LESSONS FROM QUÉBEC: TOWARDS A NATIONAL POLICY FOR INFORMATION PRIVACY IN OUR INFORMATION SOCIETY

by

NICOLE-ANNE BOYER

B.A.(Hon.), University of British Columbia, 1993

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTERS OF ARTS

in

THE FACULTY OF GRADUATE STUDIES

(Department of Political Science)

We accept this thesis as conforming
to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

April 1995

In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Political Science

The University of British Columbia
Vancouver, Canada

Date 27 April 95

DE-6 (2/88)

ABSTRACT

While on the broadest level this paper argues for a rethinking of governance in our "information society," the central thesis of this paper argues for a national policy for data protection in the private sector. It does so through three sets of lessons from the Québec data protection experience. These include lessons for 1) the policy model, (2) the policy process, (3) the policy area as it relates to the policy problem as well as general questions about governance in an information polity.

The methodology for this paper is based on a four-part sequential analysis. The first part is a theoretical and empirical exploration of the problem, which is broadly defined as the "tension over personal information." The second part looks comparatively at how other jurisdictions have responded to the problem. The third part assesses which model is the better policy alternative for Canada and concludes that Québec regulatory route is better than the national *status quo*. The fourth part uses a comparative public policy framework, as well as interviews, to understand the policy processes in Québec and Ottawa so that we can highlight the opportunities and constraints for a national data protection policy in the private sector.

TABLE OF CONTENTS

List of Tables

List of Figures

Acknowledgments

Three individuals must be thanked for the idea and substance of this paper: David Flaherty, Colin Bennett, and Pierrot Péladeau. David Flaherty is the first to thank because he planted the seed in my head at a lecture he gave for the B.C. Legislative Internships Program last April. He then helped to frame the scope of my inquiry in a subsequent meeting. Colin Bennett was also instrumental in helping me focus this paper through yet another lecture I heard as an Intern, and a meeting in which he generously provided me with some important contacts for my research. Lastly, I want to thank Pierrot Péladeau for his insight and knowledge about Québec data protection. Without his help, Chapter Four and some of the "lessons" in Chapter Five would not have been possible.

This paper is dedicated to my parents,
whose love and support made
it possible.

Who steals my purse steals trash; 'tis something, nothing;
'Twas mine, 'tis his, and has been slave to thousands;
But he that filches from me my good name
Robs me of that which not enriches him
And makes me poor indeed.

Iago, in *Othello*
Act 3:3, (157-161)

Introduction: The tension over personal information

> A woman in Montréal tested positive for cancer at a local hospital. Several days later, to her surprise, she started receiving telephone solicitations for pre-arranged funeral packages. Apparently, the hospital sold her name, and the nature of her condition, to local funeral parlours for marketing purposes. While it is conjecture how the hospital rationalised this disclosure (aiding the provision of a necessary service to the consumer?) one thing is fairly clear: to a hospital in financially strapped times this was a source of needed revenue.
>
> Not surprisingly, the woman saw the situation somewhat differently. She was deeply disturbed that this kind of thing could happen, and decided to sue the hospital. She argued that the hospital had no business to violate her fundamental right to privacy and profit from her misfortune. A Québec court concurred, and awarded her $25,000 in personal damages.[1]

This true story is the central motif for this paper because the story crystallises a growing tension within our "information society": the tension over personal information. While this tension, at first, may seem like a minor technocratic problem, there are a multitude of very political questions that flow from its complexity. For example, in the most basic terms of power, questions surface: who controls information? Or, more normatively, who *should* control information? As the story indicates, the answer is no longer obvious.

At the heart of this tension is a barrage of conflicting imperatives that deeply penetrate modern society. Pulling on one side of the tension are the demands of economics. As the economy globalizes and competition increases, corporations increasingly need the free flow and exchange of information which, many argue, is founded on the corporate right to "free speech" and legal notions of "property." From the other side, however, are "human rights" imperatives; by these, we mean the democratic right to "information self-determination" which is simply the right to have some control over what happens to our personal data. Tugging from all sides and

enveloping both economics and human rights, is the third aspect of this tension: the double-edged nature of technology - specifically information technology - as it interacts with social change. In this respect, the tension over information highlights the fact that information technology, like many of its technological predecessors, has unanticipated consequences, some of which are positive and others negative.

In theory, the modern democratic state is the forum where these conflicting imperatives are somehow mediated in the form of public policy. Therefore, if public policy is "the pursuit of problem-solving upon society's behalf,"[2] in what ways can governments seek to ameliorate this complex, growing problem? What policy solutions or models are available so that policy-makers can draw useful and suitable lessons? It is to these last two questions that this paper is primarily devoted.

The Framework of Inquiry

The perspective of this paper is through the eyes of a policy-maker or policy-advisor looking at this problem as freshly and objectively as possible. The methodology or analytical logic is thus sequential. Chapter I surveys the theoretical and empirical origins of the tension over personal information, and then defines four parameters of the policy problem.

Chapter 2 moves on to the world of comparative public policy. It examines various policy responses to the problem, both international and domestic, within the field of data protection for the private sector. Data protection, in brief, is a policy innovation that helps to delineate the "information rights" of both the individual and organisation often through a set of "fair

information principles." In Canada there are present two divergent data protection models: one found in Québec's Bill 68 based on government regulation, the other found nationally based on self-regulation.

Chapter 3 assesses the two Canadian models through a set of criteria based on the requisites of the policy problem. The idea here is to determine, as objectively as possible, which model is best suited for Canadian public policy.

Having explored the two Canadian models from a rational perspective, Chapter 4 ventures into an equally important side of public policy: the politics of the policy processes. The project of this Chapter is to unearth the **salient variables** that drove the Québec outcome so that we can see the opportunities and constraints towards an analogous outcome at the federal stage.

The Thesis: Towards a national model for database protection

The findings of this sequential analysis - Chapters 1 through 4 - underscore the conclusion that Canadian federal policy-makers can learn some important lessons from the Québec regulatory model. This process of **lesson-drawing** is defined as "the process of deriving practical conclusions about the effectiveness of a program elsewhere and about its transferability to one's own political systems."[3]

The final chapter thus summarises the findings of three sets of interconnected lessons concerning (1) the policy model, (2) the policy process, (3) the policy area as it relates to the policy problem as well as general questions about governance in an information polity.

The first, and perhaps central, set of lessons suggests that the Québec model is the better policy alternative in terms of appeasing the conflicting imperatives within the tension over personal information. First, it meets the economic demands of industry by maintaining the free flow of information, increasing trade opportunities, preventing an imminent consumer backlash, as well as offering a host of instrumental benefits like increased efficiency in information systems and clarified liability (witness the $25,000 fine to the hospital). Second, it meets the human rights concerns by legislating "fair information principles" which guarantee individuals "information privacy" in both private and public sectors. This means that individuals have a right to know what is known about them, the right to correct inaccurate data about them, and the right to a means of redress in cases of personal information abuse. Lastly, the Québec model enhances the chance for effective governance of information technology in our nascent "information polity."[4]

For these reasons, it is argued that the Québec regulatory model be transformed into a national policy for data protection. Since information knows no borders, it makes little sense to have divergent policies with a statute that is designed to protect information privacy. It is therefore crucial that the national forum be the locus of policy-making so that this tension can be ameliorated in a comprehensive, enduring and future-conscious manner. Moreover, it makes equally little sense for regulation to be too costly for organisations. It is therefore argued here that a regulatory model for technology - like the Québec model - does not have to be the stereotypical, ineffective and onerous "bureaucratic solution." Instead, if properly thought-out, regulation in this case can work to the advantage of both individual and organisation.

The second set of lessons shift to the Canadian politics of data protection. The contextual evidence in both policy climates point to both opportunities and constraints for a national data protection statute for the private sector. Whether the policy "window" will be open to the opportunities or whether the constraints will predominant, largely depends upon one empirical relationship: the perceived and real cost of divergence compared to convergence.[5] For instance, in this case study the constraints that may impede a convergence to the Québec regulatory model include: the absence of a strong and unified consumer movement at the national level, the absence of a more in-tuned media in terms of privacy issues, the absence of political will and widespread public support, and economic constraints such as the cost of implementation. If these key elements are the salient ones, then a Québec -like development in Ottawa may be much longer in the making.[6] On the other hand, the policy window for a national policy for data protection could become open with highly publicised initiatives like the "Information Highway" that may focus a more steady public debate concerning the role of information privacy within our "information society." Apart from public opinion, other factors that may encourage a convergence are: the rising cost of divergence in terms of trade and the transborder flow of data, and the ability of policy entrepreneurs to convince national policy-makers and members of the CSA process of the merits of data protection for the private sector.

The third set of lessons delves into larger issues regarding data protection and governance in an "Information Society." It is suggested that if problems inherent in the tension over personal information are only a small example of what is to come, then present mechanisms - including

the policy area of data protection - will be hard pressed to meet the escalating demands of the new technological environment. It is argued that "governance in an information polity" will require both qualitative and quantitative changes in relation to the way governments manage technology in general. While it may seem like the tension over personal information is a minor matter to governance, it may be a precursor to a transformation of central precepts of modern democracy. In other words, information technology and the techno-political environment in which it coexists, may be changing notions of self-determination and a private life as we know them, as well as the socio-political relationship that exists between the individual and the modern organisation

Chapter One: Understanding the policy problem

"Whether the problem can be solved," observes Colin Bennett, "largely depends on how the problem is defined."[7] Therefore, to define the problem, one must first understand it as completely and satisfactorily as possible. In essence, this is the task of this introductory chapter: to survey the nature of the tension over personal information, and unearth the parameters of the problem so that it can be placed within a workable public policy framework.

1.1 Our Information Society

In a fundamental sense, society has always been an "information society." The need for intelligence about our surroundings - the instinct to reduce the uncertainty of our daily lives - is perhaps an essential component of the human condition.[8] With this being the case, what makes the role of information different within contemporary life? What makes our society one prefaced by the word "information"?

Intuitively, this can be easily measured by the increasing rhetoric of the "Information Age." On a daily basis we are inundated with news about the Internet, plans for the Information Highway, the spread of multimedia, E-Mail, Smart Cards and even electronic money for cyberspace markets.

Empirically, too, there seems to be a phenomenal explosion of the need for information in all facets of human activity. Statistics tell us that the "information sector" is growing exponentially,[9] and governments are increasing their expenditures in information technology dramatically.[10] Clearly, more and more, people are "engaged in the processing of information" for both work

and leisure.[11] At the centre of the problem, however, lies our theoretical understanding of the changing role of information within society. It remains quite unclear and highly disputed what lies beneath the quantitative and qualitative changes in the way we use information. For instance, what exactly is driving these changes: is the new information technology in itself precipitating these changes? Or is information technology just a subset of something larger like a more profound, historical process towards systemic change? As this section will argue, probably the most satisfying answer is that both of these things are happening in a simultaneous, overlapping and interactive manner.

(a) Information Technology

Where the human need for information has always remained constant, the historical role and character of information has varied substantively over time as new technological environments alter the societal configurations that govern its distribution and condition its use. The development of the printing press, for example, precipitated the spread of literacy which, in turn, lead to the democratisation of modern society.[12] Similarly, many analysts contend that information technology is becoming the historical analogue to the printing press, revolutionising the way we view and use information.

This is a tempting conclusion to make; however, whether or not information technology is in fact initiating an "Information Revolution" still remains to be seen. There is equally compelling evidence to suggest that perhaps larger, macroscopic forces may be the engine propelling these changes. Even so, there are nevertheless good reasons why information technology is being heralded in such consequential terms, and it is instructive to understand why.

Information technology owes its inception to innovations in micro-electronics which have enabled a powerful linkage between the high-speed capacity of the computer and the ubiquity and instantaeity of telecommunications. Information technology is therefore a marriage between "the carriage and content of information."[13] With an understanding of Harold Innis's taxonomy of technology, such a technological union would suggest that information technology may yield some interesting properties. Innis, for instance, argues that all communication media are "biased" in terms of binding space or time. Information technology, as we will see, may do both.[14]

While Innis did not live to dissect the nature of information technology, Iskender Gokalp tries to classify what its properties might be by describing it as "both global in *scope* and global in *structure*."[15] Information technology is global in "scope" because it connects disparate data-processing systems through telecommunication networks *instantaneously* and *ubiquitously*, thus loosening the constraints of both time and space. These two important properties give information its paradox; it is both centralising AND decentralising at the same time. Information can be held in one central database with individuals all over the world accessing it from their remote locations.

More difficult to understand, however, is that information technology is also global in "structure" because of its *density* and *multidimensionality* (or *interoperablity* according to trade jargon).[16] For example, Gokalp describes information technology as:

> "dominating all the branches of production by computerisation, automation, or robotization... and at the same time providing the infrastructure for humans' nonmaterial and noncommerical activities, from education to leisure"[17]

Information technology is therefore not just one kind of technology but many: it is the fax machines and modems, the databases and the fibre optics; it is the hardware and software of both the computer and telecommunications. This is possibly the reason why there is so many names of information technology. Some analysts have called it "information and communications technologies," or just "communication technologies." In recent years, however, information technology or the abbreviation IT seems to be the commonly agreed-upon term.

There is, of course, no consensus about the lasting or even immediate imprint of these properties upon social values and social change - only hypotheses. For the purposes of this analysis, one of the most profound and all-encompassing hypothetical repercussions of information technology's "biases" may be this:

> its propensity to augment the "interconnection and complementarity" *between* and *within* existing organisational structures, and systems of organisations, within the emerging world order.[18]

Information technology, for instance, seems to be blurring the distinctions between previously separate social spheres of politics, economics, and administration. This blurring can be see on four levels.

(i) The Globalization of information

On the largest level is the impact of information technology on transnational systems. Many analysts attribute numerous socio-political and economic trends to information technology because of its unique ability to transcend the constraints of time and space. Observers cite

trends in the world-wide rise of democratic movements, cultural diffusion, changing global patterns of consumption, increasing economic interdependence, and declining political autonomy.[19]

Of particular importance to this paper is the impact of information technology on the nature of international capital and global trade. Financial markets are now a complex web of transactions of all types that involve a "bewildering array of international funds and massive transborder capital movements." What interests many observers, like Francisco Sagasti, is that these markets now have "a life of their own" because they are "uncoupled from the production and distribution of goods and services."[20]

The transborder flow of data (TDF) has therefore become essential to the viability of international finance and trade as evinced by the cliché that "information knows no borders." While in practice this may not happen as easily as it sounds, corporations are operating in all corners of the world due to information technology. However, Raab and Bennett suggest that the actual quantity of personal TDF to date has been exaggerated. They argue that "[across the 'porous' border between Canada and the United States, the volume of personal data traffic as a percentage of all information flow is very small."[21] They nevertheless add that "the growth and change in information markets is greatly increasing the prominence of the international traffic in personal data..."[22] In short, there is every reason to predict that within the near future information technology will encourage a greater integration of information between countries.[23]

Another international ramification of information technology is its effect on the role of multinational corporations. It appears as if the technological convergence of the telephone, the television and computer is creating a trend in "mega-mergers." [24] This trend is troubling for both economists and political scientists mainly because the multinational corporation can not be held accountable for the political consequences of its actions.[25] While other factors, like the political climate of deregulation and increased competition, may also have contributed to the growth of these large corporations it is pretty clear that information technology is playing a predominate role.

Overall, this new state of affairs within the global economy - whether it be the transformation of financial markets, world trade, or multinationals - is being termed as "global economic restructuring." And within this new global milieu, several important international issues are requiring attention. These include greater pressures to harmonise international trade and co-operation, and legal questions surrounding intellectual property and copyright. Also, of particular importance to this paper, are concerns about the information handling practices of nations, and information privacy across borders.

