

⁵ These results could be linked to the recent New Brunswick governmental policy demanding that single mothers receiving social assistance declare the names of the fathers, so that the provincial government can sue on behalf of mothers to collect child support. The province further proposed that non-compliant mothers be disentitled from receiving benefits, prompting women's groups to launch a campaign to name Frank McKenna as the father on all birth certificates. Such events may be responsible for the anomalous results from New Brunswick on this particular issue.

■ PHARMACISTS EXCHANGE INFORMATION ABOUT PRESCRIPTIONS

• *Experience*

Only 13% of Canadians reported being aware of pharmacists exchanging information about them by computer. Women (16%) were nearly twice as likely as men (9%) to have experienced this situation.

• *Invasiveness*

Prescription information exchanges among pharmacists were viewed by Canadians as the least invasive of all fifteen scenarios presented to respondents: only 15% of all respondents defined it as invasive.

Just over twenty percent (22%) of Québécois and Newfoundlanders (21%) viewed the practice as invasive, compared to the relatively sympathetic residents of Prince-Edward Island/Nova Scotia (11%), and Westerners living in Saskatchewan (8%), Alberta (9%) and British Columbia (10%). Francophones (22%) were twice as likely to consider the practice invasive as were Anglophones (11%).

People living in small communities (less than 10,000 residents) were somewhat more inclined to define this type of exchange as invasive (20%). This is not surprising, given the relative lack of anonymity in small communities.

Of those defining this practice as invasive, 43% construed it as a very serious invasion; 40%, as a moderate one; and 17%, as not very serious. However, when the entire survey sample is considered, only 6% considered the practice to be a very serious invasion of privacy.

Highly educated respondents and respondents who were aware of protective laws and programs were more likely than their counterparts to view the practice as a moderate invasion of privacy, suggesting a trend of greater appreciation of nuances among those groups. The highest level of extreme concern (39%) was observed among seniors, who are also more reliant on pharmaceuticals.

• *Justification*

The capability of pharmacists across a province to exchange information about prescriptions for the purposes of ensuring that prescriptions received by clients are compatible was viewed as justified by the vast majority of Canadians (88%).

• *Analysis*

The views of respondents in this scenario were, doubtless, heavily influenced by the fact that the stated purpose of the information exchange was to facilitate safer use of prescription drugs by clients who fill prescriptions at more than one drug store. The personal benefit afforded by this activity appears to be a factor mitigating concern over privacy invasion and justification. Wide acceptance may also be due to the permissive (vs. mandatory) wording of the question ("pharmacists *can* exchange information").

TELEPHONE COMMUNICATION PRIVACY

- Call Display is a popular telephone service.
- Most Canadians are aware that they can block the display of their telephone number/ name, but very few use the blocking option.
- Canadians want Call Display blocking functions to be universally available, easy to operate, and free of charge, both on a "per call" and a "per line" basis.
- A majority of Canadians think that, as a rule, the blocking function should not be available to business subscribers.
- Attitudes of Canadians about Call Display and the blocking function appear to be driven by a desire to maximize the benefits of the technology in respect of both control of incoming calls and control of outgoing information.

• *Call display and blocking: awareness and use*

Subscribers to Call Display	23%
Awareness of Call Display Blocking	60%
Use of Call Display Blocking ¹	15% (9%)
Awareness of Other Protective Services from Telco: ²	23%
Unlisted Telephone Numbers	43% (10%)
Call Trace	17% (4%)
Call Screen	9% (2%)
Voice Mail, Call Answer, Call Waiting	12% (3%)

Call Display allows the person receiving the call to see the calling person's telephone number. Just a few years after its introduction across Canada, one quarter of surveyed Canadians reported subscribing to this service. Manitoba (9%) and British Columbia (14%) had the least number of subscribers at the time of the survey. Francophones (29%) and Allophones (28%) tended to subscribe more than Anglophones (22%). Also, the younger the respondent, the more likely they were to subscribe to the services (from 11% of seniors up to 29% among younger adults). Lower income groups were also slightly more likely to have the service (28%-30%).

Three-out-of-five respondents (60%) were aware of Call Display Blocking. Awareness was highest in Saskatchewan (75%), likely because of the publicity surrounding SaskTel's refusal to allow free display blocking (until recently), unlike other Canadian telephone companies. Age

¹ Only those who indicated awareness were asked if they used Call Blocking; the percentage results in brackets are in relation to the entire respondent sample.

² The services listed below were cited by respondents as examples of other protective services offered by the telephone company (unprompted; bracketed percentages are in relation to entire respondent sample).

appears to be a factor in awareness: the older one is, the less likely one knows about this function (from 68% for the youngest to 44% for the oldest). Awareness also grows with level of education (from 58% to 66% for university graduates), and with income (from 58% up to 69% for higher incomes). Those who are aware of legislation and/or programs protecting personal information are also more likely to be aware of the blocking service (73%) than are those who are not (58%).

Fifteen percent (15%) of those who knew of call number blocking functions actually used them, with a higher proportion from Québec (22%). Again, age is a significant factor in actual usage (from 28% for younger adults to only 3% for seniors). The \$15-\$29,000 income group, which had the highest call display subscribing rate, was also the highest user of blocking (25%).

• *Other telephone services*

Only 23% of Canadians were aware of any services offered by telephone companies to protect their personal information, other than Call Display and its blocking function (11% of whom were not able to give an example, and 13% of whom referred to either call display or its blocking function).

Most of those who were aware and did mention another protective service named only one. Awareness grew with education and income (both from 21% up to 28%). Those claiming to know of legislation and/or programs aimed at protecting personal information (31%) were more aware than those who did not (21%), while computer owners (26%) were more aware than non-owners (20%). Allophones (29%) and Anglophones (25%) were also more likely to declare being aware of other services than were Francophones (19%).

Unlisted phone numbers were mentioned by 43% of aware respondents. Call tracing (recording by the phone company of calling numbers -- even blocked ones -- for possible use by police) was mentioned by only seventeen percent (17%) of respondents. Translated into the overall population, this 17% indicates a minimal percentage of awareness (4%) among all respondents compared with high levels of awareness of call blocking (60%). Call screen was even less often cited (by only 9% of those who answered this question, which represents only 2% of all respondents). Twelve percent (12%) of respondents to this question cited voice mail, call waiting or call answer as other privacy-protective services.

• *Sources of information*

The following is a list of information sources from which respondents reported having learned about available services.³

Brochures sent by companies	41%
Word of mouth	29%
Media (television, radio, newspaper)	7%
Telephone directory	7%
Phone company	6%
Work/College	3%
Asked phone company	2%
Other	1%
Could Not Provide	3%

³ Only the 23% of respondents who indicated awareness of other services were asked this question.

Allophones are more likely to have learned from word-of-mouth (48%) than brochures (33%) while the reverse is true for Francophones (word-of-mouth: 28%; brochures: 41%) and Anglophones (word-of-mouth: 31%; brochures: 37%). The reliance on brochures as a primary source of information increased with educational attainment (from 35% for respondents with the lowest levels of educational attainment up to 45% for the highest), age (from 26% up to 56-54%) and income (32% with those with less than \$15,000, than growing from 29% (\$15-29,000) up to 52% for highest earners). The use of word of mouth as an information source does not vary significantly with either educational attainment or annual household income. Reliance on word-of-mouth sources was most prevalent among younger adults (40%), declining to 14% among older respondents, but increasing again to 23% for seniors.

• *Attitudes*

	AGREE	DISAGREE
Call Display is desirable	83%	7%
Call Display invades privacy	40%	42%
Call Blocking is desirable	74%	35%
Call Blocking is not a good idea	47%	35%

	AGREE	DISAGREE
Should not have to dial a code with each call in order to block display	53%	39%
Should not have to pay to prevent display	73%	25%
Should not permit blocking by businesses	58%	33%
Permanent line blocking should be available to all	81%	18%

Calling number display is different from more traditional data appropriation techniques, in which personal information is centrally collected and used through automatic means, and in which information subjects and information users tend to be distinct stakeholders (individual subjects and organizational users). With Call Display, the same individual can be both a subject and a user of information. As discussed in the introduction to this report, such situations are increasingly typical of the "information highway" environment, in which individuals are both producers and users of information and of transactional services. Thus, to study attitudes about call display is to open a window on possible, if not probable, trends in attitudes toward the treatment of personal information on the "information highway".

Only subscribers to CMS services can benefit from calling number display, but everyone, including non-subscribers to CMS services, will have their phone number and subscriber name (where technically possible) automatically circulated. Thus, attitudes toward the service are predictably equivocal. The key element to understanding the apparently conflicting opinions of respondents is *control*: people demand services that will provide maximum control over in-coming calls as well as maximum control over the disclosure of their personal information.

It is thus not surprising that a large majority of Canadians like the Call Display service - Call

Display gives people more control over incoming calls and has been found to alleviate the problem of harassing calls. At the same time, most respondents agreed with the statement that they should have access to call blocking in order to prevent their own number from being displayed whenever they want. In fact, Canadians agreed in the same proportion (73%) as for the desirability of call display blocking that people should not have to pay in order to prevent the display of their name or number.

A slight majority of Canadians thought that people should not have to dial a three digit code in order to block the display of their numbers. The younger the respondent, (and thus part of an age group more likely to subscribe to Call Display), the more likely they disagreed with dialling a code in order to obtain blocking (61% of youngest respondents disagreed, versus 45% of seniors). A much larger majority (83%) thought that people should have the option of permanent blocking on their telephone lines.

Respondents distinguished, however, between blocking by businesses and blocking by residents: when asked if businesses should be allowed to block their numbers, a majority answered "no"; one third said "yes" and six percent answered "depending on reason".

This strong acceptance of both Call Display and its blocking function for personal telephone users helps explain why Canadians were as likely to agree as to disagree, and were more likely to be undecided, with regard to the statement "Call Display intrudes on my privacy because it gives out my personal information without me knowing" (Strong agreement: 28%; neither or weak agree/disagree: 39%; strong disagreement: 32%).

The dual acceptance of Call Display and Call Blocking also explains the split responses to the statement "Blocking is not a good idea because it hides the identity of unwanted callers." Respondent attitudes to this question were mixed: 35% strongly agreed; 47% of respondents were in general agreement; 39% neither agreed nor disagreed very strongly; and 25% strongly disagreed.

It might seem that simultaneous preference for call display and display blocking is contradictory. But a closer look at respondents' answers reveals a strong internal logic. From the individual's standpoint, the simultaneous use of Call Display and Call Blocking assists Canadians in achieving their ultimate goal of maximum personal **control** over both incoming calls and outgoing information with minimum trade-offs or inconvenience. As we have noted throughout this study, *control* is at the centre of public attitudes about the use of personal information. Thus, level of control offered by a technological system design is a key feature for assessing that system.

In fact, the very success of Call Display in North America, despite the availability of free call blocking, is compelling evidence that individuals do like it both ways: i.e. to have both Call Display and the *possibility* of blocking. Translated into the interactive information age, we have some indication of what will drive Canadian's preferences with respect to systems and services design. It would appear that Canadians prefer a design that gives them maximum capability to process and use incoming information, while at the same time, maximum control over disclosure of their personal information.

These survey results should assist companies and regulators in designing an appropriate mix of services. In particular, we recommend the following based on the survey results:

1. Call Display should be a widely available service (either universal or on demand): even those who were not subscribers to the service felt it was "desirable" as a control tool.
2. Blocking functions should be universally available, both on a "per call" and a "per line" basis, easy to operate, and free.
3. As a rule, blocking should not be available to business subscribers (although some respondents would be open to the possibility "depending on reasons").

AWARENESS AND ACTION

- Canadians are largely unaware of legislation and programs protecting the privacy of their personal information:
 - Three quarters of Canadians are unaware of any law or government program protecting personal information, and fewer than one in five could actually cite an example; and
 - Only 14% of respondents knew about any private business initiatives protecting personal information, and fewer than one in twenty could actually cite an example.
- Canadians display low levels of awareness about where they can go for recourse when their personal information is abused.
- Few people request to see their personal information which is in the possession of businesses or institutions.
- Requests to see personal information were denied to roughly 12% of respondents who made them.
- One fifth of respondents who obtained access to their personal file detected errors in it.

Awareness of Legislation and/or Programs protecting privacy

Survey respondents exhibited little awareness of existing legislation and/or programs designed to protect the privacy of their personal information. Indeed, three quarters (73%) of Canadians were unaware of any law or government program related to protection of personal information. Of the one quarter claiming to be aware of such legislation or programs, over one third could not cite an example. Examples that were cited include:

- Access to Information legislation (36%)¹
- Privacy Acts (34%)²
- Charters of Rights and Freedoms (22%)
- Consumer Protection Acts (2%)³
- laws dealing with ethics (medical, financial, legal, etc.) (2%)
- Young Offenders Act (1%)
- Better Business Bureau (1%)
- various government statutes (1%)
- other (6%)

Only seventeen percent (17%) of Canadians were able to mention at least one governmental law

¹ It should be noted that provincial legislation dealing with protection of personal information in the public sector is often included within access to information legislation.

² The federal Privacy Act deals with protection of personal information held by federal public bodies. Many provinces have similar legislation for their public sector.

³ Most provinces have a Credit Reporting Act or equivalent legislation dealing with the use of consumer credit reports. Many other provincial statutes (such as those regulating professions or social and health services) also deal with this issue.

or program protecting privacy. The lowest rates of awareness were in Prince Edward Island/Nova Scotia (8%) and New Brunswick (11%) and the highest were in Ontario (22%). Not surprisingly, these rates grew with education (from 10% to 29%) as well as with income (from 11% to 31%).

Some industries also have their own codes of fair information practices, which are even less likely to be known by Canadians. Only 14% of respondents reported that they were aware of such programs, of whom only 36% were able to cite an example (5% of all respondents). The following examples were provided:

- (11%) professional codes of conduct/confidentiality**
- (8%) Better Business Bureau/consumer affairs**
- (4%) bank confidentiality/privacy codes**
- (3%) trust companies privacy codes**
- (1%) telephone companies' privacy codes**
- (2%) various governments statutes**
- (7%) other**

Responses often varied significantly among provinces. Quebecois tended far more than others to cite professional codes of conduct, while Maritimers more often than others cited the Better Business Bureau, consumer affairs, and trust company codes. In general, residents of Ontario, Quebec and B.C. were most likely to provide examples.

Prompting the names of government and business programs did little to improve the observed levels of awareness. The following statutes/codes elicited rates of familiarity as reported below:

- (40%) federal Privacy Act**
- (20%) provincial Privacy Act regulating the public sector**
- (19%) Canadian Association of Broadcasters Privacy Code (fictitious)**
- (17%) Provincial Credit Reporting Act**
- (13%) Provincial Privacy Act regulating the private sector**
- (13%) Federal Telecommunications Privacy Protection Principles**
- (10%) Canadian Bankers' Association Model Privacy Code**
- (10%) Canadian Chamber of Commerce Privacy Code (fictitious)**
- (7%) Trust Companies Privacy Code**
- (4%) Stentor Code on Privacy and Fair Information Code**
- (26%) Have not heard of any of the above**
- (11%) Non responses**

Levels of reported awareness were fairly even across regions of the country, even where the example provided did not exist. (Quebecois, however, were least aware of the federal Privacy Act (30% vs. 40% average), but were most aware of their own provincial privacy legislation.) In addition,

significant numbers of respondents claimed familiarity with non-existent codes, suggesting that these results may be tainted by a "social acceptance bias" (desire on the part of respondents to appear informed). Moreover, this question, which requires more effort than others in the survey, was asked near the end of a relatively long telephone survey. Results may therefore reflect fatigue on the part of respondents.