(ii) The private-public sector blur

The second level where the impact of information technology can be seen descends to the nation-state. Here we see a blurring or convergence between the private and public sectors; between the organisational principles of political and economic administration. Gokalp cites the electronic deduction of taxes from employee pay-cheques, and the addition of taxes on goods and services, as concrete examples of the state directly dipping into the domain of commerce.[26]

Another illustration of this cross-over can be seen in the federal governments' *Blueprint for renewing government services using information technology.*[27] This document maps out the government's plan to establish "business rationales" for government services and a push towards a lateral integration of departmental information. The line between public sector information and private sector information will thus become even more fuzzy, as information moves more freely and invisibly from public database to private database in an effort to enhance administrative efficiency and respond to the new "rhetoric of consumerism" within modern bureaucracies.[28] Clearly, it is only people that recognise the distinction between the private and public sectors, not information. As a result, many European countries have rendered the distinction between the two as relatively "meaningless."[29]

Thus, governments are becoming like businesses with a new consumer-driven ethos and a fiscal mandate to "balance the books" like a corporation. Similarly, businesses are becoming like governments with their sheer size, growth, and ability to affect their "consumer citizens." Heilbroner, for instance, argues that despite the rhetoric about the growing size of government the private sector has grown far larger in relative terms.[30] The trend is thus for the private sector, and not government, to increase their reach and influence into the lives of the public.

(iii) The "re-invention" of the modern organisation

A third area where information technology is making dramatic changes is within the structure of organisations. The latest in management philosophy sees this ability of information technology in a very positive light. Tapscott's *Paradigm Shift,* and many others, herald information technology as "revolutionary" because of its ability to break down traditional

barriers within large organisations. He argues that not only will information technology "reinvent" the modern organisation to new heights of efficiency, but it will transform the way organisations function in everything from human resources management to strategic planning. In essence, these authors argue that information technology is "the" key to economic survival in the 1990s.

This idea is also particularly attractive to government bureaucracies. Government, increasingly, is "running up against the limitations of the bureaucratic/industrial mode of organising, and are exploring ways to develop more flexible, rapid response mechanisms that can mobilise a wider range of resources..."[31] Information technology may be the panacea that governments are looking for because it can break down departmental boundaries and integrate information flows laterally. The federal *Blueprint* embodies these ideas and trends in public administration.

Within industries, Lapierre *et. al.* also make sweeping statements regarding information technology. They contend that "the widespread use of computer and telecommunications facilities [information technology] was responsible for the change in the *modus operandi* of existing industries."[32]

Bellamy and Taylor nevertheless warn the technophiles about the widespread application of information technology within organisations. They argue that "the process of informatization disturbs inter- and intra-organisational relationships in ways that are not easily controlled or reordered."[33] Put in another way, information technology like many modern technologies has

unanticipated consequences; and one of the most notable consequences is the changing value of information.

(iv) The changing value of information

Lastly, and perhaps most importantly (at least as far as this analysis is concerned) is how information technology's "blurring effect" has altered the concept and value of information itself through the *commercialisation (or commodification)* of personal information. What this means in plain terms is that personal information is now readily bought, reconstituted, and sold for commercial profit; and by "personal information" we mean any information about an identifiable person - name, address, telephone number, income, occupation, credit-rating, hobbies or interests, etc. - in either manual or automatic form.[34]

For Vincent Mosco, the commercialisation of personal information alters the value of information in a way that he describes as "cybernetic." He illustrates this idea with a quote from the president of Olivetti Canada:

> ... You buy a magazine and pay for it with a credit card. A simple transaction? Hardly. The *information* about who you are and what magazines you prefer - recorded by computer - is worth as much as the return on the sale of the magazine. The information can be variously packaged. It can be marketed to others. Moreover, all the internal processes are affected by your decision - from marketing to purchase to finance...[35]

Information is thus cybernetic because "the very process of creating and exchanging information produces new products."[36]

In sum, there are four levels where it is becoming evident that the *scope* and *structure* of information technology is unquestionably influencing a multiplicity of social, economic and

political relationships. It is altering the concept and value of information as well as the functional designs of organisations. It is modifying the relationship between government and industry, government and citizen, industry and consumer.[37] It is even affecting both the geopolitical relations of nation-states and the possible emergence of a new world order.

We must nevertheless temper our conclusions by asking the question: to what extent is information technology "determining" these burgeoning changes? If it is, in fact, "the" defining element within these social transformations, then any political response is bound to be fruitless. Fortunately, this "deterministic" view[38] seems to fall apart when the impact of information technology is placed within the larger, macroscopic context of global systemic change.

(b) Global Systemic Change

Global systemic change is hard to define and even harder to measure. However in historical terms, systemic change is usually the marker that distinguishes one epoch from another. For example, the changes experienced during the Industrial Revolution - the systemic transition from an agrarian society to an industrial one - would be characteristic of a "systemic change."

Therefore these systemic changes, although extremely complex, can be understood as changes that have occurred within the *techno-political* environment. Techno-political, as defined by Bellamy and Taylor, is:

> **the environment created by macro decisions about the trajectory of technological development, and the broad social, economic, commercial and organisation factors that determine them.**[39]

What, then, are the relevant techno-political changes that may help us understand the changing nature of information within society, and in particular, the commercialisation of information? The answers to this question, of course, largely depend on the starting point of analysis and ideological bias. Roughly speaking, there are *two* general categories of debates concerning the changes within our techno-political environment. Both reveal some of the hidden assumptions at work within this complex policy problem.

The first group of debates can be split into the liberal and Marxist or radical view of the changing nature of capitalism. The Marxist or radical analyses look at the political economy of information. From this standpoint, they argue that the paradigms and patterns of information usage between individual and capitalistic organisations have been in place for quite some time. Vincent Mosco, for example, argues that the commercialisation of information should not be too surprising because "... information is encased in structures that are centuries old: the market, the production of commodities, exchange, pricing, and so on."[40] The emphasis is therefore on the ownership of the modes of production, the instrumental logic of efficiency, and the mechanisms of the market. It is the "economic and business logic of the information age" that is inexorably driving these changes.[41] The logical outcome, many Marxists propound, is the imperialistic creation of new transnational empires based on capitalism. In this case, "[b]igness is encouraged by regulation and technology. Supercompanies, supercountries, and megatrading blocks blossom."[42] Or, alternatively, these same forces could be creating a single "World Market." In both these senses, technology is clearly a subset of an economic order. Information technology is thus a tool or child of capitalism in that it carries and perpetuates the present economic orders' hidden values of efficiency and competition.

Another interesting sociological observation that frequently garners left-leaning analyses is the rise of "consumer capitalism." Instead of the manifestation of Big Brother, this view argues that "consumption, for the masses, has emerged as the new inclusionary reality."[43] The ideology of consumerism - the "buy,buy,buy" mentality - acts a new and perfected form of social control. It is perfect, as Foucault and others have demonstrated, because the individual self-polices herself. This happens because the tools of advertising propaganda and "consumer surveillance" internalise the market rules in order to regulate consumer behaviour.

More liberal analyses, while often taking in the critical insights from radical perspectives, are less deterministic. They see nothing inevitable in the trajectory of capitalism, with some scholars arguing that capitalism is becoming increasingly "disorganised." The most common outlook in this camp, however, portrays the shift of capitalism as a shift from "industrialism" to "post-industrialism." What society is witnessing is thus the concluding phases of a shift from an economy where the main resources were fossil fuels and steel, to a "knowledge-based" economy where the central resource exploited is information. Information is thus "the currency of the post-industrial economy."[44]

The second locus of debate concerning systemic change can be found within the *post-modern* perspective.[45] In contrast to the liberal and Marxists views, which see more continuity over the long term, this perspective argues that society is witnessing changes that are without historical precedent. Postmoderns thus spend much time distinguishing our era from the rest of human history.

The first argument, and possibly the most important, to put forward is the idea that "rapid discontinuous change" has become a permanent phenomenon. Societal changes are speeding up so quickly humanity no longer has, what Marshall McLuhan, calls "rear-view mirrors" to look behind us and understand what is happening.[46] However, the most important prediction that McLuhan and Powers make in the *Global Village* is in relation to information technology. They argue that the human mind cannot work at the speed of light, which it is increasingly being called to do with the instantaeity of information technology. This is bound to create considerable anxiety in the public consciousness, and people will need a place to hide from these technologies. However the problem is, according McLuhan, that these technologies will destroy what we know of the private sphere; there will be no place to hide.[47]

Wilson Dizard similarly contends in *The Coming of the Information Age* that society is experiencing the nascent stages of an entirely new epoch that will be ontologically different due to information technology; that is, individuals will have a whole new way of knowing and being compared to present norms.[48] Like McLuhan, Mark Poster argues that information technology is creating a whole new "mode of information."[49] For instance, he points out that human identity is being refracted through the medium of electronics, which is creating a dual image for the modern individual: one that is based on a "data-image" circulating within commercial and government data-bases, and another that is grounded in the "real self."[50] Thus, in this connection, Poster may be taking up Marshall McLuhan's seminal idea that "the medium is the message."

If the postmodern perspective places the emphasis on information technology as the driving force behind systemic change, does this mean we have come full circle? Not necessarily. While information technology may, in fact, be precipitating a whole new way of being within human existence, it remains one - albeit very important - variable in the dialectical calculus that creates our techno-political environment. This means that while technology may be changing parts of society at a more accelerated rate, other forces may be changing at a much slower pace, offering a modicum of stability over a longer period of time. Put in another way, information technology may not be "the" autonomous force within this dynamic societal equation but it may mirror, amplify or alter certain elements or values already present within a longer historical transformation.[51]

A useful metaphor to understand this dialectic is perhaps the biological model of homeostasis. Like a cell membrane, society is continuously readjusting and re-configuring to the entrance of new elements, the exit of old ones, and the commingling effect of the two as they overlap in the interchange.[52]

In terms of old elements, we have the elements that are integral to our evolving , capitalistic economic order: the instrumental logic of efficiency, notions of competition and the changefulness of capital, as well as the lure of the profit motive. These elements have been with us for hundreds of years; and in many respects, information technology reinforces their presence with society. There are also unmistakable signs of new elements entering society as well, with the unique characteristics of information technology, plummeting humanity into new ways of knowing and being.

What usually occurs when there is an overlap between the old and the new is numerous "grey areas" where there is much uncertainty. One of these areas, I would argue, is the point where the applications of information technology within the private and public sectors meet the values of democracy and human dignity. A quick revisit to the opening example about the woman in Montréal is ample testimony to this confusion and uncertainty about what is and is not the appropriate use of personal information.

1.2 The Commercial Use of Personal Information

As the first section illustrated, there are a myriad of reasons for the explosive growth in the use of personal information. They include larger shifts to a "knowledge-based," "post-industrial" economy, as well as the new environment created by the application and spread of information technology. However in plain commercial terms, it can be succinctly explained in one phrase: personal data is now worth money. The endeavour of this section is to detail why commerce has become so interested in personal information.

In particular, the powerful tools of databases, and their connectivity to other databases, have been an information technology that has been employed for a multitude of commercial activities - of which *four* will be discussed here: databases used for market research; tele-marketing and direct marketing; loss prevention; and as a foundation for new sectors of economic activity.

(a) Market Research

Marketing performs the instrumental function of promoting or persuading potential and present consumers to purchase, or continue to purchase in the future, the goods and services

that a company is offering. Market research aids in this effort by collecting data about consumers so that they can respond to, or predict, the changing supply and demand of markets. This concept is not a very old one, originating in the 1920s when Alfred Sloan from General Motors first postulated that the creation of customer "profiles" based on buying habits would be immensely useful in maintaining and targeting future market niches.[53]

Since then, databases have begun to revolutionise the way this statistical research is being conducted for two main reasons. Firstly, this is because what databases can do. By definition, a "database" is

> [the] collection of works or materials arranged, stored, and accessed by electronic means, and the electronic materials necessary for the operation of the database such as its thesaurus, index, or system for obtaining or presenting information.[54]

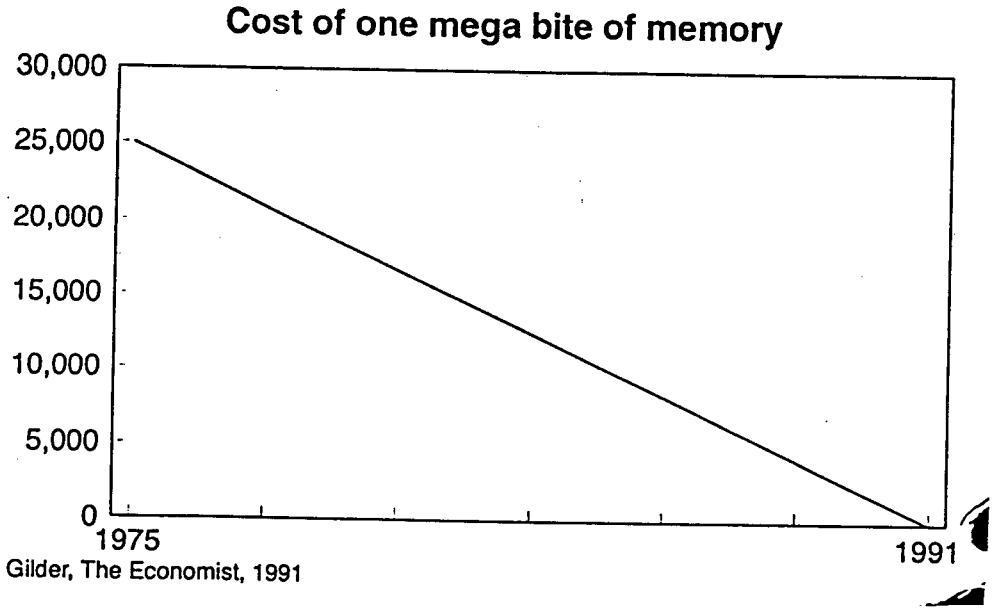
Therefore the term "database" is perhaps a misnomer. They are clearly more than just a device that houses data. A functioning database is more like an organism, "one that grows and changes at countless terminals, shaped and reshaped by users and compilers."[55]

For market research, databases are extremely useful because they can combine large quantities of socio-economic and geo-demographic information from national census data with other databases that have lists of names, addresses, telephone numbers, even income - or seemingly unrelated databases that have lists of club memberships, hobbies and interests, spending habits and purchasing power. This process of combining databases in novel ways is often called database "matching".

A recent illustration of the technical sophistication of databases is A.C. Nielsen's new service called SCANTRACK. At present, it monitors more than 41,000 households in the United States and can track a "brand's sale by distribution outlet, by how often a household has been exposed to commercials, and by purchase behaviour at different times of the year or day (important for seasonal or impulse items)."[56]

A second factor explaining the proliferation of databases is related to operational costs. In 1984 one megabyte of storage cost $25,000. By contrast, in 1994, the same megabyte of storage is was a mere $5. (see Figure 1.1)

Figure 1.1 The declining cost of database storage, 1975-1994



Gilder, The Economist, 1991

Thus, databases are financially accessible to almost any organisation with an application, whereas just ten years ago they were considered a luxury only for a large corporation or government.

(b) Database Marketing

A second use of database technology can be see within the exploding business of direct marketing and telemarketing, which together, employ the techniques of "database marketing (DM)."[57]

DM is significant because it perfects the efficiency, speed, and flexibility of the concepts of "Sloanism;" namely, the consumer profiling techniques like *targeting*, *tailoring*, and *tying*. For instance, a database marketer tries to seek out the *target* group of people that a particular service or good may appeal to. The most common target groups tend to be large demographic profiles like "baby-boomers," "yuppie-thirty-something," or the "generation Xers." The next thing a direct marketer tries to do is *tailor* down the target groups into one specific profile, and then make important linkages. For example, the middle-aged/male/ frequent-flyer may also be interested in a new life insurance policy; or a new mother who just bought a baby stroller may be interested in some diaper coupons. The third aspect of direct marketing is simply maintaining better *ties* with the consumer by sending them a newsletter or coupons as a reward for their patronage. According to one direct marketer, the ultimate goal of these marketing techniques is to create a "continuing dialogue" with consumers through direct communication or contact on either telephone or through mail solicitation.[58]

DM is therefore more focused. It utilises a micro approach to selling goods and services to actual consumers instead of statistical analysis on an aggregate level.[59] It is also why we hear the frequent question: "how did they get my name?" A company, thanks to databases, can access this type of information in one of two ways. First, it can purchase an already compiled list of potential clients from the database of a list broker. A Toronto-based company called Infomart, for example, routinely purchases a new-listing compilation from Bell Canada. This information is then repackaged, perhaps "matched," with other databases like new drivers' licenses from the Motor Vehicle Branch. This list may then be sold to market everything from new tires, to memberships to the Canadian Automobile Association.[60]

Also, a private organisation can easily create its own database due to the reduced cost of information technology. For example, a common method in building a database is through sponsoring a contest like a trip-for-two to Hawaii, or a large event like the Dragon Boat Festival, or, say, a performance by the Vancouver Symphony Orchestra. In return, the sponsor would receive prized, socio-economically specific, data about the participants.