Whether tainted by a "social acceptance" bias, by confusion among similarly-named codes and statutes, or by simple fatigue, it is likely, as well as apparent, that respondents erred by overstating their familiarity. On the basis of these results, we therefore conclude that Canadians' awareness of legislation and programs related to protection of personal information is extremely low.

Low awareness was also exhibited with respect to sources of recourse in the event of perceived abuse of their personal information. When asked where they would go in such a situation, respondents gave the following answers:

- (35%) Lawyer/Legal clinic**
- (19%) Go to the source/service provider**
- (14%) RCMP/Police**
- (14%) Local elected official**
- (6%) Provincial ombudsman**
- (5%) Provincial Consumer Bureau**
- (3%) Provincial privacy or information commissioner**
- (3%) A consumer association**
- (3%) Better Business Bureau**
- (2%) Office of the Privacy Commissioner of Canada**
- (2%) Human rights commission**
- (2%) Government**
- (2%) Friend or relative**
- (1%) CRTC**
- (1%) Media**
- (1%) Blue Pages of telephone book**
- (2%) Other**
- (19%) Non responses**

A few geographic and socio-economic variances are worth noting: Quebecois were more likely to cite lawyers, provincial ombudsman, provincial consumer bureau and consumer association, than were other Canadians. Maritimers were more likely than others to say they would take their complaint to the service provider, to government, or to the Better Business Bureau (along with Albertans and British Columbians). University graduates and higher income earners were most likely to go to the service provider, or to local politicians for recourse. Allophones and young adults were most likely to think of the police as an appropriate source of redress.

Interestingly, the institution created by the best-known law or program in both public and private spheres is one of the least likely options for recourse, even among those who claimed to be aware of

government laws and programs: only 2% of respondents cited the federal privacy commissioner as a source of redress, and only 3% cited the provincial equivalent. Clearly, information and privacy commissioners need to make greater efforts toward raising public awareness of protection of personal information legislation and programs -- not to mention private sector programs. This may require expanding their mandates with a redirection of public funds from other areas into privacy awareness and protection.

Individual Action to protect privacy

Focus group sessions indicated that individuals feel compelled to play an active role in protecting their interests in relation to the use of their personal information. Scepticism about the capability of government/legislation alone to adequately protect individual rights and interests with regard to their personal information was a common theme. This view was consistent with the Ekos (1992) results which showed that, while a large majority of respondents favoured a legislative response (83%), as well as a cooperative approach between government and business to come up with guidelines for the private sector (80%), a significant number of Canadians still thought that it was also up to individuals to protect their own personal privacy (65% agreed, while 54% strongly agreed).⁴

In this survey, people were first asked if, within the past three years, they had ever requested to see personal information about themselves that was kept by a given institution.⁵ Those who had tried were then asked if they had been successful in obtaining the information, and if so, whether they had noticed any errors.

Requests for Information

Small percentages of respondents (1% to 18%, depending on the circumstance) reported requesting to see their personal information at some time in the past three years. The rarity of these requests is not surprising, given the low levels of awareness reported above. Another possible factor is that people are likely to seek access to a specific personal file only when there is a problem, or when an important decision is about to be made on the basis of such information.

	Doctor or Hospital	Bank	Employer	Credit Bureau	Gov't Agency	Phone Co.	Landlord
Access Attempted	18%	16%	11%	10%	9%	3%	1%
<i>Of those, Access Gained</i>	91%	94%	90%	85%	80%	87%	80%
<i>Of those, Error Detected</i>	10%	16%	17%	34%	27%	30%	16%

Young adults were much more likely to request access to their information kept by doctors/hospitals, banks and credit bureaus than were older respondents, and women were substantially more likely to ask to see their doctor/hospital records than were men. New Brunswickers and

⁴ Ekos 1992, p. 58-59.

⁵ Respondents were asked about banks, telephone companies, landlords, employers, credit bureaus, government agencies, and doctors/hospitals.

Newfoundlanders were most likely of all to have asked to see information held by their telephone company, but New Brunswickers were also least likely to have requested access to their credit reports.

A large majority of those who requested access were able to obtain it. Easiest access occurred with banks, employers, and doctors/hospitals. Those who knew about legislation or programs with respect to protection of personal information were more likely to secure access to their personal information, particularly in the case of credit bureaus. Manitobans were significantly less successful in obtaining access to doctor/hospital records (71% vs. 91% average).

A significantly high proportion of those who gained access found errors among personal information kept by credit bureaus, phone companies, and government agencies. In almost all instances, the more educated the respondent, the more likely they were to detect errors in obtained information. Ontarians detected errors in their credit reports most often (44% vs. 34% average). These figures are not necessarily indicative of overall error rates since it is often the very fact that someone *suspects* a possible error in his or her personal file that prompts the request in the first place.

REGULATORY PREFERENCES

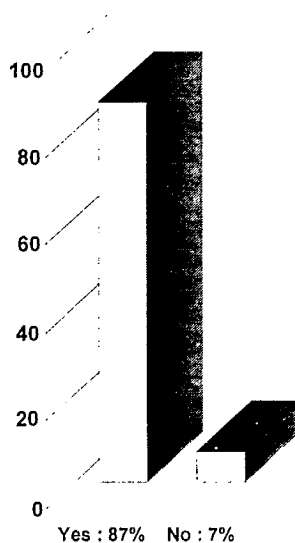
- **Canadians lack confidence in private sector self-regulation.**
- **Canadians distrust both private business and government in dealing with the protection of personal information.**
- **Public involvement is essential for both rule-making and enforcement; and**
- **Canadians think that governments should treat this issue as a priority.**

In 1992, both Ekos and Equifax found that Canadians considered privacy to be such an important value that governmental action was needed. Equifax found that 66% were in favour of a specific guarantee of personal privacy added to the Charter of Rights "as a guide for officials and to support legal actions by citizens". Ekos identified considerable scepticism about private sector self-regulation, as well as a strong support for active involvement of government, including legislation. Respondents were substantially agreed that government has an important role to play and that rules should apply to both the public and private sectors. Respondents also felt strongly that government should be working together with industry to develop rules.¹

Past surveys focused on the roles of government and the private sector in the process of defining rules for privacy and information transactions, but did not assess the public's views on the role of the public and consumer groups. Building on the previous survey work which clearly established that enforceable rules/legislation is required, this survey extended that analysis by assessing the public's views on the role consumer groups and the public should play. Respondents were not given a choice to rate each option, but were asked to choose their preference among three options. When asked which statement most closely agreed with their own views, only 7% of respondents chose industry self-regulation.² Twenty-one percent (21%) preferred government legislation, while a strong majority (69%) shared the opinion that neither private business nor government can be trusted to protect the personal information of Canadians, and that there is a need for greater public involvement in rule-making and enforcement.

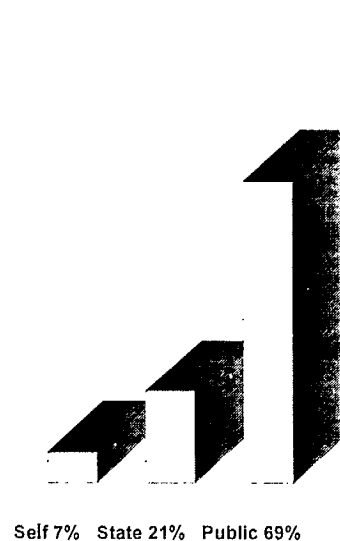
Protection of personal information should be a priority of government

Yes : 87%
No : 7%



Regulatory preferences for private sector :

Self regulation : 7%
State regulation : 21%
Public Involvement : 69%



¹ Ekos p.28.

² It should be noted that the Ekos asked about privacy whereas this survey asked about personal information.

These results mirror opinions expressed by focus group participants, who demonstrated a strong distrust of both business and government in relation to protection of personal information. Governments were viewed as being in a conflict of interest on this issue, because they are also among the largest personal information users. However, at the same time, only government is able to legislate and enforce privacy protection for Canadians. While respondents showed a disdain for government at a general level, as well as objecting to paying more in taxes for the protection of personal information (71%), they still felt very strongly that protection of personal information should be a priority for government (87%). In this regard, it should be noted that public oversight of personal information protection need not cost much.³

Canadians thus appear to view legislation as an important *part* of the answer. Their preference is for state initiatives that will also include individuals and consumer groups as participants in the solution. This is consistent with Ekos' (1992) conclusions that Canadians expressed both a desire for state action and an assertion that individuals must also have a key role to play.