Companies can also collect a large amount of data (that otherwise would be illegal in some provinces) through "joint ventures" or "cross promotional activities." Cathay Pacific, for instance, is an airline mainly geared for air travel to the far east. In order to reach this target group, Cathay may approach BC Tel for data on frequent long-distance callers to Hong Kong. Since BC Tel cannot by provincial law hand over this information from its database, it can for a tidy sum, send Cathay Pacific's promotional material to all the addresses within this target group.[61]

While most of the databases remain outside consumer knowledge, more recently corporations have been offering incentives or rewards to consumers who give them information. For example, MCI, a new American telephone company, has a new service called *Friends & Family.* The offer, or deal, is this: if a customer provides twelve names of people who need long-distance services, MCI will rebate 20% of that customer's long-distance bill.[62]

Another notable "customer rewards program" is Safeway's *AirMiles.* This marketing campaign represents the latest application in information technology, i.e. the use of "scanners," in obtaining valuable consumer data. The scanners are extremely useful because they link in a database the identification bar code on the back of your Airmiles card - that is, all personal information like name and address, even income (this is optional) - with the universal product codes of your purchases. The significance of this, according to Oscar Gandy, cannot be overstated:

> Scanning from point-of-purchase terminals, such as check-out counters in the supermarket, provides data at high speed and in real time about the status of the market as well as the responsiveness of consumers to variations in price and representation. The information helps in co-ordination of the distribution system that supplies the market with products in the right size, style, color, and so on to match the apparent tastes of the shoppers who frequent a particular store.[63]

There is also "the option of gathering information at the time of purchase by identified individuals."[64] This information can, in turn, be sold to other companies. Kraft Foods may want to know what brands it sells the most and to whom, and then market tailored coupons through the mail based on spending patterns. Similarly, a marketer may be interested in individuals who purchase expensive delicacies like caviar or ethnic speciality foods in compiling

certain socio-economic "profiles." The essential idea in *AirMiles* is based on an exchange: the consumer receives free air travel points in return for invaluable market research data on their purchasing habits. Not surprisingly, *AirMiles* has set the standard for the industry, and many other organisations are quickly following suit.[65]

Lastly, it should be mentioned that the most common source of personal information for databases is public. Addresses, telephone numbers, building permits, lists of property owners, and census data: all are on public record. A company, for instance, is presently marketing a CD rom package that compiles all the telephone books in Canada.[66] Commercial enterprises can therefore combine and "match" public data with other aggregations that they have collected from other sources. In addition, some governments have also begun to sell categories of lists, such as newly issued driving or fishing licenses, to private marketing firms as a source of revenue.[67]

(c) Loss Prevention

As we have seen through the linkage of scanner technology, databases have made industries unbelievably efficient in responding to consumer demand. Thus, databases prove indispensable in preventing loss of profits through increasing the speed at which information travels. Within the credit industry, databases also help businesses decrease losses through poor credit decisions.[68] Gandy's research tells us that American Express has over thirty-four million names in its international database and "detailed knowledge of where they travel, where they eat, and, increasingly, what they buy."[69] AMEX can then make assessments of creditworthiness -

thirty-two times a day - through a computerised classification program based on the users spending and consumption patterns.[70]

(d) The Electronic Information Industry

Clearly, the expanding number of uses for the commercial application of databases, and related information technology may be excellent news for the economy. As Table 1.1 shows, Information technology benefits traditional sectors as well as creating a whole new "electronic information" or "commercial data" industry.

Table 1.1 The electronic information industry	
Non-technical/ tradtional sectors	Technology sectors
Credit Banking Finance Marketing	computer hardware & software telecommunications hardware telephone, cable, wireless services electronic publishing & information services interactive multimedia development systems integration services
Information Technology Association of Canada (ITAC), The Canadian Information Infrastructure (June 1994).	

In the United States this industry is worth over fifty billion dollars.[71] In Canada, the database marketing sector alone sold $8.4 billion in goods and services last year in Canada.[72] In short, the commercialisation of information is becoming a lucrative line of business. Governments are consequently pouring resources and capital into information technology and infrastructures like the "Information Highway." According to a recent *Globe and Mail* advertising supplement for information technology, Canada has targeted $18 billion for a "high-tech marketplace" and will "spend a bundle on [information technology] products, services."

This electronic information industry, however, is still in its nascent stages; and as such, there are signs of growing pains as it begins to stretch the seams of society. These signs are manifesting themselves in a multiplicity of ambiguities, what I call "grey" issues, that remain unresolved and highly disputed. For example, questions of intellectual property - that is, who owns the data within the database - are very unclear.[73] This is largely because some databases collect *transactional data.* Transactional data is the information created by all electronic transactions. For example, new service order information like subscriptions to magazines, telephone call records, billing and credit records, calls to 1-800 numbers: all leave a "data trail" that has potential market value.

AT&T has recognised the value of data trails. In a 1991 legal battle, AT&T claimed ownership for all data that passed through its phone networks so that it could target frequent callers for marketing.[74] AT&T's customers, on the other hand, considered information about their calling habits - who they call, for how long, and where they call - to be *their* data.[75] The battles over information ownership, I would advance, will only escalate in the near future.

There are also serious concerns about the security of personal information within the database and while it travels through the permeable walls of "cyberspace." The emergence of a computer "hacker" culture (and underground industry) is making it impossible to guarantee the safety of information within databases. According to an article in *Scientific American* entitled "Trends in Communication: Wire Pirates" even the most sophisticated encryption scheme can be broken.[76] The fiasco around the Pentagon's so-called unbreakable "Clipper-Chip" is a case in point. However while epithets like "cyberspace crime" and "information warfare" are rapidly

entering the vernacular, the electronic information industry is down-playing the very real problem of information security.[77] And plainly, it is not in their interest to scare consumers.

Technical and legal details aside, however, perhaps the most important "grey" area that remains un-addressed is the larger issue of information privacy, and even wider humanistic concerns about the negative impact of these new commercial practices upon individual rights and identity.

1.3 The externality: Information Privacy

There are many ways to view the negative social effects of the commercialisation of information. This analysis adopts the economic term - *eternality* - to describe what often happens when the market produces undesirable consequences.[78] As Robert Heilbroner discusses in *Twenty-first Century Capitalism,* "all acts of production have external effects, both good and bad."[79] Seen in this way, it is hardly surprising, even expected, that the commercial use of personal information has the eternality of impinging upon the information privacy of individuals. Information privacy (to be distinguished from the culturally relative and vague concept of "privacy") denotes the ability for people "to determine for themselves when, how and to what extent information about them is communicated to others."[80]

To what extent, therefore, has the corporate use of personal information trespassed upon the information privacy of individuals? In empirical terms, this claim is hard to prove conclusively because there has been little study on these commercial practices. This is perhaps due to the newness of the problem. Also, it is rarely in a corporations interest to document the dubious

side of their activities both for liability and public relations reasons.[81] And lastly, seminal public policy studies like David Flaherty's *Protecting Privacy in a Surveillance Society* (1989) and Colin Bennett's *Regulating Privacy* (1992) focus on the impact of the public sector's use of these techniques and not the private sectors.

There are nevertheless several propositions that can be inferred from what we know about the corporate use of information. For starters, the characteristics of information technology - its ubiquity, instantaeity, density and multidimensionality - have taken the commercial transactions that involve our personal data away from our immediate consciousness. These transactions have become invisible with the sheer speed and complex circuitry of electronic communications. A U.S. study conducted by Cespedes and Smith supports this contention. They found that most people were surprised to learn that information was being collected and disseminated about them.[82] This is because "informed consent" for the disclosure of personal information is not mandated by law in North America. For instance, if one looks at the application form for Safeway's *AirMiles,* or other customer rewards programs, an individual would be hard pressed to find a consent clause, and if one does (which is slowly becoming a "good business practice") it is likely to be in "fine print" and rather cryptic. (See **Appendix 1.**)

Thus, almost by definition, businesses are trespassing upon our information privacy. The average person does not and cannot "determine for themselves when, how and to what extent information about them is communicated to others." The important question is: what are the social and political impacts of this infringement?

Industry analysts argue (although not all) that invasions of information privacy are relatively innocuous. In their view, it is a reasonable trade-off for added benefits like increased consumer choice and the speed and efficiency of service. They also contend that a loss of information privacy is minimal and over-exaggerated by privacy advocates because industry guidelines and "privacy codes" are in place to prevent any kind of information abuse.

Privacy advocates tend to counter industry's arguments with the fact that information abuse still occurs - some contend at a growing rate. It is suffice to recall our introductory example of the "Woman in Montréal." There are many others like it; some "horror stories," others just minor inconveniences like a misplaced number or an incorrect name. The reality is that, in practice, most Canadians have little or no formal control over the use of their personal data once it enters the porous walls of cyberspace. Studies also show that a frightening percentage of the personal data within any given commercial database is inaccurate, yet there is no form of redress is available if a serious abuse occurs, other than the cumbersome and expensive court system. In short, there is no such thing as information privacy.

Consequently, the civil libertarian perspective sees the problem as a political imbalance in terms of democratic human rights. Information privacy they persuasively argue "is essential to maintain a free society. It is fundamental to the democratic notion of self-determination or autonomy - of retaining control over our lives."[83]

For the sake of a healthy democracy, individuals must therefore have a fundamental right to control the details of their lives, the right to "informational self-determination," and the right to know what other people know about them. Achieving this, however, is highly problematic

because "in the headlong rush to assemble information, companies and governments often forget who owns the information."[84] The problem then reverts to questions about who owns personal information. Is it the individual or banks or credit reporting agencies?

Sociological analysts, however, see the situation as beyond the notion of information privacy. Gary Marx maintains that commercial practices have the very real potential to assail and diminish human dignity. This assertion, at first, may sound far-fetched. However it is amazing how the simple "matching" of computer databases, in novel combinations from a variety of sources, can have some serious negative social implications. Marx powerfully illustrates how this could happen:

> "Purchasers of pregnancy-testing kits may receive solicitations from pro- and anti-abortion groups, or from sellers of birth-control products and diaper services. Purchasers of weight-loss products or participants in diet programs may be targeted for promotional offers from sellers of candy, cookies and ice cream, or conversely, those whose purchases of the latter exceed the average may receive offers for weight-loss products and services. Subscribers to gay and lesbian publications may be targeted by religious and therapeutic organisations or face employment denials, harassment, and even blackmail."[85]

Cespedes and Smith also point to the negative ramifications of "exclusion" in the commercial use of personal information. As they argue, "in most Western societies, people from different race, religions, and ethnic groups tend to live in distinct areas, and income and education are also highly correlated." Thus the "segmentation criteria are not socially neutral. Certain groups can be substantially under-represented in targeted campaigns, in effect widening the gulf between lower- and upper- income groups."[86] Wealthier households tend to get more coupons, more "special offers" on things like furniture or cars, and more applications for credit -cards; whereas the lower income groups tend to not make the marketers' list.

There is also evidence that the reach of these transactions is becoming more pervasive and extensive than ever before. In essence, commercial activities are entering the "domestic threshold"[87] of our lives through the telephone and "junk mail." While this may increase consumer choice and convenience, it also has a darker side in that it can affect our "life-chances," often unconsciously, through decisions made about credit-worthiness.[88]

Similarly, and more radically, Oscar Gandy's *The Panoptic Sort: The Political Economy of Personal Information* (1994) views "consumer surveillance" in more systemic terms and describes it as the "panoptic sort": "the all seeing eye of the difference machine that guides the capitalist system ... a high-tech, cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value."[89] Indeed, in one of the most exhaustive studies about the impact of consumer surveillance on society, Gandy makes a convincing empirical case.

Democratic theory aside, there is also an important psychological dimension for the need of information privacy. Cathay Goodwin's analysis demonstrates this by combining behavioural psychological with public policy theory in her 1991 article, "Privacy: Recognition of a Consumer Right." She argues persuasively that individuals have negative social reactions from the impression that they have little control within their external environment.[90]

While there will be much disagreement about the impact of these practices upon the individual - whether it be in terms of democratic theory, sociology, political economy, or psychology - one thing is clear: there is substantial empirical evidence documenting the public's growing

concern about the intrusiveness of technology on information privacy. In Canada, there have been two influential surveys indicating this mood within public opinion. The first was *The Equifax Report on Consumers and Privacy in the Information Age* released in 1992, and the second was *Privacy Revealed: Public Perceptions of Privacy in Canada.* The findings of both surveys were very similar: in the Equifax survey, 58% of Canadians rated privacy as "extremely important;" while the Ekos survey shows 52% of Canadians as "extremely" concerned with the issue of privacy and a total of 92% who are at least "moderately" concerned. Thus one of the conclusions of the Ekos survey states that "there is a pervasive sense that personal privacy is under siege from a range of technological, commercial and social threats."[91] In short, privacy is slowly becoming an important issue within Canadian political culture.

It would be a mistake, however, to paint public attitudes towards privacy as homogenous. Most survey research on privacy find significant group variation in public opinion. The Ekos survey, for instance, finds five segments of Canadians in terms of attitudes towards privacy and new information technology as summarised in **Table 1.1**. Across attitude segments, in general, the survey results find that elderly Canadians, the less educated, women, and francophones are more concerned about their loss of privacy.

Table 1 Public opinion attitudes towards privacy

Fearful Regulators (31 per cent)

This group is fearful about the insidious possibilities of new information technology. Regulators are a relatively sophisticated group. They are over-represented by white collar Canadians, women and Quebeckers. This group seeks strong governmental controls.

Extroverted Technophobes (23 per cent)

This group has even stronger anxieties about the unknown possibilities of technology and its impact upon privacy. This group tends to comprise mainly the poor and the elderly.

Guarded Individualists/ Self-Reliants (6 per cent)

This group shows a moderate level of concern about technology and privacy, but does not see government intervention as necessary. It sees individual self-reliance and responsibility as the key solution. This group tends to be younger and computer literate.

Open Pragmatists (22 per cent)

This is the middle-of-the-road group. These respondents are not too concerned about new technology and reveal no notable social and demographic characteristics.

Indifferents (18 per cent)

This group is not highly engaged by privacy issues. These respondents tend to be younger, less educated, and francophone.

Source: *Privacy Revealed.* Ottawa: Ekos Research Associates (1993)

In a similar vein, it would be inaccurate to depict industry as homogenous in its stance on privacy. In recent times, (especially since the privacy surveys) there has been a noticeable shift in corporate attitudes. Also, with new "principle-centred" approaches to management, it has simply become a good business practice to pay attention to individual privacy.

1.4 Parameters of the problem

Without question, this policy problem is far from a technocratic glitch in the use of personal information. It is a montage of conflicting imperatives and rights, social values and social groups. It is thus worthwhile re-stating the parameters of the problem. In reduced form, this particular policy problem has four interrelated dimensions; and it has roughly three stake-holder groups, that is, discernible groups of people that have a stake in the commercial use of personal information.