At first blush, these results appear to contradict Equifax's conclusion (1994) that "most Canadians [74%] indicate that they would rather have businesses adopt good voluntary privacy policies as opposed to government regulation of privacy".⁴ There is no contradiction, however, since Equifax's question was heavily qualified, and did not ask respondents to choose a preferred option among two or more. Instead, respondents were asked to react to a single hypothetical statement:

If companies and industry associations adopt good voluntary privacy policies, that would be better than enacting government regulations, in this country. (emphasis added)⁵

Canadians would prefer not to unnecessarily increase government regulation, or to add to their burden as taxpayers. Yet, this survey, along with previous ones, reports a growing problem, as Canadians feel an increasing loss of control over their personal information. Canadians have more faith in government action, especially action which includes public involvement than industry self regulation or codes.

³ Québec, the only province in Canada with legislation for protection of personal information covering both the public and the private sectors, provides a good illustration: The annual budget of the Commission d'accès à l'Information for oversight of 250,000 to 800,000 potential data users (depending on sources) is \$2.9 m. That represents some 42 cents per year per Quebec citizen. As well, experience shows that sound implementation of personal data protection principles usually results in a reduction of costs of information management: P. Péladeau "Data Protection Saves Money", *Privacy Journal*, June 1995, vol.21, no. 8, p. 3-4.

⁴ Equifax (1994) p. XII.

⁵ Equifax 1994 p. 26.

APPENDIX A

Sampling strategy and weighting procedures

1. Sampling strategy

The survey sample was to consist of 2000 cases randomly selected from across private households in Canada. Eligible respondents were required to be over the age of 18 years and capable of responding to a telephone survey in either of the two official languages.

Households were randomly selected using a computer listing of telephone numbers. Additional numbers were randomized numbers using a process known as Random Digit Dialling (RDD), which involves altering the last digit of the telephone number to create a new number. This procedure ensures that households with unlisted numbers and more transient members of the population have a chance of being interviewed.

No stratification was imposed in the sampling approach. The final sample was to reflect natural population proportions. The sample was monitored as the survey data was collected to ensure adequate representation by province, sex, language.

2. Weighting procedures

Sociodemographic characteristics of the sample population were compared to Census data. From a comparison of gender, region mother tongue, age, income education, only mother tongue and age were found to be marginally different. Exhibit 1 below presents this comparison. Based on this, a weighting scheme was developed to adjust for the slight over-representation of younger Canadians in the sample. Since under-representation was consistent across age groups under 50 years of age, a weight was placed on respondents under 50, with another corresponding weight on those over 50. Similarly, based on slight under-representation of Allophones in the sample, six weights were developed - those of Anglophones, Francophones and Allophones first in Quebec then in the rest of Canada. This served to re-adjust the sample proportions slightly to reflect the true distribution of the population.

EXHIBIT 1

Comparison of sample and population

DEMOGRAPHICS	POPULATION	SAMPLE %
Gender		
Male	49%	50%
Female	51%	50%
Age		
20-24	10%	10%
25-29	12%	13%
30-34	13%	15%
35-39	12%	13%
40-44	10%	12%
45-49	8%	9%
50-54	7%	6%
55-59	6%	5%
60-64	6%	6%
65+	16%	9%
Mother tongue		
English	62%	65%
French	25%	26%
Other	13%	9%
Education		
High School	48%	42%
Trade school/College	34%	35%
University	15%	23%
Household Income		
Less than 15 K	16%	12%
15-30	21%	22%
30-49	26%	29%
50-60	11%	12%
60+	26%	25%

APPENDIX B

SURVEY MARGINALS

SHIFTING BOUNDARIES BTW PROTECTION AND INVASION OF PERSONAL PRIVACY

Hello, my name is _____ and I work for Ekos Research Associates. We have been hired by the Public Interest Advocacy Centre. The Public Interest Advocacy Centre is a not-for profit organization which provides legal representation and research support to individuals and groups on issues of public concern.

The survey focuses on issues of privacy and protection of your personal information. Your household was selected at random. Your responses will be kept **completely confidential** and participation in this survey is **completely voluntary**.

May I begin?

The first question has four parts. I will read some different examples and ask you four related questions for each situation.

1 a(i). If a business you deal with sells personal information it has about you to others without your consent. Have you ever experienced this situation?

Yes	1	19%	
Yes, I think so	2	7%	
No	3	54%	
No, I don't think so	4	19%	
DK/NR	9	2%	n=2035

a(ii). Do you consider this to be a privacy invasion [If a business you deal with sells personal information it has about you to others without your consent]?

Yes	1	95%	
No	2	5%	
DK/NR	9	1%	n=2034

a(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS	MODERATELY SERIOUS			EXTREMELY SERIOUS	DK/NR		
1	2	3	4	5	6	7	
0%	1%	2%	9%	12%	18%	57%	0%
							n=1933

a(iv). Is this situation justified?

Yes	1	12%	
No	2	86%	
DK/NR	9	2%	n=2035

1 b(i). If a business you deal with monitors the information it has on you and then tries to promote new services to you. Have you ever experienced this situation?

Yes	1	44%	
Yes, I think so	2	6%	
No	3	41%	
No, I don't think so	4	8%	
DK/NR	9	1%	n=2035

b(ii). Do you consider this to be a privacy invasion [If a business you deal with monitors the information it has on you and then tries to promote new services to you]?

Yes	1	48%	
No	2	50%	
DK/NR	9	2%	n=2034

b(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
2%	3%	8%	23%	22%	16%	27%	0%	n=934

b(iv). Is this situation justified?

Yes	1	50%	
No	2	46%	
DK/NR	9	3%	n=2035

1c(i). If a business you deal with provides personal information about you to a related company, without your consent, have you ever experienced this situation?

Yes	1	19%	
Yes, I think so	2	6%	
No	3	56%	
No, I don't think so	4	16%	
DK/NR	9	2%	n=2035

c(ii). Do you consider this to be a privacy invasion [If a business you deal with provides personal information about you to a related company, without your consent]?

Yes	1	90%	
No	2	9%	
DK/NR	9	1%	n=2034

c(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
1%	1%	4%	15%	18%	20%	42%	0%	n=1834

c(iv). Is this situation justified?

Yes	1	17%	
No	2	81%	
DK/NR	9	2%	n=2035

1d(i). If your employer tapes your telephone conversations at work to determine if you are doing personal business during work hours, have you ever experienced this situation?

Yes	1	5%	
Yes, I think so	2	1%	
No	3	88%	
No, I don't think so	4	5%	
DK/NR	9	1%	n=2035

d(ii). Do you consider this to be a privacy invasion [If your employer tapes your telephone conversations at work to determine if you are doing personal business during work hours]?

Yes	1	80%	
No	2	18%	
DK/NR	9	2%	n=2034

d(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
1%	1%	2%	9%	12%	15%	60%	0%	n=1656

d(iv). Is this situation justified?

Yes	1	28%	
No	2	69%	
DK/NR	9	3%	n=2035

1e(i). If a government agency sells a database which includes your health history to an insurance company, have you ever experienced this situation?

Yes	1	2%	
Yes, I think so	2	2%	
No	3	78%	
No, I don't think so	4	17%	
DK/NR	9	2%	n=2035

e(ii). Do you consider this to be a privacy invasion [If a government agency sells a database which includes your health history to an insurance company]?

Yes	1	90%	
No	2	9%	
DK/NR	9	1%	n=2034

e(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
1%	0%	4%	8%	13%	16%	61%	0%	n=1815

e(iv). Is this situation justified?

Yes	1	17%	
No	2	81%	
DK/NR	9	2%	n=2035

1f(i). If you receive uninvited telephone calls from someone selling a product or service, have you ever experienced this situation?