The Dimensions of the problem

1. The techno-political dimension

The problem is a by-product of a changing and globalizing techno-political environment. It is emblematic of the shift of modern capitalism to a knowledge-based economy, as well as the new environment created by information technology. The role of information has become central to the operations of the modern organisation in both government and industry. The growing presence of information technology is also accelerating and contributing to the complexity of society. Its enigmatic properties of ubiquity, instantaeity, density, multidimensionality, and invisibility may be bringing about a different epoch, possibly a "postmodern" one, where society will be ontologically and epistemologically different. Important trends to watch are the increasing rise of "consumerism" as the central characteristic defining human activity and identity; and the decreasing salience between the distinctions of the "private" and "public" sectors through the development of electronic infrastructures.

2. The international dimension

The international implications of this problem remain contingent upon the techno-political domain. Two factors are nonetheless important. Firstly, there are growing pressures to harmonise laws and information handling practices as the transborder flow of data increases. Canadian citizens need to be assured through further international co-operation that their information privacy is protected across international borders.[92] Secondly, the role of multinational corporations' use of personal data, and ultimately their lack of organisational accountability, will be a pressing part of this problem in the near future as global trade increases.

3. The economic dimension

The economic dimension, also a subset of the techno-political, is instrumental in creating this policy problem. Information technology has given businesses powerful tools. It is increasing an organisation's efficiency, it is facilitating new opportunities to explore and create markets, and it is creating a whole new electronic information industry. However, with these new powerful tools comes also a new social responsibility. In the final analysis, consumer studies have demonstrated that it is highly doubtful that this responsibility will supersede the corporate motivations - such as the profit and the logic of efficiency inherent in information technology - which seem to be in direct conflict with humanistic concerns such as privacy and individual dignity. Moreover, as economic indicators underscore, the widespread application of commercial practices using personal information has only just begun, and can be expected to grow in an exponential fashion.

4. The democratic and human rights dimension

This last aspect represents an opposing force to the economic imperatives. This dimension is illuminated within the work of political economists, sociologists, privacy advocates, and legal experts; and it is evinced in the growing public apprehension about the loss of information privacy. From this diverse body of literature, there are three "imbalances" that contribute to this problem.

The first is an economic imbalance. As people become aware of the commercial use of personal information, they are beginning to wonder why corporations should profit from their information. It is not inconceivable that individuals may demand to know what their information is worth to the tele-marketer or company. In the near future, individuals may demand some form of monetary compensation for "their" information.

The second is a political imbalance. As the private sector grows in size and influence, there appears to be a democratic deficit in terms of organisational accountability. For instance, while we have mechanisms that check the power of government and its bureaucracy, there is comparatively little redress when it comes to the private sector. Moreover, information technology has magnified these power differentials between the corporation and individual. This state of affairs has brought about the sensible conclusion from Colin Bennett that:

> "the processing of personal data by banks, credit card companies, insurance firms and others must be conducted under no lesser conditions of accountability than those which should pertain to tax offices, social security departments, health services and the police."[93]

The third is a social imbalance. This view-point sees the problem in more systemic terms; that is, a product of the wider forces of the capitalistic order, like the instrumental logic of efficiency, which in Charles Taylor's words seems to be one of the key "malaise's of modernity"[94] because it cloaks commercial practices that impinge upon human dignity through discrimination or manipulation.

The Stakeholders

The three discernible groups of people that would be affected by a policy - or lack thereof - on the commercial use of personal information are: industry, the general public, and privacy and consumer advocates.

Industry is naturally the most enthusiastic about the use of information technology and personal information for commercial purposes. It is constantly finding new ways to employ the invaluable techniques of database marketing in order to find new markets and increase efficiency. However, industry's attitudes towards the issues surrounding information privacy are far from homogenous. Whether industry views information privacy as a good business practice or as a nuisance, largely depends on education and knowledge about privacy issues. Generally speaking, industry analysts who know about the wider implications of the commercial use of personal information, and have the foresight to see the potential damage of a consumer backlash, generally pay a greater attention to information privacy.

The public is also quite heterogeneous in its opinions; some want the government to regulate, while others are either indifferent or pragmatic about the use of their information. These attitudes, however, may shift through education and increased politicisation of this issue. A

central part of this problem is a general ignorance concerning the commercial use of personal information. Studies indicate that if informed, people demand a bundle of rights implicit in information privacy: that is, the right to know what is known about you, and the right to information self-determination. This is perhaps where the third set of stakeholders - the privacy and consumer advocates - fit into the equation. These stakeholders definitely do know about the issues, and consequently spend their time trying to educate both the public and industry about the merits of information privacy. On the whole, privacy advocates tend to push for regulation in the private sector, and they tend to come from academic backgrounds.

The role of public policy

The challenge of public policy is to restore the necessary political, economic and technological balance so that these conflicting elements can coexist without any extreme social consequences. One strategy that is frequently employed for complex societal problems is the idea of **"balancing"** competing claims and values.[95] This strategy owes its theoretical roots to the liberal and pluralistic view of governance, especially the Madisonian notion of checking one powerful contingent against another.[96]

This "balancing approach," however, has its critics and rightly so. David Lyon, in *The Electronic Eye*, writes that this approach is "chronically limited, not only in the sense that such measures may be 'too little, too late' but also in the sense that law itself is inadequate to the task of regulating electronic surveillance."[97] Clearly, it still remains an empirical question whether governments can, in fact, balance the heady imperatives that underlie many of the problems within our changing techno-political environment. Even so, it is important to distinguish

"actual" responses and "sociological" responses. Critical theory may have a role in the latter category whereas public policy must nevertheless act positively and often pragmatically with limited resources and knowledge.[98] As we shall see in the next chapter, the field of data protection is possibly such a response.

Chapter Two - Responding to the policy problem

Chapter One canvassed the multifaceted dimensions of the policy problem from a wide theoretical and empirical angle, and then defined its parameters in terms of its four dimensions and three stakeholder groups. The present task is to see how public policy can respond to the problem, and the place we look to is the field of data protection.

2.1 The field of data protection

The issue of information privacy has been with us since the early 1970's when the use of information technology (especially databases) became institutionalised within public sector bureaucracies. The debates of the day argued that governments were incrementally creating a surveillance infrastructure akin to an Orwellian, "Big Brother" state.

The field of data protection evolved as a policy innovation designed to curb the realisation of these fears by balancing the conflicting imperatives of administrative efficiency with the privacy rights of individuals through the enactment of data protection statutes.

In retrospect, the Orwellian prognosis was a bit off: although governments show no signs of curtailing the desire to engage in surveillance activities,[99] commercial enterprises are in an equally strong position to conduct "consumer surveillance."[100] This does not mean that corporations have intentionally developed this situation. More probably this is something that has just evolved over time. Nor does the existence of consumer surveillance mean that

businesses malfeasantly monitor and manipulate consumers; it just means that they have the potential to do so with uncertain consequences.

A turn to data protection statutes, however, may be the key to resolving the germinating tensions between information privacy, and the efficiency and demands of the marketplace. By definition, data protection is quite similar to information privacy: it is "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[101] According to Colin Bennett, there are three interrelated goals of data protection: "to protect a sense of privacy, dignity, and anonymity from the increasingly intrusive organisation; to enhance [organisational] accountability; and to improve the integrity and efficiency of administrative decision making."[102]

Another thing to note for clarity is that the term "data protection" is a bit of a misnomer, partially because of its European derivation.[103] The laws do not protect data, as the name implies, but the right to information privacy. As a result, North American policy-makers elected to choose the title of "privacy protection" which commanded more popular appeal than the technocratic term of "data protection."[104] This analysis sticks with the policy title of "data protection" because as Colin Bennett argues: "it distinguishes the policy problem better than the broadly elusive and culturally relative term of 'privacy'."[105]

Aside from national differences in its appellation, data protection statutes have become an indispensable tool for governance in post-industrial democratic states as **Table 2.1** illustrates.

Table 2.1 Data protection statutes in the postindustrial states		
Country	Legislation	Data of passage
OECD Countries		
Sweden	Data Act	1973/82
United States	Privacy Act	1974
West Germany	Data Protection Act	1977
Canada	Privacy Act	1977/82
France	Law on Informatics&Liberties	1978
Norway	Personal Data Registrars Act	1978
Denmark	Private Registrars Act	1978
Austria	Data Protection Act	1978
Luxembourg	Data Protection Act	1979
Iceland	Act on the Systematic Recording of Personal Data	1981
New Zealand	Official Information Act	1982
United Kingdom	Data Protection Act	1984
Finland	Personal Data File Act	1987
Ireland	Data Protection Act	1988
Australia	Privacy Act	1988
Japan	Personal Data Protection Act	1988
The Netherlands	Data Protection Act	1988
Source: Colin Bennett, *Regulating Privacy* (1992): 57		

At present, over twenty OECD countries have data protection laws on the books. There are also signs that even non-OECD, and not necessarily democratic, states like Hong Kong are seeing the need to have data protection.

The comparative history of data protection is fascinating because it is an excellent test case of contemporary nation-states responding to a complex, technological problem. In particular, data protection is an interesting exemplar for the policy theory of convergence: the hypothesis that "technological and economical development has a levelling impact on diverse social structures, cultural traditions, and public policies."[106] This thesis posits that with similar technological circumstances the imprint left by divergent institutional and cultural configurations will diminish in significance as countries respond with similar policy solutions.

With the case of data protection, two important comparative policy studies, David Flaherty's *Protecting Privacy in a Surveillance Society* (1989) and Colin Bennett's *Regulating Privacy* (1992), find a remarkable convergence around a set of fair information principles in Table 2.2.

Table 2.2 "The Core Fair Information Principles"

(1) The Principle of Openness

The collection of information should not be concealed from the individual; an organisation's information handling practices should be transparent.

(2) The Principle of Individual Access and Correction

Individuals should be able to access, verify and change incorrect data about themselves.

(3) The Principle of Collection Limitation

Organisations should only collect the necessary data required to perform its task, and not collect information that may have an unanticipated value at a later date.

(4) The Principle of Use Limitation

Organisations should only use the data for the purpose in which it was collected, and not for another purpose.

(5) The Principle of Disclosure Limitation

Information should not be transmitted to a third party without the consent of the individual.

(6) The Security Principle

Data should be protected with adequate security measures in the processing of personal data

Source: Colin Bennett, *Regulating Privacy* (1992): 101-110

These principles are significant, not only because they help establish an important "balance" between the claims of efficiency and information privacy, but also because they represent an international consensus on the proper use of personal data in both public and private sectors.[107] In Colin Bennett's words, fair information principles "...reflect the insurmountable

problem of regulating a diversity of institutions in order to protect an elusive resource that individuals may value in widely different ways."[108]

One of the most influential marks of this consensus is embodied in a document produced by the Organisation for Economic Co-operation and Development (OECD) titled the *Guidelines on the Protection of Privacy and the Transborder Flow of Personal Data* (the Guidelines).[109]

These *Guidelines* codified the fair information principles, and applied them to both public and private sectors with the expectation that countries would:

> "establish legal, administration or other procedures or institutions including appropriate domestic legislation, measures for self-regulation, reasonable means for individuals to exercise their rights, adequate sanctions and remedies for failure to comply."[110]

The motivations behind the OECD efforts for a concerted, transnational action flowed from a concern that there was evolving an "unnecessarily complex and disparate framework of procedures and compliance requirements for transborder flows of personal data."[111] Thus, the *Guidelines* were designed to promote the dual goals of an international harmonisation in information handling practices, as well as tempering fears that sensitive personal data was making its way across borders without an individual's control or consent.[112] In essence, the *Guidelines* try to balance the two.

Although twenty-four countries, including Canada, signed the document, the *Guidelines* had the drawback of being a non-binding, transnational document that left "appropriate measure to individual countries" for the implementation of these principles.[113] Therefore, it is hardly

surprising that with a convergence there also came a noticeable divergence with the way these principles were implemented within individual countries. These divergences have been comprehensively documented in the work of David Flaherty and Colin Bennett, and are crudely summarised for the sake of illustration in **Table 2.3**.

Table 2.3 Comparative Data Protection in Six OECD Countries

Country	System of Government	Policy Model	Scope	Enforcement
Canada	Federal	Data Commissioner/ Voluntary for private sector	Public sector only with similar statutes in most provinces.	Advisory with auditing powers in public sector. No authority in private sector.
West Germany	Federal	Data Commissioner	Both sectors, automatic records only	Centralised regulation/ advisory with constitutional protection of privacy
Sweden	Unitary	Licensing/ Registration	Both sectors	Regulatory powers through a "mini-Parliament" Data Protection Board
France	Unitary	Registration	Both sectors	Regulatory powers through a Data Protection Board
United Kingdom	Unitary	Registration	Both sectors, automatic records only	Regulatory / advisory powers through Data Registrar
United States	Federal	Subject control/ Voluntary for private sector	Pubic sector only, variation among states	Advisory in theory through OMB (but not in practice) with reliance on court system

Sources: David Flaherty (1989) and Colin Bennett (1992)

From **Table 2.3** we can see the various policy models, with different scopes and styles of enforcement, that countries have employed to protect information privacy. They all have manifested, in some form, the spirit of the fair information principles.

West Germany's system of data protection is based on the *data commissioner model.* This model centralises decision-making in a Data Commissioner who acts like an ombudsman on behalf of individuals, performing the role of watch-dog for new, potentially invasive, technologies as well as monitoring the information handling practices of both public and private sectors. In Germany, data protection is considered by Flaherty as comprehensive, although implementation is decentralised through the eleven German states which regulate the private sector.[114]

Sweden chose the more bureaucratic system of *licensing* all data users to make sure they comply with proper information handling practices. In practice this proved to be too cumbersome so the *Data Act* was amended to a registration model that now acts like a "supervising system" for organisations.[115] Sweden also has a decentralised decision-making process through a board made of a "mini-Parliament" of elected and non-elected officials.[116]

Like Sweden, France also went the *registration* route in order to enforce compliance, and like Sweden, makes decisions through a decentralised and rather politicised board.[117]

The United Kingdom followed in the foot-steps of both France and Sweden through the adoption of a registration model, however it adopted a more centralised Data Registrar to monitor the activities of industry and government.[118]

The United States chose a combination of two approaches. The first is what Bennett calls the "*subject control model*" and is embodied in the federal *Privacy Act,* 1974. This act grants

information privacy within the public sector through the codification of the fair information principles; however, "enforcement is *post facto*, and individuals must initiate any action."[119] The second approach is the "voluntary" or "self-regulatory" model which applies to the private sector.

Canada's *Privacy Act (1982)* is also a mixture of models. It adopted an approach similar to the West German data commissioner model; however, it is considered a "second generation" data protection statute because it was the first to combine both "freedom of information" and "privacy" into one law. Also, when it came to regulating the private sector, policy-makers chose the American route and adopted a self-regulatory policy.

Thus, the most notable contrast in comparative polices is rooted in whether the private sector is regulated or not.[120] With this comparative perspective, it must be stressed that the Canadian and American choice of the self-regulatory model for the private sector is the exception and not the rule.[121] This is an important distinction because in Flaherty's estimation, self-regulation is only a "partial policy solution"[122] given the blurring between the public and private sectors and the use of information technology.

Bennett's work is largely devoted to explaining why we see a wider convergence around these fair information principles and a divergence when it comes to implementation. As we shall see in **Table 4.1** in Chapter 4, he provides an explanatory framework to help understand this within the field of data protection. However, recent developments in data protection within

the European Community may indicate that these divergences may not last for too much longer.

In July of 1990 the European Community introduced a *Draft Direction on the Protection of Individuals in Relation to the Processing of Personal Data.* After intense lobbying by industry representatives (especially the direct mail firms), a revised Draft emerged in 1992, making some concessions because, as industry argued, the first version was not "balanced," favouring information privacy over commercial interests.[123] The statute, however, even in its present, diluted form is a strong data protection statute in comparison to North American standards because it applies to both private and public sectors.[124] Another key component of the *Directive* is that all data users are required to notify or resister "their processing operations to their national data protection authority" and ensure that "judicial remedies are available to individuals."

Although an examination of the politics of the *Directive* escapes the scope of this paper, it suffices to mention that industry opposition was naturally - and still is - strong. The Direct Marketing sector objected to the provisions that require all individuals to be informed of third-party disclosures of data. The Financial Credit industry was also particularly displeased about an article that gives individuals redress for the adverse effects of "automated individual decisions."[125]

However, in terms of trade issues, the most crucial provision is Article 24. This article prohibits the transmission of personal information to non-member countries without

"equivalent" or "adequate" data protection. Therefore, to countries like the United States and Canada this poses a serious threat to potential trade relationships - relationships that increasingly rely on the free and unencumbered flow of information. Flaherty also contends that the European "litmus test" for adequate data protection is an "independent administrative authority" over both the public and private sectors.[126] However, Canada and the United States do not even have in place formal rules for the private sector, apart from their own efforts to self-regulate. It is thus highly questionable whether North America will meet the EC requirements.

Industry resistance and rhetoric aside, the *EC Directive* is good news for both information privacy and industry. Clearly, a thrust towards the harmonisation of information handling practices would unquestionably improve the efficiency of commercial activities by leaps and bounds. Raab and Bennett are nevertheless sceptical in their recent article, "Protecting Privacy Across Borders: European Policies and Prospects," about the realisation of this harmonisation and they document several "significant obstacles to convergence in practice."[127] As we will see later in Chapter 4, this scepticism is hardly surprising given the intricate interplay of the politics within data protection.

2.2 The Canadian data protection responses

With the comparative background of data protection in view, what is the precise nature of the Canadian responses? To date, the Canadian responses have been characterised as a "patchwork" of legislation, initiatives and developments.[128]

The first model is derived from Canada's most recent development in data protection - Québec's Bill 68 - which became the first statute within North American to develop enforceable rules for the private sector's use of personal information. Furthermore, this statute reflects more closely the model embodied within the *EC Directive 1992*. It is thus paradoxically an exemplar within North America of a new direction for data protection as well as a product of a wider, transnational convergence with European standards.

The second model is based more on the *status quo* in terms of data protection legislation, as well as recent concerted efforts to develop a national self-regulatory regime through a process headed by the Canadian Standards Association (herein, the CSA process). This direction is also being followed within the United States, and will represent a divergence in data protection in lieu of the adoption of the *EC Directive 1992* scheduled at the end of 1994.

Bill 68: Québec's Regulatory Model

The Québec regulatory model is compromised of three, interrelated, components: the changes within the Québec legal environment, the written letter of the law embodied in Bill 68, and the quasi-judicial functions of the data commission, the Commission d'accèss à l'information.

1. *The legal environment*

Bill 68 is largely a product of two changes made within the Québec legal environment. The first pertains to the adoption of the Québec *Charter of Human Rights and Freedoms* which, in Article 5, guarantees every person a "right to private life."[129] The second change was the revision of Québec's *Civil Code* which included a chapter entitled "the Rights of Persons." This

Chapter, strongly influenced by the OECD *Guidelines*, encoded in Québec law a set of fair information principles that gave all Québecers information rights.

2. *Bill 68: The letter of the law*

Bill 68's full title is *An act respecting the protection of personal information in the private sector*. It became law on January 1, 1994 and resembles the data protection act for the public sector, the *Act respecting access to documents held by a public bodies and the protection of personal information* which came into effect in 1982, about the same time as the federal *Privacy Act.*

Bill 68 specifies several standards for information handling practices that are now familiar to us, given Bennett's condensed list of the fair information practices in Table 2.2 that have formed the corpus, over time, of data protection statutes.

This piece of legislation mandates all "data users," that is, both commercial enterprise and government, to do the following:

- obtain an individual's consent to the communication or use of his/her personal data that is "manifest, free and enlightened" (Article 14);
- limit the collection of personal information to specific and stated purposes;
- inform the "data subjects" of the object of the file, the uses and disclosures that are permissible, as well as the place where the file is being kept (Article 8);
- ensure that all data files are kept confidentially and accurately, with appropriate safety measures, and retained only for the prescribed time by law (Article 10-12);
- ensure that all citizens have a right to access and correct any information being held on them.

In addition, the Bill establishes special rules for "personal Information agents" which include all members of the electronic information industry, i.e., the credit, financial reporting, direct marketing sectors. These rules require personal information agents to register with the Commission and submit for review the operational methods for the processing of personal information. In return, personal information agents can use special "nominative lists" for marketing purposes, that is, lists containing personal data that has met the standards of the Commission.

3. *Commission d'accèss à l'information*

Another essential part of Bill 68 also was the implementation of these principles through the independent oversight and expertise of the Commission d'accèss à l'information. The Commission's role is both regulatory and advisory in that it must ensure that both public and private business meet the requirements of the law, as well as facilitate practical measures on how to interpret and respect the spirit and letter of the law.[130]

The CSA Process: The National Self-Regulatory Model

The national self-regulatory model presented here is also a combination of three things: the recent process towards self-regulation headed by the Canadian Standards Association; the existing legislation that governs consumer law; and the foundation of common law principles.

1. *Voluntary Sectoral Codes*

Self-regulation is a policy model depicting the voluntary adoption of sectoral codes by industry. The first step towards a conscious move to self-regulate occurred when Canada formally signed

the OECD *Guidelines* in 1984. Since then, although not until most recently, there have been several "Privacy Codes" that emulate these *Guidelines* and thus the internationally agreed upon fair information principles.

An important sectoral code, and one of the first developed, started with the Canadian Direct Marketing Association (CDMA) *Privacy Code* which was strengthened as recently as February 1993. This code gives consumers the right to have their names removed from marketing lists, in addition to other fair information practices like the right to access personal information. In addition, the CDMA has had since 1978 a complaint handling system called *Operation Integrity* that was devised in co-operation with the Department of Consumer and Corporate Affairs. Other noteworthy, industry-led codes include: the Canadian Bankers' Association *Model Privacy Code* which was released in May 1992; the *Code of Practice* in the Financial Sector; and the *Stentor Code on Privacy and Fair Information Practices.*[131]

However, amidst the backdrop of EC trade threats and the results from the two privacy surveys, the CSA Privacy Initiative was started to help improve and standardise information handling practices on a national scale. This initiative was designed to be a consensus facilitating process bringing together consumers, business, government, labour and industry representatives "to debate the issues around the protection of personal information, and arrive at acceptable solutions."[132]

The stated objective of the CSA Process is to "develop a simple model code on privacy protection which reflects the OECD Guidelines." The model code will set minimum national

standards for handling personal information, and it is hoped that it can implement nation-wide a standard logo - much like the environmental recycling designation - so that consumers can be made aware of enterprises that adopt the good business practice of information privacy. The model code is also designed to be supported by supplementary technical standards, as well as more detailed sectoral codes.

2. *Existing Legislation*

It is also a premise of this model that additional consumer legislation is not needed at the federal level because (a) consumer law is within the jurisdictional purview of the provinces and not the federal government; and (b) there is plenty of legislation already on the books protecting consumers. The *Credit Reporting Act* in British Columbia is such an example for the use of personal information in making credit-worthiness decisions.[133]

3. *Common Law Tradition*

The last premise within the Canadian self-regulatory model is that information privacy does not fall in a legal vacuum; it has the common law tradition that relies on notions of "tort", "property" and "contract" to fill any information privacy gaps that the codes and existing legislation may not cover. [134] Therefore, other than a sector's own redress mechanism (if it has one), the principle forum for enforcement of information privacy is within the Canadian court system.

2.3 Two models for data protection

The results of the dialectical "patchwork" of Canadian legislation, developments and initiatives has been the production of two dynamic models for data protection within the Canadian federation: one at a provincial level and the other at the national level. This patchwork has emanated, prism-like, from the channelling effect of larger conflicts surrounding the tension over personal information, the competing imperatives of technology and society, as well as the comparative policy patterns and pressures of convergence and divergence within data protection.

The next task at hand is to assess which model is the most effective in appeasing the problem over personal information within Canada.

Chapter Three:
Assessing the Canadian Data Protection Responses

3.1 The Criteria for Assessment

The endeavour of this chapter is to assess which approach - the Québec regulatory or the CSA self-regulatory model - is the best route for Canadian public policy. To assess the models, we must first have a set of criteria in which to measure their effectiveness in balancing the conflicting societal tensions over personal information.

Based on the analysis of the problem in Chapter 1, we can extrapolate three criteria for a policy that may meet the demands of this tension.

Table 3.1 Model criteria for assessment

(1) The model must respect the **human rights imperative** in that it must perform the dual goals of protecting *information privacy and* promoting *organisational accountability* within the private sector.

(2) The model must appeal to the **economic imperatives** of industry and the Canadian economy by *minimising bureaucratic policy solutions* and *onerous regulatory demands* on industry. The *free flow of information* should be a primary goal.

(3) The model must confront the reality of the **technological imperatives** that will escalate in the future as information technology increases in its pervasiveness and ubiquity within Canadian society. The model must thus be an *enduring, future-conscious* solution that has the capacity to adapt to new challenges and circumstances.

The Human Rights Imperative:

How do each of the models protect - or fulfil - the requirements of the human rights imperative? The answers are mixed.

With the Québec model, information privacy is protected by making legal in the Québec *Civil Code* a set of fair information principles. Also, article 65 of the Québec Charter of Rights guarantees all Québecer's "the right to private life". Bill 68, on top of that, establishes a form of redress through the Commission d'accèss à l'information if an individual feels that her information privacy has been violated. Moreover, this process of redress is efficient, speedy and user-friendly for the individual. To initiate a compliant, a person simply notifies the Commission and a decision must be handed down within thirty (30) days. It is also noteworthy that the onus is on the commercial enterprise to prove that it did not invade ones information privacy. This method of redress is important because, in the words of Marie Vallée, a Québec official who deals with a consumer aid service, "consumers do not have strong tools... they don't know the right person to talk to with complaints ... and they don't have the resources to pursue legal measures ... instead, they just let things go."[135]

In contrast to the Québec model, the national self-regulatory model has several problems in terms of delivering adequate information privacy. For starters, Canada does not have a clear constitutional right to privacy other than its implicit derivation from the Canadian *Charter of Rights* and the federal *Privacy Act* 1982. This has, in turn, created some interpretational discrepancies. The *Annual Report 1993-1994* of the Privacy Commissioner of Canada, for instance, documents two Federal Court decisions with differing interpretations of "personal

information and the relationship between the *Privacy Act* and the *Access to Information Act*."[136] It appears that one case, *Robert Sutherland and the Minister of Indian and Northern Affairs*, "recognises privacy as a fundamental human right worthy of and demanding government and court protection;" while the other, *The Minister of Finance and Michael A. Dagg*, "dilutes that right significantly."[137] Experiences within the United States also echo this problem with interpreting privacy.[138]

Clearly, there are drawbacks to relying on the courts. Not only do courts interpret concepts like "privacy" inconsistently, but they are also an inefficient and expensive form of redress for individuals. This is compounded when the issue is based on rapidly changing technological problems.

There are also significant problems within the *Privacy Act* itself, possibly because the Act is now ten years old and thus showing signs of age. Most notably, the statute falls short of its goal to protect information privacy because it does not extend to the private sector. As we saw in the previous chapter, in Europe data protection statutes are applied to both sectors because the distinctions are seen as meaningless.

Other major short-comings of the *Privacy Act* are that it does not cover institutions like Crown corporations, the courts and Parliament. Perhaps most significantly, however, is the fact that its principle of consent has been undermined with exceptions and loopholes created by ambiguous clauses like "consistent with that purpose".[139] This means that organisations covered

by the act can devise creative situations in which almost any use of personal information collected is "consistent with that purpose."

Outside of the *Privacy Act*, many proponents of self-regulation argue that there is ample protection through existing legislation and institutions. However from a legal perspective, Blackman demonstrates that this is a somewhat tenuous assertion.[140] He argues, like Marie Vallée, that it is an arduous task for the average individual to navigate the labyrinth of "niche" legislation surrounding consumer issues. Peter Dorsey from the B.C. Credit Reporting Branch makes similar claims based on his professional experience. He argues that "consumer rights" are difficult to define in many Canadian statutes, like the B.C. *Credit Reporting Act,* because they have numerous ambiguities and "grey areas" that leave too much room for interpretation.[141]

Organisational Accountability

Bill 68 also scores points in promoting a greater degree of organisational accountability, which is vital considering the technological and political dimensions of the problem. It does so by giving the Commission the power to advise, audit, and investigate information systems, as well as the power to fine commercial enterprises for flagrant abuses of information.

Again, by contrast, the self-regulatory model posited by the CSA process - although a definite improvement from before - still fails to enforce an adequate measure of organisational accountability. It fails to do this for one fundamental reason: the inherent conflict of interest between the interests of information privacy and the interests of business. At the most logical

level, it intuitively flows that organisations cannot be "both protector and collectors" of personal information.[142] Blackman argues that this would especially be the case in times of recession; that information handling practices would be "inevitably subject to vagaries." In short, self-regulation is an "insecure system for personal data."[143] With voluntary privacy codes, for instance, many companies could simply can opt out. Also, not all companies are members of the sector associations, like the CDMA, because of costly membership fees.

Industry analysts, in rebuttal, argue that competition is an effective motivating force to get industry to meet the needs of information privacy. Privacy would simply become a good business practice, and corporations who stray from it will be accordingly penalised by the market. Consumer studies nevertheless find evidence to the contrary. Mary Gardiner Jones from the U.S. Consumer Research Institute cites numerous examples where competition has failed to protect the public's interest: unit pricing, full warranties, clear and complete disclosures in product descriptions, ingredient listings, and care instructions.[144] In Canada, similar evidence abounds as well. For instance, a Report Submitted to the Department of Consumer and Corporate Affairs in 1990 titled "Pre-authorizes Debits: A Profile" found that many tellers knew very little about fair information practices like the right to correct inaccurate information.[145] Consumer demand is thus an imperfect mechanism for something as important as information privacy.

Thus with the CSA model the chief problem is enforcement. There is simply no bite with voluntary codes of compliance. Bob Crow from the Information Technology Association of Canada nevertheless argues that the CSA model would have "sanctions against scoundrels" who

violate the principles.[146] However, given what we already know about what motivates industry, such public castigation is probably unlikely.

Industry analysts naturally contest the validity of the studies on self-regulation. Instead of regulation, what they claim is needed is strong voluntary codes and public education.[147] And they are right: both conditions would be highly desirable. But again, what would be the most appropriate mechanism for consumer education: an independent expert like the federal or provincial Privacy Commissioner with a budget to devote specifically to privacy concerns, or relying on industry to deliver the material?

The immediate experience with the implementation of Bill 68 suggests that possibly both, when working together, perform the best job in different ways. On the one hand, the Privacy Commissioner is useful in publicising important issues within the media; while on the other hand, industry (when legislated to do so as in Québec) can communicate information about privacy and information rights to consumers in an innovative and cost-effective manner, perhaps better than the public sector.[148] The burden of promoting information privacy is thus shared. Individuals can then assume a measure of responsibility themselves if properly informed. Therefore, as Lola Fabowalé's study *Voluntary Codes: A Viable Alternative to Government Legislation*? demonstrates, government-led codes are usually the best way to ensure compliance.

On the more negative side, the Québec model does have its problems. According to an analysis done by Richard Maurel, there several drawbacks.[149] For instance:

- There is no requirement for the information to be "complete." Decisions on an individual can therefore be based on partial information.

- The act does not provide any guidelines for database matching.

- The act requires individuals to pay a fee for initiating a compliant at the Commission. This may defer some applicants.

- Security will still be a problem. The act grants legalised telephone access to personal information, but with no specific security provisions guarding this data.