Yes	1	95%	
Yes, I think so	2	0%	
No	3	4%	
No, I don't think so	4	0%	
DK/NR	9	0%	n=2035

f(ii). Do you consider this to be a privacy invasion [If you receive uninvited telephone calls from someone selling a product or service]?

Yes	1	61%	
No	2	37%	
DK/NR	9	2%	n=2034

f(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
3%	5%	7%	22%	18%	14%	31%	0%	n=1204

f(iv). Is this situation justified?

Yes	1	41%	
No	2	55%	
DK/NR	9	3%	n=2035

1g(i). If you receive uninvited telephone calls from a charity seeking a donation, have you ever experienced this situation?

Yes	1	85%	
Yes, I think so	2	0%	
No	3	13%	
No, I don't think so	4	1%	
DK/NR	9	0%	n=2035

g(ii). Do you consider this to be a privacy invasion [If you receive uninvited telephone calls from a charity seeking a donation]?

Yes	1	42%	
No	2	56%	
DK/NR	9	2%	n=2034

g(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
5%	6%	10%	26%	20%	9%	23%	0%	n=820

g(iv). Is this situation justified?

Yes	1	64%	
No	2	33%	
DK/NR	9	3%	n=2035

1h(i). If you call a 1-800 number and your telephone number is automatically registered for marketing purposes by the business you called. Have you ever experienced this situation?

Yes	1	12%	
Yes, I think so	2	6%	
No	3	51%	
No, I don't think so	4	26%	
DK/NR	9	5%	n=2035

h(ii). Do you consider this to be a privacy invasion [If you call a 1-800 number and your telephone number is automatically registered for marketing purposes by the business you called]?

Yes	1	74%	
No	2	24%	
DK/NR	9	2%	n=2034

h(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
1%	2%	6%	22%	20%	16%	32%	0%	n=1492

h(iv). Is this situation justified?

Yes	1	28%	
No	2	69%	
DK/NR	9	3%	n=2035

1i(i). If you have to provide information about your employment status in order to open a bank account. Have you ever experienced this situation?

Yes	1	61%	
Yes, I think so	2	3%	
No	3	33%	
No, I don't think so	4	2%	
DK/NR	9	1%	n=2035

i(ii). Do you consider this to be a privacy invasion [If you have to provide information about your employment status in order to open a bank account]?

Yes	1	43%	
No	2	56%	
DK/NR	9	1%	n=2034

i(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
2%	6%	24%	24%	22%	16%	26%	0%	n=870

i(iv). Is this situation justified?

Yes	1	62%	
No	2	36%	
DK/NR	9	2%	n=2035

1(i). If a prospective employer insists that you take a drug test. Have you ever experienced this situation?

Yes	1	3%	
Yes, I think so	2	0%	
No	3	96%	
No, I don't think so	4	0%	
DK/NR	9	0%	n=2035

j(ii). Do you consider this to be a privacy invasion [If a prospective employer insists that you take a drug test]?

Yes	1	46%	
No	2	50%	
DK/NR	9	4%	n=2034

j(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
2%	2%	5%	17%	20%	18%	36%	0%	n=966

j(iv). Is this situation justified?

Yes	1	64%	
No	2	30%	
DK/NR	9	5%	n=2035

1k(i). If someone returns a telephone call even though the caller did not leave a message. Have you ever experienced this situation?

Yes	1	51%	
Yes, I think so	2	2%	
No	3	44%	
No, I don't think so	4	3%	
DK/NR	9	1%	n=2035

k(ii). Do you consider this to be a privacy invasion [If someone returns a telephone call even though the caller did not leave a message]?

Yes	1	30%	
No	2	68%	
DK/NR	9	2%	n=2034

k(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
3%	5%	8%	30%	18%	14%	21%	0%	n=565

k(iv). Is this situation justified?

Yes	1	64%	
No	2	32%	
DK/NR	9	4%	n=2035

l(i). If Employment Canada and Revenue Canada share information about you to ensure that you are not cheating on their unemployment insurance. Have you ever experienced this situation?

Yes	1	5%	
Yes, I think so	2	2%	
No	3	85%	
No, I don't think so	4	7%	
DK/NR	9	1%	n=2035

l(ii). Do you consider this to be a privacy invasion [If Employment Canada and Revenue Canada share information about you to ensure that you are not cheating on their unemployment insurance]

Yes	1	26%	
No	2	72%	
DK/NR	9	2%	n=2034

l(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
2%	4%	5%	20%	19%	14%	35%	0%	n=511

l(iv). Is this situation justified?

Yes	1	79%	
No	2	18%	
DK/NR	9	3%	n=2035

m(i). If Revenue Canada deducts an amount a court has ordered a delinquent parent to pay for child support from her or his income tax refund. Have you ever experienced this situation?

Yes	1	3%	
Yes, I think so	2	0%	
No	3	96%	
No, I don't think so	4	0%	
DK/NR	9	0%	n=2035

m(ii). Do you consider this to be a privacy invasion [If Revenue Canada deducts an amount a court has ordered a delinquent parent to pay for child support from her or his income tax refund]?

Yes	1	21%	
No	2	75%	
DK/NR	9	4%	n=2034

m(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
3%	4%	7%	20%	19%	15%	31%	0%	n=439

m(iv). Is this situation justified?

Yes	1	81%	
No	2	15%	
DK/NR	9	4%	n=2035

1 n(i). If pharmacists across the province can exchange information by computer about your prescriptions to ensure that the medications you are receiving are compatible? Have you ever experienced this situation?

Yes	1	11%	
Yes, I think so	2	2%	
No	3	79%	
No, I don't think so	4	7%	
DK/NR	9	1%	n=2035

n(ii). Do you consider this to be a privacy invasion [If pharmacists across the province can exchange information by computer about your prescriptions to ensure that the medications you are receiving are compatible]?

Yes	1	15%	
No	2	84%	
DK/NR	9	1%	n=2034

n(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
4%	6%	7%	21%	19%	16%	27%	0%	n=301

n(iv). Is this situation justified?

Yes	1	88%	
No	2	11%	
DK/NR	9	1%	n=2035

1 a(i). If a charity to which you donated money sells its list of donors to another charity. Have you ever experienced this situation?

Yes	1	28%	
Yes, I think so	2	11%	
No	3	47%	
No, I don't think so	4	13%	
DK/NR	9	2%	n=2035

a(ii). Do you consider this to be a privacy invasion [If a charity to which you donated money sells its list of donors to another charity]?

Yes	1	81%	
No	2	18%	
DK/NR	9	1%	n=2034

a(iii). [If Yes] How serious do you consider this situation to be an invasion of your privacy? Rate your answer on a seven point scale where one is not at all serious, 7 is extremely serious and the midpoint four is moderately serious.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
1%	3%	6%	20%	19%	17%	34%	0%	n=1649

a(iv). Is this situation justified?

Yes	1	22%	
No	2	76%	
DK/NR	9	2%	n=2035

2. How concerned are you about the linking of personal information which one organization has on you with the information which other organizations have on you in the following situations, using a seven point scale where one is not at all concerned, 7 is extremely concerned and the midpoint 4 is moderately concerned

2a. [How concerned are you with the linking of personal information...] If two or more government organizations shared information they have on you

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
16%	7%	6%	23%	12%	10%	25%	1%	n=2035

2b. [How concerned are you with the linking of personal information...] If two or more private firms shared information they each have on you

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
5%	1%	2%	14%	13%	17%	46%	1%	n=2035

2c. [How concerned are you with the linking of personal information...] If government departments and private firms link the information they each have on you.

NOT AT ALL SERIOUS		MODERATELY SERIOUS			EXTREMELY SERIOUS		DK/NR	
1	2	3	4	5	6	7		
6%	1%	3%	13%	12%	16%	49%	1%	n=2035

3a. Currently, telephone companies offer a service called Call Display which allows the person receiving the call to see the caller's telephone number. Do you subscribe to this service?