Another problem with the enactment of statutes as a policy instrument is that they often have unintended consequences. For instance, Flaherty warns about two things: first, the complacency that can emerge with a data protection law on the books; and second, the institutional inertia of regulating agencies. On the first point Flaherty notes:

> It is naive to believe that surveillance societies will not flourish by reason of the existence of data protection; in fact, one unintended consequence of their presence is the prospering of surveillance societies, because the public has a false sense of security, and the data protectors themselves have, or have used, limited power.[150]

And on the second point he cautions that:

> Unless a deity is endowed data protectors with some form of special status to insulate them from historical forces, there is every expectation, based on comparable performances by other such specialised bureaucracies, that the quality and effectiveness of their performance will deteriorate and become debased over time. This phenomenon is not only the result of a lack of appropriate diligence, but a natural developmental process, a life cycle, that appears to be systemic to public administration.[151]

A regulatory model for data protection by no means is not guaranteed to meet its objectives. However an aware public and media can help to avoid these potential pitfalls.

<u>The Economic Imperatives:</u>

How do the two models compare in meeting the imperatives of economics? This is probably the most crucial and decisive question that needs to be addressed. The most common

argument lodged against a regulatory approach such as Québec's is that the cost of compliance and administration would far out-weigh its benefits, and that the demands imposed upon industry would be too onerous. In terms of public sentiment and an era of government fiscal restraint, the arguments against the creation of bureaucratic solutions are becoming very salient and should be taken seriously.

Does Québec's regulatory scheme therefore fail on these rationales - that it is too bureaucratic? In one respect it does: if implemented at a national level there will be, without question, the need to increase the staff and budget of the Privacy Commissioner's offices both federally and provincally. However, with the comparative experience of Europe in mind, the extension of jurisdiction may not prove to be too costly. Germany, for instance, regulates both sectors and has approximately the same number of staff as the federal Privacy Commissioner's office. Also, with the Commissioner's office having been in place for over ten years, the infrastructure is already in place for an oversight mechanism. And finally, the combined budget for the 1993-94 fiscal year for the federal Commissioner's office was $6,819,000 which is a fraction of the cost compared to many federal programs with half the scope and mandate. Thus, although it is perhaps too early to tell the impact of Bill 68 in terms of additional bureaucracy and work load, it will probably not be too taxing on the public purse, especially when weighed against the benefits that it creates.

The second argument, that a Québec-like regulatory scheme would be too onerous for businesses, can also be turned on its head: on the contrary, it may help the efficiency and profits within the private sector. How can this be?

Firstly, as Péladeau maintains, data protection in the private sector can be a good tool for **human resource management.** With a law to fall back on, it will be easier for Québec managers to do their jobs properly without any ethical dilemmas regarding the disclosure of personal information. For instance, what may happen is that a middle-manager may be pressured by her superiors to make inappropriate disclosures of personal information; or alternatively, this may happen anyway due to ignorance and "not knowing any better."[152]

Secondly, data protection can also be supported on the grounds of "**good housekeeping.**"[153] The most obvious example of this can be see from the experiences of the federal data protection statute. Brian Foran argues that data protection improved government record-keeping by making civil servants more accountable for what they do with personal data: "the policy did not [as the rhetoric of the day predicted] bring the government to its knees, but brought the bureaucracy towards a more democratic system that protects information privacy."[154] Similarly, there is every reason to believe that these instrumental benefits would occur in the private sector as well - perhaps to an ever greater degree, given the wide variation of information handling practices within industry.

Thirdly, a data protection statute like Bill 68 could help in defining liability issues. Already, as in the case with the woman in Montréal, companies are getting sued for misusing personal information. This is likely to increase in the coming years. Similarly, with a growing public disenchantment with the collection and dissemination of personal information, the support of a law could aid in legitimising their use of personal information.[155] One, now classic, example of this was a database produced by Lotus called "MarketPlace Households." This database, housed

on a laser disk, compiled tremendous amounts of lifestyle and demographic data of American households for marketing purposes. However, when consumer and privacy advocates got wind of this, they publicly criticised the company for violating thousands of Americans' information privacy. As a result, more than 30,000 people demanded to have their names removed from the disk. Within nine months, Marketplace was cancelled, and Lotus took a multi-million dollar loss.[156] In short, Mosco predicts that privacy is a "ticking time bomb" within the public consciousness.[157] The threat and damage of a consumer backlash upon the private sector cannot be underestimated.

Fourthly, according to one expert, the vague OECD *Guidelines* are not predictable enough for the private sector.[158] In this respect, the specificity and plain language of Bill 68 helps to minimise an uncertain investment climate, which is essential with information technology because of its capital-intensity.

Fifthly, the regulatory scheme in Québec does meet with the trade requirements of the EC *Directive.* This will, in turn, provide valuable economic opportunities for Québec companies within the EU. By contrast, it is highly doubtful whether the CSA model will comply to EC standards. As we mentioned earlier, the European "litmus test" for "adequate", "equivalent" data protection is an independent administrative authority over both the public and private sectors;[159] it is thus very doubtful whether the CSA process will be able to fulfil the EC's standards.

In economic terms, there are also some drawbacks. Quite probably there will be costs to industry if the model is implemented. The insurance industry, for instance, is at loggerheads with the Commission d'accèss à l'information over exactly this. However, it could be argued that perhaps the long-term, instrumental benefits from the regulatory model may outweigh the costs of compliance. Furthermore, not all sectors see the adoption of "fair information practices" as additional costs but as a necessary cost of doing business. Consequently, according to one industry observer, Bill 68 does not seem to be causing havoc within the Québec private sector. There have been no "horror stories" about the costs of compliance with the Québec regulations; and "corporations just don't seem to be too upset."[160] This is perhaps the biggest sign of all that data protection is not as onerous as industry analysts would like everyone to believe.

The Technological Imperatives

How do the two models meet the technological imperatives of the present and the future? It is here that both models fall by the wayside.

The Québec regulatory model *in theory* helps to abate the inherent intrusiveness of information technology. It places a primacy on information privacy and a watch-dog mandate for the Commission to monitor potentially invasive practices or technologies.

There is, however, some uncertainty about the effectiveness of data protection *in practice*. As Bennett notes,

> "... it is arguable that efficacious data protection has been in practice, and how robust it might in the context of further deployment of the new [information technology] and the internationalisation of information processes."[161]

This is where the self-regulatory model has its advantages: it can remain a relatively flexible response to an ever-evolving technological environment.[162] The development and enactment of legislation is a lengthy and involved process. Amendments are difficult to make compared to making changes within a national Privacy Code. However, it is highly doubtful - again for reasons of self-interest - that industry will be able to police the negative implications of technology. As the world economy becomes global, and competition increases, information technology may be industry's closest ally, and it will not be in their interest to look at its darker side.

3.2 A model for national data protection

Clearly, the two models have both positive and negative aspects. The self-regulatory model is more flexible and less bureaucratic. It imposes smaller costs of compliance on industry, and it may adapt faster to new technological environments. And lastly, the CSA process is a valuable arena for gaining a necessary consensus between all stakeholders in terms of information privacy.

It is in these respects that a national model for data protection should emulate. However, overall the Québec regulatory model seems to outweigh the merits of self-regulation on several grounds: in terms of enforcement, international trade, instrumental benefits, and public education. The key features of the Québec model include:

- An independent Privacy Commissioner that acts like a watch-dog for invasive and potentially harmful practices using information technology in both private and public sectors.

- A plain language law that legislates fair information principles, such as
  - the right for individuals to have informed consent with the third-party disclosure their information;
  - the right for individuals to access and correct inaccurate data about them;
  - the right for individuals to have their data secure;
  - the right for individuals to know what is known about them;
  - the right for individuals to limit the collection of their data to only the purpose in which it was gathered

- A clear, constitutional right to information privacy.

- An efficient and accessible means of redress in case of information abuse that avoids the court system;

- Sensible provisions to balance the claims of industry like "nominative lists" which facilitate the free flow of information.

The explication of a policy's rationales are nevertheless only half of a policy-makers task. The other half is understanding the political climate so that the constraints and opportunities for the proposed policy can be similarly weighed and assessed. As we shall see in Chapter 4, with the mediation of politics there is no inevitability about the push towards convergence based purely on the rationality - that is, the merits and sound logic - of any given policy.[163]

Chapter Four: The politics of Canadian data protection

After surveying the societal tension over personal information, and placing it within a comparative and domestic context, the first conclusion of this thesis has underscored the desirability of a legislative response similar to Bill 68 in contrast to the *status quo* situation at the federal and provincial levels.

The project of this Chapter is to unearth the salient variables that drove the Québec outcome so that we can see the opportunities and constraints towards an analogous outcome at the federal stage. In order to do so, we must first understand the vector of social forces, influential events and developments within each policy climate.

4.1 The Story behind Québec's Bill 68[164]

The antecedents of Bill 68 can be traced to a variety of legal, socio-political and institutional changes that formed an interesting and dynamic policy climate within Québec.

As we mentioned earlier, the first noteworthy development began in the legal realm with the introduction of Québec's *Charter of Human Rights and Freedoms.* The new Charter had an important clause, Article 5, which guaranteed every person a "right to private life."[165] This addition set in motion the second major development in 1987: the completion of Québec's revised *Civil Code* - a monumental process tantamount to re-writing English common law.[166] The *Civil Code* was originally adopted in 1866 and structured according to the Napoleonic code of 1804. It took nearly thirty-years before the new *Code* was finally enacted in December 1991.[167] An important chapter in the new Code is titled the "Rights of Persons"

which expands an individuals' repertoire of rights to information privacy. The influence and language of this chapter can be traced to "fair information principles" found in the OECD guidelines.

Following and concomitant to these legal changes, a number of important reports were produced that began to influence public policy debate. One document from the academic community in particular, *L'identité piratée,* issued by the *Groupe de researche informatique et droit* of the Université du Québec à Montréal, made its way to an inter-ministerial committee where it was studied for two years.[168] The work of this committee produced another report in 1988 called *Vie privée: zone à accès restreint.*

In 1989, the public sector act (*Act respecting access to documents held by public bodies and the protection of personal information*) required its five-year implementation review by the National Assembly's Commission on Culture. After reviewing the work of the public sector statute, the Commission presented a report, *La vie privée un droit sacré,* which made the recommendation to improve Québec's data protection regime by expanding regulation to the private sector.

After deliberating on the Commission's recommendations, the Minister of Communication, Lawrence Cannon, then asked the same commission to examine, more specifically, the implications of regulating the private sector with the 1989 report as a reference paper. This consultation convinced the Minister to go ahead with the Commission's recommendations.

Interestingly, the Bill went through two drafts each quite different from one other. The first draft embodied the principle of self-regulation. The second draft, the version that passed, went the regulatory route. Why this happened, however, is very much an "inside story."[169] The insights of this story were gleaned from several interviews with Pierrot Péladeau who was an instrumental player in bringing about the adoption of Bill 68. Much of the following material is therefore secondary impressions of a privacy advocate.[170] Even so, it is valuable contextual evidence, and as we shall see, essential to understanding the politics behind Québec data protection.

The first clue lies in the fact that, since the 1970's, there has been a growing and knowledgeable contingent of privacy and consumer experts within Québec, working hard towards the goal of better privacy protection for individuals. Péladeau sees this as the "rise of a social movement based on consumer and privacy issues."[171] This movement is composed of a coalition of advocacy groups, consumer unions and associations linked to an international groups of experts. This epistemic community has become institutionalised over the years with regular international conferences.[172] Thus, with this body of expertise to draw from, the privacy advocates were in a good position to lobby for increased information privacy through a data protection statute for the private sector.

Certain members were also well connected with Québec policy-makers. In June 1989, they were able to disclose at a data protection conference in Cambridge, England the fact that the first draft of Bill 68 was based on self-regulation for the private sector. After that, a privacy and consumer rights coalition in Québec began a campaign to oppose the bill and send a clear

message to the government. Pierrot Péladeau (then a volunteer for the advocacy group *Ligue des droits et libertés)* informed Robert Parent, the senior civil servant responsible for the Act, that if the Act was based upon self-regulation the Minister would find no support from the Québec consumer movement. In effect, the Minister would be alone in defending his Bill.

In the meantime, the movement coalesced under the leadership of *La Table de concertation informatiique et libertés*, an informal network of non-governmental organisations, and the *Ligue des droits et libertés.* The chief co-ordinator was Pierrôt Péladeau.

Other members of *La Table* were as follows:[173]

- the tenants' associations which in 1982 grouped under the *Regroupement des comités logements et associations de locataires du Québec*;
- the *Confederation of National Trade Unions* and the *Centrale de l'enseignement du Québec*;
- the *ACEF Centre de Montréal,* a family cooperative association and *FACEF* which is a federation of ACEF;
- the *Service d'aide au consommateur* in Shawinigan, Québec;
- the *Fédération nationale des associations de consommateurs du Québec (FNACQ)*;
- and lastly, the Québec Human Rights Commission.

Apart from this group of experts, a second instrumental element to the policy environment within Québec was the presence of an activist media. The term "activist" is used because certain members of the Québec media became, in effect, active voices for consumer and privacy issues. Throughout the debates surrounding Bill 68, there were several very well-informed "specialists" within the media who became devoted to the privacy cause. The

star expert for *Le Devoir*, for example, is Michel Venne, who has also has written a book on these issues called *Vie privée & démocratie à l' ère de l'informatique.*[174]

Other key players within the media during Bill 68's arrival were also André Bélanger, former editor of *Consommation* and now freelance journalist with *Protégez-Vous,* who wrote two crucial stories on the consumer movement; and Gaetan Nadeau who was freelance journalist connected to the *Ligues des droits et libertés.* In addition, many journalists on the *Tout compte fait*, a daily consumer show on Radio Canada, spent a great deal of time on privacy issues.

Péladeau posits that there are good reasons, rather unique to Québec, for the rise of this specialised core within the media. He puts out the idea that within the early 1970s Québec experienced a proliferation of news media, television networks, print media and journals. Young journalists needed new subject-areas to attract audiences. The issues surrounding privacy and the expansion of computer power into human affairs seemed to be a drawing card for many.

Privacy advocates also take credit for this development within the media. It has been their strategy to interact with the media, encouraging them to publicise this issue through the provision of information such as reports, statistics and studies, and analyses on comparative developments. Seen in this way, it was perhaps easier in these special circumstances to get the media on the privacy band-wagon, and create a lasting synergy between privacy experts and journalists - a connection that persists today.[175]

Therefore in short, the press was, and still is, on the side of privacy. During the debates of Bill 68, it launched many headlines lambasting the abuse of personal data by the private sector, and publicising "horror stories" like the one about "the woman in Montéal." *Le Devoir*, for example, was able to send tremors through the insurance industry by getting hold of a life insurance file that was left by accident in a corridor of a different building. In repeated fashion, the media was there to discover and document industry negligence in the improper handling of personal information.

To the network of experts, the activist media, add another important ingredient: the Ekos and Equifax privacy surveys. Interestingly enough, the Ekos survey found that Québéckers were more concerned about privacy related issues than the rest of Canadians. Thus, the results from these surveys only seemed to solidify support for a strengthened bill.

With this socio-political backdrop it is now perhaps easier to understand why the Minister decided to change the first draft of the Bill, and hold further private consultations with all the stakeholders. These consultations culminated in December 1992 when the second draft was presented in front of the National Assembly substantially revised. It practically mirrored the language and logic of public sector act. This was seen as a "victory" for the consumer movement.

According to Péladeau, industry was not ready for this shift in policy. All along, the mentality within industry was that Bill 68 would never become a reality because the new Liberal government under Daniel Johnson was more conservative, and thus more sympathetic to

business interests compared to the social democrat leanings of Bourassa.[176] Therefore when it was rumoured that Bill 68 was being tabled in the National Assembly, industry was caught by surprise. At first, there was a loud denouncement by industry. The *Conseil du Patronat*, a powerful lobby for the business community in Québec, immediately hired a lawyer from Equifax and began an anti-Bill 68 campaign. However, opposition was short-lived as the credibility of industry started to fall apart with bad media coverage and insufficient expertise in comparison to the privacy advocate community.[177]

3.2 The national path to self-regulation

The politics behind the national path to self-regulation is even less straightforward for several reasons. First and foremost, this is because it is an on-going process. In contrast to the Québec model, it is not complete nor will it get "passed" like a piece of legislation. Consequently, the politics is harder to uncover and discern because the events do not have the allowances of retrospection. And secondly, there is the problem of interconnectedness: clearly, by virtue of the Canadian federation, the politics of both models effect each other in a bi-directional and important manner.

The first phase of the steps towards self-regulation started in 1985 when Canada formally signed the OECD *Guidelines.* This signified a commitment by Canada to harmonise information handling practices through the implementation of the stated fair information principles.[178] It was suggested that because Canada was a common law country the best way the federal government could promote fair information principles was through voluntary codes for the private sector. However, the *Guidelines* also stipulated that industry would need to

demonstrate with "substantial evidence" that it was effectively complying with the principles in practice.[179]

The codes from industry trickled in, most of them coming well after the *Guidelines* were signed, with the exception of the Canadian Direct Marketing Association (CDMA)'s "Operation Integrity" which was in place by 1978. The CDMA nevertheless strengthened its Privacy Code in February 1994 and the Canadian Bankers' Association developed its Model Privacy Code in 1993 after the Ekos survey released its findings, as did the code of practice for the Financial sector and the STENTOR Fair Information Principles.[180]

In the meantime, the public sector become regulated in its use of personal data by the *Privacy Act* in 1982. The debates shifted towards the public sector and fears of "Big Brother." Even so, there was some controversial debate about regulating the private sector with a "uniform federal-provincial law."[181] As Bennett notes,

> the possibility of a uniform federal provincial law on the subject was raised by several provincial attorney generals [sic.] Many supporters of the law suspected that this was being used as an excuse for delay, and possible withdrawal.[182]

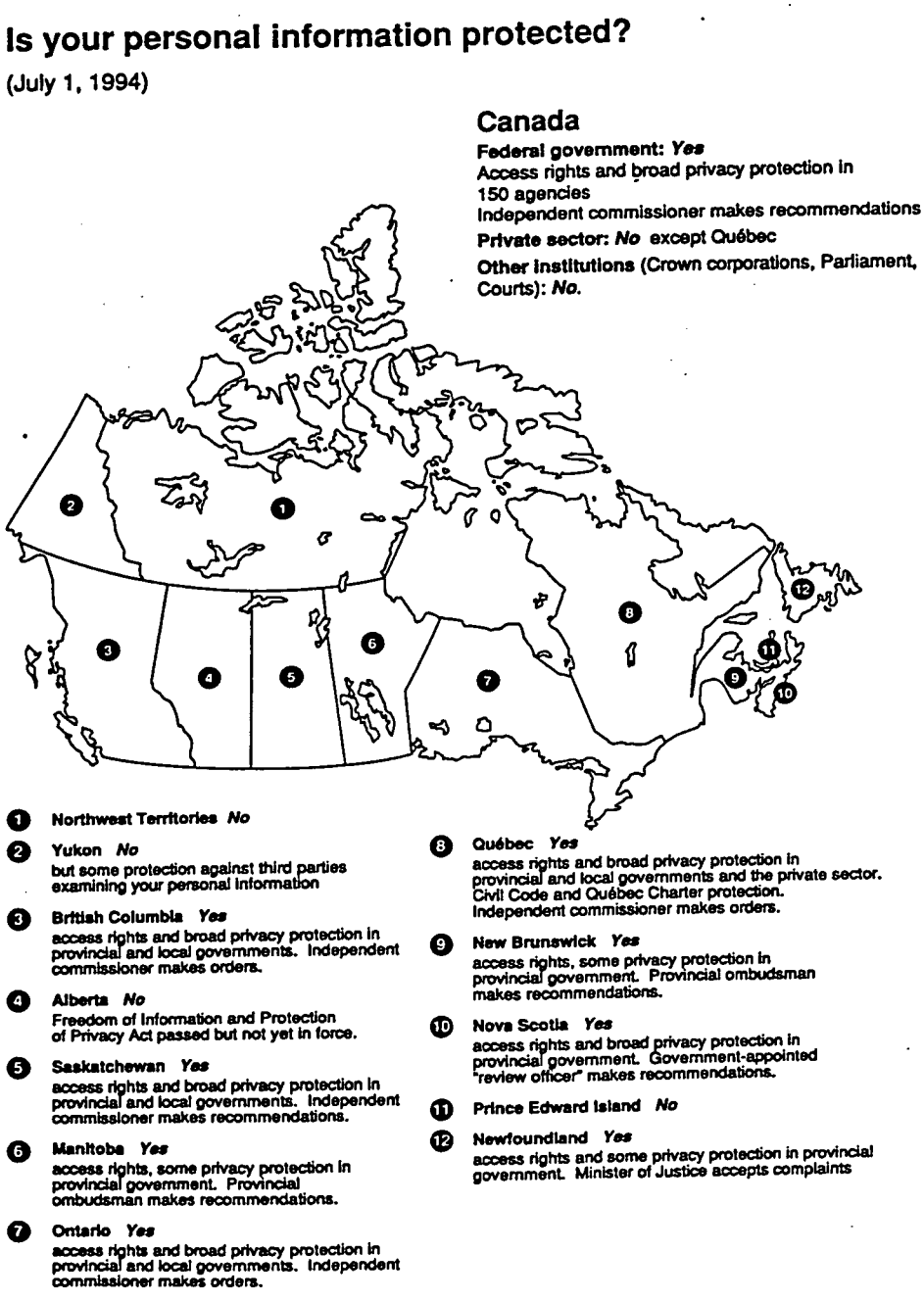
It should be also noted that while these legislative debates did penetrate the media's and thus the public's attention, they did not linger there for long.[183] The issue of "privacy" has traditionally been a "motherhood" issue, defying the ideological categories of left and right;[184] and data protection, just by virtue of its technocratic name, has never managed to command much emotional public appeal. As a consequence, this area of policy has been relatively un-politicised. This does have its advantages, as Colin Bennett has argued; however, when the

policy actors happen to be politicians, it often takes some political heat and public support to get an issue on the government agenda.

The issue about regulating the private sector thus petered out from debate until the *Privacy Act* had its mandatory five-year review in 1987. This review by the Standing Committee on Justice and Solicitor General produced an influential report titled *Open and Shut: Enhancing the Right to Know and the Right to Privacy.* It recommended that the Act be extended to crown corporations and all public institutions, and that Canadians should be given a constitutional right to privacy.[185] To date, the government has not been forthcoming in responding to these recommendations.

On the provincial level, there was also much activity towards developing data protection statutes as Figure 4.1 demonstrates.

Figure 4.1 Privacy Protection at a glance



Source: Office of the Privacy Commissioner of Canada, *Annual Report 1993-1994.*

These statutes are very similar to the federal *Privacy Act.* They function according to the data commissioner model and a set of fair information principles. In recent years, however, some provincial laws - British Columbia and Québec, for example - have surpassed the ten-year old act in terms of comprehensive protection. For instance, as mentioned in Chapter 3, one of the main deficiencies of the federal law is that its principle of consent has been undermined with exceptions and loopholes created by ambiguous clauses like "consistent with that purpose."[186] The upshot of the this, in the view of one Treasury Board official, is that the federal statute has been out-stripped with more progressive, provincial legislation.[187] The federal-provincial dynamic in data protection thus adds another, complicating element to the policy climate equation.

The next key development occurred when the Canadian Standards Association (CSA) received its mandate from Industry Canada to promote a harmonisation of information handling standards within the country. The chair of the CSA Privacy process is David McKendry who began to speak boldly about the dangers of present business practices on information privacy. In public addresses he described compliance with the OECD *Guidelines* as "not encouraging" and that business would have to do better within the CSA process.[188] This process also gained the approval of the Privacy Commissioner who called it "the most ambitious and earnest" of data protection initiatives within the private sector.[189]

The private sector, too, became keenly interested in this process for several reasons. First, and perhaps foremost, industry became interested because of the two privacy surveys released in 1992, *The Equifax Report on Consumers and Privacy in the Information Age* and the *Privacy*

Revealed: Public Perceptions of Privacy in Canada. Interestingly, the rhetoric of industry leaders began to shift. Instead of a stumbling block, privacy protection became a good business practice. "Invasions of privacy are in nobody's best interest," stated one industry analyst;[190] and in an address, Michael Globensky, Assistant Vice-President of Equifax Canada, maintains:

> As the leader in the Canadian information industry today, we are very much aware of our responsibility as regards the collection, safeguarding, and use of personal information for business decisions...[191]

In short, corporate leaders are starting to become aware of the detrimental impact of a consumer backlash, which could easily ensue if industry does not take a proactive stance.

Also, a second reason for industry's new interest in privacy and the CSA process stems from the possible trade barriers that the EC could impose with the "equivalent" protection clause in its new *Draft Directive.* As was mentioned previously, the EC represents a lucrative market for many industries that rely on the free flow of information.

Lastly, there is a fear which springs from the first two; it is industry's natural misgivings that if the private sector does not respond fast enough to public opinion and trade threats, governments will make sure that they do through regulation.

Another key actor within the national politics of data protection is the role of the Privacy Commissioner himself. Bruce Phillips sees himself as a "specialised ombudsman" and a watch-dog for privacy issues. Although his mandate extends only to the federal public sector, he has established an informal leadership role with the provincial data commissioners.

Phillips' style as a Commissioner is also of consequence.[192] He is pro-active and public, making statements about potential areas of concern whenever and wherever possible: within the media - at public addresses, or on radio talk-shows - and within publications like the Commissioner's *Annual Report.* In his latest report, for instance, he sees two "projects that have crystallised the tensions which can arise between efficiency and privacy."[193]

The first is the development of the National Advisory Council on the Information Highway. Phillips claims that there is not adequate representation from the privacy advocate community. This is a problem because, according to the recent Anderson Survey by Gallup, 84% of Canadians are worried about their privacy on the information highway.[194]

The second item of concern is the use of information technology in the federal *Blueprint.* Phillips maintains that its core principles - the standardisation and centralisation of information - undermine the protections set out in the *Privacy Act.* He argues that these plans may be more efficient but "the very reason for segregating personal information is to prevent governments from amassing detailed dossiers about individuals."[195] Furthermore, Philips raises an important question about the down-loading of government information into private databases. In this case, "what recourse will the individuals have against the misuse or wrongful disclosures of their information?"[196]

Phillips also goes on to attack industry's move towards self-regulation. Instead, he sees the solution much in the same way as this analysis: he is an emphatic advocate for a comprehensive, national statute for personal information. Thus, in a sense, the Office of the Privacy

Commissioner and its provincial counterparts can be viewed as a group of independent state actors that are, in effect, institutionalised privacy advocates. They can also be seen as having a vested interest in promoting the regulation of the private sector. While it could be argued that an expansion of jurisdiction would cause numerous head-aches in terms of extra work-load, the Office would surely benefit in other ways like an increased budget and mandate. The Privacy Commissioner is thus an important player in understanding the politics of Canadian data protection.

Amidst the advocacy of the Privacy Commissioner, the more concerted effort by industry to self-regulation, the sporadic shift in public mood towards privacy-related issues, and the trade threat from the EC - came Québec's Bill 68. In the words of the Paul André Comeau, the president of the Québec commission:

> "Some observers were stunned when they heard, last December, that Bill 68 had been tabled in Québec's National Assembly. Another strange move by la Belle Province, some dared to say. Others, more deferential, simply asked why the Québec government had to tackle that question." [197]

Why Québec did "tackle that question" is a combination of what has already been inferred. It had to do with the very merits of the policy in rational terms; and it had to do with the vector of social groups present within the Québec policy environment. But to what extent did Bill 68 impact the rest of the Canadian policy climate? While hard to measure in precise terms, there is no question that it did add some fuel to the "regulation vs. self-regulation" debate within the stakeholder group. Not surprisingly, from industry's point of view, it received harsh criticism. One representative from the Information Technology Association of Canada (ITAC) commented that Bill 68 is "a peremptory strike into unknown territory. It is quick and risky

without assessment of the trade-offs between the costs of compliance and administration with effectiveness."[198]

Within the Canadian Direct Marketing Association, fears were also aroused by John Gustavason, President of the CDMA. He made it clear that business "just cannot live with further constraints on their industry ...The Privacy Code is as far as we can go." Moreover he also claims that the new Privacy code will meet "the needs for today and the foreseeable future."[199]

Similarly, in a public address, Globensky from Equifax paints a lugubrious picture of future regulation on the private sector, and does so by quoting Alvin Toffler in *Powershift*: "the more any government chokes off or chills this rich, free flow of data, information and knowledge ... the more it slows down the advance of the new economy."[200]

However, at this point, it would be a mistake to portray the politics as an "industry vs. privacy advocate" struggle. In reality things are not so black and white. For instance, there are several privacy advocates who act as consultants to industry. Colin Bennett and Pierrot Péladeau were consultants for the Ekos survey, as was Alan Westin for the Equifax survey. Bennett has also been hired as an expert for the CSA process. Meanwhile, Péladeau is working "inside" the Québec business community to help them improve their information handling practices and privacy standards. In effect, there is a considerable amount of cross-over between the camps of industry and advocacy. Nevertheless, at the national stage the influence of privacy advocates is inherently limited, despite the active stance of the Privacy Commissioner. The reason is simply

because there are not very many of them to go around in such a large country. Privacy advocates, in many respects, have no choice but to work with industry.

Meanwhile, the CSA process continues and is expected to be released sometime in 1995 for public review. It is uncertain how the public will react to it, that is, if it gets any attention at all. One thing that is clear is the configuration of interests that will surround it. First, there will be the small collection of privacy advocates and the Offices of the Privacy Commissioners (both provincal and federal) pushing for greater protection and, if at all possible, the regulatory route. Second, there will the ambiguous role of federal bureaucrats, mostly from Industry Canada and Treasury Board (although the Department of Justice may be involved as well.) Third, there will be the heterogeneous interests of the private sector, the majority of which want to minimise government interference and prevent any further regulation. Fourth, there will be public perception which will be divided as well, with some individuals being more cautious and others being more pragmatic or indifferent in their attitudes.

4.3 Explaining the divergence

Within the field of data protection, there is good cause to expect a convergence. First, there is the nature of the technological problem in an insecure policy-climate. Second, there are the incentives to harmonise information handling practices for trade and economic reasons. Third, there is an established epistemic network of privacy experts promoting data protection within the OECD countries.

There has nevertheless been a distinct divergence within the Canadian federation. To help understand why, **Table 4.1** summarises Bennett's explanatory framework for comparative public policy in data protection.

Table 4.1 Colin Bennett's Explanatory Framework	
Explanations for Convergence	Explanations for Divergence
1. Technology driving common policy solutions; 2. Pressures to emulate within an insecure policy climate; 3. The impact of transnational elite-networking; 4. Trade and economic pressures to harmonise; 5. Penetration of another state's preferences and forcing them to conform.	1. Formal structures of the state, i.e. constitution, system of governance; 2. Preference of dominant social groups; 3. The role of political parties; 4. The position and power of the bureaucracy; 5. Economic constraints in carrying out effective data protection implementation.
Source: *Regulating Privacy* (1992)	

This analysis similarly isolates five variables that help explain why Québec went the regulatory route, and the rest of Canada (for the moment) has chosen the self-regulatory model. They include: (1) the impact of the formal structures of state; (2) the role of the bureaucracy in terms of structure and policy preference of state officials; (3) the function of political culture in differentiating the outcome; (3) the interplay of social groups within the policy environment; (5) and the effect of economic constraints on the development of policy.

It must be stressed that these five factors are *in theory* independent variables. In practice, however, they are inter-related and overlap each other, often becoming dependent variables

which can, in turn, obfuscate, explaining the "cause" and the "effect" within the policy process. These five possible explanations can nevertheless clarify the forces that drove the divergent policy outcomes.