Yes	1	23%	
No	2	77%	
DK/NR	9	0%	n=2035

3b. Are you aware that you can block your number from being displayed on another party's telephone?

Yes	1	60%	
No	2	40%	
DK/NR	9	0%	n=2035

3c. [If Yes] Have you ever used this blocking service?

Yes	1	15%	
No	2	85%	
DK/NR	9	0%	n=1259

3d. Are you aware of any other services your telephone company offers to protect your personal information?

Yes	1	23%	
No	2	76%	
DK/NR	9	1%	n=2035

3e. [If Yes] Briefly describe the services you are thinking of

Call screening	02	9%	
Call tracing	03	17%	
Unlisted phone number	04	43%	
Star 67	05	10%	
Voice mail/Call waiting/Call Answer	06	12%	
Vista 2000/Call Display	07	3%	
Call forwarding	08	0%	
Other	01(0)	9%	
DK/NR	99(X)	11%	n=486

3f. [DO NOT READ LIST] Where did you hear of these services

Telephone Directory	1	7%	
Brochures sent by telephone company	2	41%	
Word of Mouth/Someone you know told you	3	29%	
Media (Television, Radio, Newspaper)	4	7%	
Phone company	5	6%	
Asked phone company	6	2%	
Work/College	7	3%	
Other (specify)	8(0)	1%	
DK/NR	9	3%	n=487

4a. Telephone companies offer different options for call blocking. Do you think people should have to dial a three digit code in order to block the display of their number every time they make a call?

Yes	1	39%	
No	2	53%	
DK/NR	9	8%	n=2035

4b. Should people have to pay in order to prevent the display of their name or number?

Yes	1	25%	
No	2	73%	
DK/NR	9	2%	n=2035

4c. Should business be allowed to block their numbers?

Yes	1	33%	
No	2	58%	
Depends on reason	3	6%	
DK/NR	9	3%	n=2035

4d. Should people who want to, be able to have permanent blocking on their telephone line?

Yes	1	81%	
No	2	18%	
DK/NR	9	2%	n=2035

5. With which of the following statements about Call Display and Call Blocking do you agree? Please rate your response on a scale of one to seven where "7" means you strongly agree, "6" means you agree, "5" means you somewhat agree, "4" means you neither agree nor disagree, "3" means you somewhat disagree, "2" means you disagree and "1" means you strongly disagree.

5a. Call Display is a desirable service because it gives people more control over the calls they receive and may help to avoid harassing calls

STRONGLY DISAGREE		NEITHER					STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7				
3%	2%	2%	8%	12%	24%	47%	1%		n=2035	

5b. Call Display intrudes on my privacy because it gives out my personal information to others without me knowing

STRONGLY DISAGREE		NEITHER					STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7				
20%	12%	10%	17%	12%	11%	17%	2%		n=2035	

5c. [Agree/Disagree...] I should have access to call blocking to protect my number from being displayed whenever I want

STRONGLY DISAGREE		NEITHER					STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7				
8%	4%	3%	10%	11%	19%	44%	1%		n=2035	

		STRONGLY DISAGREE		NEITHER			STRONGLY AGREE		DK/NR	
		1	2	3	4	5	6	7		
		15%	10%	10%	17%	12%	14%	21%	2%	n=2035
5d.	[Agree/Disagree...] Blocking is not a good idea because it hides the identity of unwanted callers									
6a(i).	Within the past three years, have you ever requested to see personal information about yourself that is kept by a government agency? IF MORE THAN ONCE..THINK ABOUT MDST RECENT EXPERIENCE									
	Yes	1				9%				
	No	2				90%				
	DK/NK	9				0%				n=2035
a(ii).	[If Yes] Were you able to actually obtain the information?									
	Yes	1				80%				
	No	2				19%				
	DK/NK	9				1%				n=200
a(iii).	[If Yes] Were there any errors?									
	Yes	1				27%				
	No	2				73%				
	DK/NK	9				1%				n=161
a(iv).	[If 6a(iii) =Yes] Within the past three years, have you ever attempted to CORRECT your personal information held by a government agency?									
	Yes	1				79%				
	No	2				21%				
	DK/NK	9				0%				n=42
a(v).	[If Yes] Were you successful in getting the information corrected?									
	Yes	1				74%				
	No	2				23%				
	DK/NK	9				3%				n=33
a(vi).	[If Yes] Were you satisfied?									
	Yes	1				68%				
	No	2				32%				
	DK/NK	9				0%				n=24
6b(i).	Within the past three years, have you ever requested to see personal information about yourself that is kept by your bank IF MORE THAN ONCE..THINK ABOUT MOST RECENT EXPERIENCE									
	Yes	1				16%				
	No	2				84%				
	DK/NK	9				0%				n=2035
b(ii).	[If Yes] Were you able to actually obtain the information?									
	Yes	1				94%				
	No	2				5%				
	DK/NK	9				1%				n=338
b(iii).	[If Yes] Were there any errors?									
	Yes	1				16%				
	No	2				83%				
	DK/NK	9				1%				n=315
b(iv).	[If 6b(iii) = Yes] Within the past three years, have you ever attempted to CORRECT your personal information held by Your bank?									
	Yes	1				89%				
	No	2				11%				
	DK/NK	9				0%				n=50

b(v).	[If Yes] Were you successful in getting the information corrected?			
	Yes	1	91%	
	No	2	9%	
	DK/NK	9	0%	n=44
b(vi).	[If Yes] Were you satisfied?			
	Yes	1	87%	
	No	2	12%	
	DK/NK	9	2%	n=39
6c(i).	Within the past three years, have you ever requested to see personal information about yourself that is kept by your phone company. IF MORE THAN ONCE..THINK ABOUT MOST RECENT EXPERIENCE			
	Yes	1	3%	
	No	2	97%	
	DK/NK	9	0%	n=2035
c(ii).	[If Yes] Were you able to actually obtain the information?			
	Yes	1	87%	
	No	2	13%	
	DK/NK	9	0%	n=66
c(iii).	[If Yes] Were there any errors?			
	Yes	1	30%	
	No	2	70%	
	DK/NK	9	0%	n=57
c(iv).	[If 6c(iii)=Yes] Within the past three years, have you ever attempted to CORRECT your personal information held by your phone company?			
	Yes	1	70%	
	No	2	30%	
	DK/NK	9	0%	n=14
c(v).	[If Yes] Were you successful in getting the information corrected?			
	Yes	1	100%	
	No	2	0%	
	DK/NK	9	0%	n=9
c(vi).	[If Yes] Were you satisfied?			
	Yes	1	100%	
	No	2	0%	
	DK/NK	9	0%	n=9
6d(i).	Within the past three years, have you ever requested to see personal information about yourself that is kept by your doctor/hospital. IF MORE THAN ONCE..THINK ABOUT MOST RECENT EXPERIENCE			
	Yes	1	18%	
	No	2	82%	
	DK/NK	9	0%	n=2035
d(ii).	[If Yes] Were you able to actually obtain the information?			
	Yes	1	91%	
	No	2	9%	
	DK/NK	9	1%	n=385
d(iii).	[If Yes] Were there any errors?			
	Yes	1	9%	
	No	2	90%	
	DK/NK	9	1%	n=346

d(iv).	[If 6d(iii)=Yes] Within the past three years, have you ever attempted to CORRECT your personal information held by your doctor/hospital?			
	Yes	1	68%	
	No	2	32%	
	DK/NK	9	0%	n=30
d(v).	[If Yes] Were you successful in getting the information corrected?			
	Yes	1	68%	
	No	2	32%	
	DK/NK	9	0%	n=21
d(vi).	[If Yes] Were you satisfied?			
	Yes	1	72%	
	No	2	28%	
	DK/NK	9	0%	n=15
6e(i).	[Have you ever requested personal information about yourself from...] Within the past three years, have you ever requested to see personal information about yourself that is kept by your employer. IF MORE THAN ONCE..THINK ABOUT MOST RECENT EXPERIENCE			
	Yes	1	11%	
	No	2	79%	
	Not Applicable (Self-employed)	3	3%	
	Not Applicable (Unemployed)	4	7%	
	DK/NK	9	0%	n=2035
e(ii).	[If Yes] Were you able to actually obtain the information?			
	Yes	1	90%	
	No	2	8%	
	DK/NK	9	1%	n=242
e(iii).	[If Yes] Were there any errors?			
	Yes	1	17%	
	No	2	81%	
	DK/NK	9	2%	n=218
e(iv).	[If 6e(iii)=Yes] Within the past three years, have you ever attempted to CORRECT your personal information held by your employer?			
	Yes	1	69%	
	No	2	31%	
	DK/NK	9	0%	n=38
e(v).	[If Yes] Were you successful in getting the information corrected?			
	Yes	1	72%	
	No	2	22%	
	DK/NK	9	5%	n=26
e(vi).	[If Yes] Were you satisfied?			
	Yes	1	80%	
	No	2	20%	
	DK/NK	9	0%	n=19
6f(i).	Within the past three years, have you ever requested to see personal information about yourself that is kept by a Credit Bureau. IF MORE THAN ONCE..THINK ABOUT MOST RECENT EXPERIENCE			
	Yes	1	10%	
	No	2	90%	
	DK/NK	9	0%	n=2035
f(ii).	[If Yes] Were you able to actually obtain the information?			
	Yes	1	85%	
	No	2	14%	
	DK/NK	9	1%	n=207

f(iii).	[If Yes] Were there any errors?			
	Yes	1	34%	
	No	2	65%	
	DK/NK	9	2%	n=175
f(iv).	Within the past three years, have you ever attempted to CORRECT your personal information held by a Credit Bureau?			
	Yes	1	74%	
	No	2	26%	
	DK/NK	9	0%	n=58
f(v).	[If Yes] Were you successful in getting the information corrected?			
	Yes	1	82%	
	No	2	13%	
	DK/NK	9	6%	n=44
f(vi).	[If Yes] Were you satisfied?			
	Yes	1	84%	
	No	2	13%	
	DK/NK	9	2%	n=36
6g(i).	Within the past three years, have you ever requested to see personal information about yourself that is kept by your landlord. IF MORE THAN ONCE..THINK ABOUT MOST RECENT EXPERIENCE			
	Yes	1	1%	
	No	2	70%	
	Not Applicable (Own home) ... B	B	29%	
	DK/NK	9	0%	n=2035
g(ii).	[If Yes] Were you able to actually obtain the information?			
	Yes	1	80%	
	No	2	20%	
	DK/NK	9	0%	n=29
g(iii).	[If Yes] Were there any errors?			
	Yes	1	16%	
	No	2	84%	
	DK/NK	9	0%	n=23
g(iv).	[If g(iii)=Yes] Within the past three years, have you ever attempted to CORRECT your personal information held by your landlord?			
	Yes	1	100%	
	No	2	0%	
	DK/NK	9	0%	n=3
g(v).	[If Yes] Were you successful in getting the information corrected?			
	Yes	1	100%	
	No	2	0%	
	DK/NK	9	0%	n=3
g(vi).	[If Yes] Were you satisfied?			
	Yes	1	53%	
	No	2	47%	
	DK/NK	9	0%	n=3
7a.	Are you aware of any laws or government programs that serve to protect personal information in Canada?			
	Yes	1	26%	
	No	2	73%	
	DK/NR	9	1%	n=2035

- 7b. [If 7a=Yes] [DO NOT READ LIST—DO NOT PROMPT IN ANY WAY] Please list those laws or government programs that you are aware of? [**** DO NOT PROMPT ****]
- | | | | |
|---|-------|-----|-------|
| Human Rights Legislation | 01 | 11% | |
| Access to Information Act | 02 | 166 | |
| Freedom of Information Act | 03 | 20% | |
| Privacy Act | 04 | 34% | |
| Charter of Rights and Freedoms | 05 | 11% | |
| Better Business Bureau | 06 | 1% | |
| Consumer Protection Act | 07 | 2% | |
| Law of Confidentiality | 08 | 0% | |
| Laws of Ethics - Medical, Financial, Legal, etc | 09 | 2% | |
| Various Government Acts | 10 | 1% | |
| Young Offenders Act | 11 | 1% | |
| Other (Please specify) | 97(O) | 6% | |
| DK/NR | 99(X) | 34% | |
| 14 | | % | n=533 |
- 8a. Are you aware of any private business program or code of practice aimed at the protection of consumer personal information in Canada
- | | | | |
|-------------|---|-----|--------|
| Yes | 1 | 14% | |
| No | 2 | 86% | |
| DK/NR | 9 | 1% | n=2035 |
- 8b. [If 8a=Yes] [DO NOT READ LIST—DO NOT PROMPT IN ANY WAY] Please list any business program or code of ethics laws or programs you are aware of which deals specifically with the protection of your personal information. [**** DO NOT PROMPT ****]
- | | | | |
|--|-------|-----|-------|
| The Canadian Bankers' Association Model Privacy Code | 01 | 4% | |
| The Stentor Code on Privacy and Fair Information Practices .. | 02 | 1% | |
| Trust Companies' Model Privacy Code | 03 | 3% | |
| Confidentiality/ Codes of Ethics - Medical, Legal, Financial ... | 04 | 11% | |
| Various Government Acts | 05 | 2% | |
| Better Business Bureau\ Consumer Affairs | 06 | 8% | |
| Other (please specify) | 97(O) | 7% | |
| DK/NR | 99(X) | 64% | n=282 |
9. [READ LIST.....ACCEPT UP TO 14 RESPONSES..PROBE FOR FURTHER ANSWERS] Which of the following privacy legislation and private business codes have you heard of?
- | | | | |
|--|-------|-----|--------|
| The Federal Privacy Act | 01 | 40% | |
| Your Provincial Privacy Act Regulating the Public Sector | 02 | 20% | |
| The Federal Telecommunications Privacy Protection Principles | 03 | 13% | |
| Your Provincial Privacy Act Regulating the Private Sector | 05 | 13% | |
| The Canadian Bankers' Association Model Privacy Code | 06 | 10% | |
| The Stentor Code on Privacy and Fair Information Code | 07 | 4% | |
| Trust Companies Privacy Code | 08 | 7% | |
| The Canadian Direct Marketing Association Privacy Code | 09 | 10% | |
| The Canadian Association of Broadcasters Privacy Code | 10 | 19% | |
| The Canadian Chamber of Commerce Privacy Code | 11 | 10% | |
| Your Provincial Credit Reporting Act | 12 | 17% | |
| [QUEBEC ONLY] The Quebec Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information | 13 | 10% | |
| [QUEBEC ONLY] The Quebec Act respecting the protection of personal information in the private sector | 15 | 5% | |
| Others not mentioned (specify) | 97(O) | 2% | |
| [DO NOT READ] Have not heard of any of the above | 98(X) | 26% | |
| [DO NOT READ] DK/NR | 99(X) | 11% | n=2032 |

10. Were you to experience an invasion of your personal information, who would you go to?

Go to the source/The service provider (bank, telephone company, cable company)	01	19%	
Federal Consumer Bureau	02	3%	
Provincial Consumer Bureau	03	5%	
Provincial ombudsman	04	6%	
Office of the Privacy Commissioner of Canada	05	2%	
CRTC	06	1%	
Your provincial Office of Privacy and Information Commissioner	07	3%	
Better Business Bureau	08	3%	
A Consumer Association	09	3%	
Local elected official (MP,MPP,MLA or Municipal official)	10	14%	
Media	11	1%	
Lawyer/Legal Clinic	12	35%	
RCMP/Police	13	14%	
Friend(s)/Relative(s)	14	2%	
Human Rights Commission	15	2%	
Blue pages (telephone book)	16	1%	
Government	17	2%	
Other (specify)	97(O)	2%	
DK/NR	99(X)	19%	n=2762

Please tell me if you agree or disagree with the following statements. Please rate your response on a scale of one to seven where "7" means you strongly agree, "6" means you agree, "5" means you moderately agree, "4" means you neither agree nor disagree, "3" means you moderately disagree, "2" means you disagree and "1" means you strongly disagree.

11. The collection and circulation of my personal information, aside, I am concerned about the decisions taken on that information, which affects me.

STRONGLY DISAGREE		NEITHER			STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7		
13%	6%	4%	11%	12%	21%	30%	3%	n=2035

12. I should not have to pay more to protect privacy of my personal information under any circumstances

STRONGLY DISAGREE		NEITHER			STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7		
5%	3%	4%	6%	7%	18%	57%	0%	n=2035

13. I don't mind making a special effort to protect privacy of my personal information to keep up with technological changes

STRONGLY DISAGREE		NEITHER			STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7		
9%	6%	5%	11%	18%	23%	26%	2%	n=2035

14. I feel that I have less control over my personal information than I did ten years ago

STRONGLY DISAGREE		NEITHER			STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7		
4%	3%	3%	11%	10%	20%	46%	3%	n=2035

15. I don't think it is necessary to notify me in advance when information about me is collected
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|-----|---------|----|----|----------------|----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 56% | 18% | 6% | 4% | 5% | 4% | 6% | 1% | n=2035 |
16. I am willing to pay more taxes to the government to enhance protection of my personal information
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|-----|---------|----|----|----------------|----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 56% | 18% | 6% | 4% | 5% | 4% | 6% | 1% | n=2035 |
17. I would find it useful to have more information on how new technologies might affect my privacy
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|----|---------|----|-----|----------------|-----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 3% | 1% | 2% | 6% | 12% | 27% | 47% | 0% | n=2035 |
18. Government should treat protection of my personal information as a priority but should not collect more taxes for this purpose
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|----|---------|----|----|----------------|-----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 3% | 2% | 2% | 5% | 8% | 22% | 57% | 1% | n=2035 |
19. I don't mind companies using information about me as long as I know about it and can stop it
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|----|---------|----|-----|----------------|-----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 10% | 4% | 3% | 5% | 12% | 26% | 41% | 0% | n=2035 |
20. I should be asked for my permission before an organization can pass on information about me to another organization
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|----|---------|----|----|----------------|-----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 2% | 1% | 1% | 2% | 3% | 17% | 74% | 0% | n=2035 |
21. When information about me is collected, I should be told what it will be used for
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|----|---------|----|----|----------------|-----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 1% | 0% | 1% | 2% | 3% | 19% | 73% | 0% | n=2035 |
22. I do not mind paying more to protect my personal privacy to keep up with technological developments
- | STRONGLY DISAGREE | | NEITHER | | | STRONGLY AGREE | | DK/NR | |
|-------------------|----|---------|----|----|----------------|-----|-------|--------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| 1% | 0% | 1% | 2% | 3% | 19% | 73% | 0% | n=2035 |

23. I should not have to make a special effort to protect privacy of my personal information, regardless of technological changes.

STRONGLY DISAGREE		NEITHER					STRONGLY AGREE		DK/NR	
1	2	3	4	5	6	7				
4%	4%	4%	5%	9%	23%	50%	1%		n=2035	

Which one of the following Three statements most closely agrees with your own views about how the privacy issue should be addressed.

24. Which of the following statements most closely agree with your own views

I am confident that private firms can regulate themselves to protect my personal information, without any intervention by government and consumer	1	7%	
Private industry cannot be trusted to regulate itself effectively; therefore government should pass legislation	2	21%	
Neither private business nor government can be trusted to protect the personal information of Canadians; there is a need for greater public involvement in	3	69%	
Other (Please specify)	4	1%	
NR/DK	9(X)	2%	n=2035

Finally, I would like to ask you just a few background questions and I remind you that all of the information you give me is completely confidential.

25. Do you have a computer at home or at work?

Yes	1	57%	
No	2	43%	
NR/DK	9	0%	n=2035

26. Do you sometimes have to place calls from your home for either paid or voluntary work that you do?

Yes	1	44%	
No	2	56%	
NR/DK	9	0%	n=2035

27. Which language did you first learn at home and still understand?

English	01	64%	
French	02	24%	
German or low german	03	2%	
Ukranian	04	1%	
Italian	05	1%	
Chinese	06	0%	
Spanish	07	0%	
Dutch	08	1%	
Other (Specify)	97(0)	6%	
DK/NR	99	0%	n=2035

28. Would you say that you are between:

18-24	01	10%	
25-29	02	12%	
30-34	03	13%	
35-39	04	12%	
40-44	05	10%	
45-49	06	8%	
50-54	07	7%	
55-59	08	6%	
60-64	09	6%	
65 years or alder	10	15%	
DK/NR	99	1%	n=2035

29.	What is the highest level of schooling that you have completed?			
	Elementary School or less	01	3%	
	Some High School	02	16%	
	Graduated High School	03	25%	
	Some community college/CEGEP	04	11%	
	Some university	05	10%	
	Graduate community college/CEGEP	06	11%	
	Undergraduate Degree (b.a. b. Sc.)	07	15%	
	Graduate Degree (Masters, PhD)	08	8%	
	Trade school	09	0%	
	Other	97(0)	0%	
	DK/NR	99	1%	n=2035
30.	Are you presently employed?			
	Yes	1	62%	
	No	2	38%	
	NR/DK	9	0%	n=2035
31.	What is your current employment status?			
	Full-time	1	76%	
	Part-time	2	19%	
	Self employed	3	3%	
	Seasonal	4	0%	
	Other (please specify)	8(0)	1%	
	NR/DK	9	0%	n=1362
32.	Which of these occupational groups best describes your current/most recent employment?			
	Semi-skilled	01	7%	
	Skilled Tradesperson	02	14%	
	Sales, service, clerical	03	20%	
	Professional	04	21%	
	Junior management or administrative	05	5%	
	Senior management or administrative	06	6%	
	Student	07	4%	
	Retired	08	14%	
	Homemaker	09	5%	
	Volunteer	10	0%	
	Disabled	11	0%	
	Other (please specify)	97(0)	1%	
	DK/NR	99	2%	n=2035
33.	Which of these professional occupational groups best describes you?			
	Nurse	01	12%	
	Doctor	02	4%	
	Engineer	03	12%	
	Social Worker	04	7%	
	Lawyer	05	2%	
	Politician (self-defined)	06	0%	
	Civil Servant (self defined)	07	5%	
	Teacher	08	25%	
	Technical	09	11%	
	Communications and Information	10	10%	
	Accountant/Other Finance	11	5%	
	Scientist	12	1%	
	Architect	13	0%	
	Fine Arts and Entertainment	14	2%	
	Other (please specify)	97(0)	2%	
	NR/DK	99	3%	n=445

34. What is your annual household income from all sources before taxes? Would you say is is...

less than \$15,000	1	10%	
\$15,000 - \$29,000	2	19%	
\$30,000 - \$44,999	3	19%	
\$45,000 - \$59,999	4	14%	
\$60,000 - \$74,999	5	8%	
\$75,000 or more	6	11%	
DK/NR	9	18%	n=1782

35. [SEX *** DO NOT ASK *** BASED ON OBSERVATION. The sex of the respondent is...]

Male	1	49%	
Female	2	51%	n=2035

Thank you for your cooperation and time!

Completion	1(D)	100%	n=2035
------------------	------	------	--------

36. About how large is the community you live in. Would you say you live in a community that has...[READ CATEGORIES]

Less than 1,000 people	01	7%	
Between 1,000 and 10,000 people	02	21%	
Between 10,000 and 100,000 people	03	32%	
Between 100,000 and 500,000 people	04	18%	
Over 500,000 people	05	20%	
DK/NR	99	2%	n=1709



QUEEN JC 596.2 .C3 S9 1995
Public Interest Advocacy Cen
Surveying boundaries : Canad

DATE DUE - DATE DE RETOUR

JAN 24 1996	

- Nouveautés -- New titles -
- 2 semaines -- 2 weeks -
- i (exp. 96-0²1-01) √ -