However, before we can employ this comparative framework, one question needs to be addressed: how can we compare and contrast one model that is provincially-based and another that is federal? Clearly, there are methodology problems with this "apples-to-oranges" comparison, not to mention complicated federal-provincial jurisdictional questions. There are nevertheless some good reasons to employ this comparative framework. Firstly, by virtue of the decentralised Canadian federation with divisive forces like regionalism, language, and increasing pluralism in ethnic and group diversity, it makes sense to treat provinces as "mini-states" which have different elements that may, in turn, drive different outcomes. Secondly, when we revisit the policy problem and the converging state of data protection, the "federal-provincial" question seems to diminish in significance.

1. Formal structures of the state

The first factor that may have influenced the policy outcome is the impact of the institutional arrangements or logic of a system of government. This prominent school of thought, for instance, would argue that the nature of Canada's decentralised federalism would influence the possible outcome of any given policy.

Peter Hall, in his influential book *Governing the Economy* (1986), summarises this view by arguing that "the organisation of policy-making affects the degree of power that any one set of

actors has over the policy outcomes. As Weber (1958) noted, that should be particularly true in the modern era where politics and administrations have become increasingly organised activities."[201]

The premises of "institutionalist" or "state-centric theories" do make a degree of intuitive sense. The arrangements of Britain's unitary government and unwritten constitution, for instance, must impact public policy somewhat differently than the American decentralised congressional system. Thus the institutionalist question is: what about *within* the Canadian federation? How have the differing arrangements of provincialism and federalism affected the divergent policy outcomes?

One obvious explanation lies within the delegation of provincial responsibilities within the Canadian Constitution. While the Constitution relegates consumer issues to the provincial realm, there is a growing confusion over the exact nature, limits - and even desirability - of this division of powers in terms of consumer protection. This ambiguity is possibly why federal policy-makers have shied away from data protection in the private sector. Brian Foran, a policy aid to Bruce Phillips, contends they would have to hire a lawyer to clearly understand these complex arrangements. For Foran, unravelling this constitutional juggernaut is the key factor in any progress towards a Québec-like model at the federal level.[202]

Was it institutional confusion that contributed to the divergence in policy outcomes? Possibly, in part; but it was not necessarily "the" driving force for contrasting outcomes within the Canadian federal structure. In actuality, the comparative policy evidence marshalled by Bennett

points out that the opposite should happen; that in an insecure and confusing policy climate, there is more likely to be a convergence as policy-makers collectively venture out into the unknown. From a longer term perspective, the CSA Process may be evidence of a convergence happening.

However, there is another aspect that an institutionalist would draw our attention to: what about the divergent legal environments between Québec and the rest of Canada? As we know, Québec law is based on the civil law tradition while anglo-Canada is based on common law. Would not this condition the outcome of policy? It would, at first, seem commonsensical to answer yes. Bill 68, for example, did flow directly from changes within in the revised *Civil Code.* In this regard, it could also be argued that Bill 68 was necessary because civil law, by its nature, requires more detailed and specific statutes due to the fact that it does not have the precedential foundation of common law to fall back on. However, as we have seen, in practice the right to information privacy does fall through the cracks of common law; and there is a serious legislative hole to fill.

In opposition to the institutionalist argument, however, the empirical findings from Colin Bennett's research finds that formal structures of the state are not necessarily the most salient factors. He observes that

> "... at the level of statutory principle, convergence has been relatively unaffected by constitutional differences. Most basically, the fair information principles have bridged the legal systems of countries based on the common law tradition (the United States, United Kingdom, [and Canada] those based on the continental civil-law (Roman law) approach."[203]

2. The role of the bureaucracy

A subset of this institutionalist school of thought also examines closely the role and character of the bureaucracy in bringing about policy outcomes. This view argues that state officials can act in an autonomous manner, often exercising their policy preferences within the bureaucracy.[204]

In the case of public sector data protection, Bennett's analysis found the role of the bureaucracy as an important variable in explaining the outcome. This was because the data protection statutes would, in effect, be asking the regulators to regulate themselves. It was therefore expected that the bureaucracy would exhibit resistance in developing suitable data protection regimes.[205] While perhaps not as important for regulating the private sector, there is some indication that the nature of the bureaucracies in both Québec and Ottawa are important in understanding the divergence.

In Québec, one view suggested by Péladeau is that the state of the bureaucracy impacted the policy climate because it was going through a period of crisis in terms of restructuring and public perception. Péladeau argues that Bill 68 was seen as a "good news" piece of legislation in that it would help regain some public confidence in the government apparatus. In essence, proof that the bureaucracy was in fact responsive to public demand.

Also, as far as "state actors" are concerned, the influence of Paul André Comeau, the President of the Commission d'accèss à l'information, played an important liaison role between state officials and the consumer movement within Québec. Perhaps the state officials within Québec

were thus better positioned to engage in policy learning? They were able to understand in a comparative light the lessons of European data protection and foresee the need to harmonise information handling practices.

At the federal level, the structure of the bureaucracy may have also played (and will continue to do so) a part in differentiating the outcome. This particular policy area may be the site of conflicting mandates between departments within the civil service. Industry Canada, for instance, is in place to promote the growing sectors of economic activity within the Canadian business community. It naturally has underscored the "information technology" and the "commercial data" industry as an area of growth within the economy. Conversely, the Department of Justice's jurisdiction covers privacy and human rights issues. If there was some jurisdictional competition between these departments, perhaps there would be less of a problem; but, according to one Treasury Board official, the Department of Justice at present is very little engaged with privacy issues: "there are no official plans to update or revise the *Privacy Act*, only housekeeping changes to the *Access to Information Act*."[206] Meanwhile, Industry Canada is assuming centre stage with initiatives like the *Blueprint*. There is also the National Advisory Council on the Information Highway which will receive more attention in the near future. In this respect, it could be argued that the dominance Industry Canada's preferences has taken precedence over others; or more cynically, officials in this department could be viewed as a conduit for the interests of industry, and thus predispose the outcome to industry's favour.

Without question the "institutional" explanations do yield valuable insights. The configuration of federalism, the nature of the Canadian constitution, the different legal traditions, the role of state actors, and the state of the bureaucracy: all are important variables in determining this particular policy outcome. However, they do not explain everything nor are they necessarily the most salient.

3. The role of political culture

Another theoretical school in public policy literature examines the nature of the political culture within the state or jurisdiction. Verba defines political culture as "the system of empirical beliefs, expressive symbols, and values which define the situation in which political action takes place."[207]

In this case, the question would ask: what is it about Québec political culture that may help to explain this policy innovation? Hall argues that unearthing "national styles in policy-making," in cultural terms, "is often too sweeping to pinpoint and conceptually to circumscribe the differences between them."[208] While this may be true, public opinion surveys are a common gauge that seeks to measure (albeit imperfectly) the pulse of political culture. For instance, there may be some evidence within the Ekos survey of a cultural variation between francophones and anglophones. In this study, sixty percent (60%) of the francophones were concerned about invasions of privacy compared to forty-eight (48%) of the anglophones.[209] In addition, the Ekos survey suggested that "Québec residents are twice as likely as residents of other provinces to report awareness of privacy-related legislation or agencies: 33 per cent versus less than 15 per cent in any of the other provinces."[210]

One reading of the survey would suggest that Québéckers were exhibiting a stronger preference for the ideals of privacy. Possibly a bit of evidence could be found within what was mentioned earlier about the province's legal tradition. Throughout the policy debates, it was said by legal experts within Québec that notions of "the private life" go back centuries in Roman Law jurisprudence. Perhaps a hypothesis can be made that Québéckers had a better sense of privacy than other Canadians?

This postulate is quickly dismissed when the history of Québec is considered. Clearly, Québec has traditionally relied on communitarian beliefs which place less, not more, emphasis on the private life. The infamous "sign law" is an oft cited example of the Québec state subordinating individual rights to collective rights.

With this being the case, the public opinion results have some contradictions that need to be understood. Péladeau suggests that these can be resolved when we understand that "privacy" has traditionally been an Anglo-Saxon concept. Indeed, before 1982, the issue of privacy was heard mainly in anglophone Canada and not in Québec. It is true that Québec's jurisprudence has a notion of the "private life" but the proper French word is "liberté" which has different connotations. "Privacy," by virtue of convenience, has simply become its anglicised version.

The second factor, however, veers back to something that may exist within the political culture. According to Péladeau, Québeckers may have registered a higher concern for privacy in the opinion survey because Francophones, as a rule, are more responsive than Anglophones. Péladeau explained that francophones simply like to talk, whereas anglophones tend to be more

reluctant and suspicious of telephone opinion surveys. However, it should be noted that even this distinction is starting to change due to technology which has a habit of provoking attitudes that transcend culture.

Thus, while it cannot be claimed with much confidence that notions of privacy are intrinsic to Québec political culture, there may be some elements within Québec that are intrinsically different from other provinces, one of which may be the loquacious nature of francophones. Another view may be that Quebecker's are simply more politically sophisticated than the rest of Canadians; they know the issues and they like to talk about them. Whatever the case, the role of both public opinion surveys did serve an important purpose: it helped to back the legislative goals embedded within Bill 68. [211]

4. The interplay of social groups

One of the most plausible explanations as to why Bill 68 occurred in Québec, and not anywhere else in Canada, lies in the dynamic interaction of the social groups interested in privacy issues and database protection. These groups include the media, privacy and consumer advocates, the industry, and state actors.

In many respects, the Québec consumer and privacy advocates acted like "political entrepreneurs" in the pursuit of greater data protection.[212] The attitudes and language of Péladeau certainly suggest this. In retracing the development of Bill 68, Péladeau talks about "their first strategy" which was "to make sure that any legislative solution was not just a smoke screen for industry."[213] As he tells it, when it became clear that the first draft was relying on

self-regulation, he and others began to organise political opposition to the draft. *La Table* was formed to present a uniform front. Privacy and consumer experts, both local and international, were drawn upon to articulate the merits of a regulatory approach. The privacy consortia, in turn, fuelled the media with information to keep the issue "hot" in the minds of the public.[214] Consequently, the findings in the Ekos survey suggest that:

> Higher levels of awareness [of Quebeckers] may also be linked to the strength of the consumer and the public services users' associations movement and the priority that these movements have placed on privacy. [215]

In a similar vein, an equally important variable was an "activist media" that understood and gave a lot of coverage to privacy issues. Without this added pressure on government officials, and the educational function of the numerous articles about the importance of data protection in the private sector, it is doubtful that Bill 68 would have come to pass. Public opinion may not have been so poignant, and industry and bureaucratic resistance may have been strong enough to block the legislation. The comparative experiences in data protection also confirm that the media is an important ally in the policy process.[216]

By contrast, the anglophone media pays sporadic attention to privacy issues, with some journalists more likely to criticise data protection statutes. For instance, the influential B.C. columnist, Vaughn Palmer, distrusts information privacy because "ones individual's invasion of privacy is another's freedom of information." It is possible to assume that Mr. Palmer places more importance on a society's "openness" than individual privacy. And plainly, his stance makes a certain degree of sense considering the nature of his profession. Fortunately, there are signs that the national media is beginning slowly to join the information privacy cause. We

now see occasional segments speaking about to the need to regulate the private sector. For instance, last October, CTV's *The Sunday Edition* aired a long piece on the need to control what companies do with our personal information; CBC Radio's popular program *Morningside* has interviewed both Bruce Philips and David Flaherty several times in the past year.

Clearly, the vectors of social groups are aligned somewhat differently on the federal stage. The media is not fully on side and the privacy and consumer advocates do not figure as predominantly as they do within Québec. A possible reason for this is because the voice of industry has traditionally been the loudest within federal policy-making circles. With the issue of data protection, this could continue to be the case for economic reasons alone. Here we have a growth industry - the electronic information sector - which has great potential to enhance the Canadian economy. With this being the case, it is quite plausible that some officials at Industry Canada would be more sympathetic to the arguments from industry that arguments from small, special interest groups like privacy and consumer advocates.

Another explanation why the privacy advocates are so strong within Québec and not within Ottawa is size. Péladeau describes Québec as being like "a little village." The province is simply smaller and thus easier for messages to be heard, as opposed to the enormity of the federal political stage. Therefore, in this respect, perhaps the fact that Québec is a province matters a great deal.

While the emergence of a consumer movement nationally is difficult to conceive of or measure (at least one similar to the one in Québec), there are perhaps some signs of its potential. The

recent political opposition to the Rogers Cable Network imposing a "negative option" on consumers for additional television channels is a good example of the power of the consumer in forcing industry to pay attention. The outrage pouring out from this event seemed to reveal a dormant but hostile sentiment among Canadian consumers towards the "arrogance of industry."[217]

It is this variability in public opinion which may be the most decisive factor in changing the federal political landscape. Clearly, Canadians' temperament can change overnight, as it did with Rogers Cable. Perhaps it will take only one flagrant example of information abuse - like the woman in Montréal - to provoke public opinion, and thus pressure our legislators to fill the legal void in consumer protection. Even John Manley, Minister of Industry Canada, has been quoted as saying on television, "the line has to be drawn with the selling of information and the lack of control in the private sector."[218] Meanwhile, privacy advocates speculate that the CSA process may be industry's "last chance" to make self-regulation work before other forces - like public opinion - will bring about regulation.[219]

This tendency for the public to be "event-driven" is not new. Some of the comparative lessons of Flaherty's and Bennett's studies show that the "open window" or momentum for public sector statutes often came after an event that struck the public consciousness. In the United States, it was Watergate; in Sweden it was the 1986 study "Project Metropolitan";[220] and for the private sector, we have already seen what happened with Lotus's MarketPlace.

However, having said this, it will take additional public opinion research to measure if there is a constancy of support for consumer issues like information privacy to warrant the assertion that

a consumer movement is emerging within Canada. At present, it appears that Canadians are spurious in their awareness of privacy issues, and sporadic in their support. It may take a while before the rest of Canada is as sensitised to the debates over information privacy as are Quebeckers. It is the hope of many advocates that the debates surrounding the Information Highway will heighten public awareness of "consumer surveillance" and the potential for information misuse and abuse.

5. The political constraints of economics

Economic constraints can be the most decisive factor in determining any given policy outcome. Fiscal restraint, government cut-backs, and widespread deregulation characterise the policy climate in the 1990s. In the national case, it is quite conceivable that these arguments will be marshalled against any regulatory solution to the tension over personal information. However, similar arguments were heard throughout the public hearings for Bill 68, and Bill 68 still managed to be passed. One possible explanation for this is that Québec privacy advocates were able to convince the government of Bill 68's instrumental benefits; that is, the enhanced efficiency in information handling practices, economic benefits of EC trade, and avoidance of liability issues. In this case, it is a matter of whose voice is heard amidst the rigmarole of the political process. At present, it appears that these voices have not reached the national stage, but could do so if the CSA process is able to mediate the differences.

Another economic explanation, however, has to do with the overall economic philosophy of the current government. As Flaherty showed in his study, the anti-bureaucratic thrust of the Thatcher and Reagan regimes during the 1980's were not the most hospitable climates for data

protection.[221] The emphasis was on fighting fraud and enhancing administrative efficiency, and electronic surveillance was (and still is) very useful for these purposes.. With the present political climate, there may be a similar temptation by the Canadian government to engage in surveillance at the expense of civil liberties. In today's world, there are arguably even greater imperatives than ever before to do so, with the economic pressures for businesses to survive in the global marketplace, and the imperative of bureaucracies to reinvent themselves so that they can meet the challenges of modern governance.

4.4 The Salient variables

In sum, there are several important explanation for the divergent outcome. Firstly, the outcome had to do with institutional factors. The decentralised nature of the federation made Québec an easier arena for consumer groups to place their concerns on the government agenda. Moreover, the constitutional confusion surrounding consumer protection helped to maintain the *status quo.* According to Michael Atkinson this is far from surprisingly. In his words "[p]erhaps no institutional arrangement contributes more to policy diffusion and structural incoherence than federalism."[222] And lastly, the changes in the legal environment contributed directly to the emergence of Bill 68.

However, these institutional factors by themselves are not enough to explain the outcome, which brings us to the second, and most important, variable: the role of the privacy advocates and an activist media. Although Colin Bennett warns against exaggerating the influence of a group of individuals with no institutional authority, the existence of these two elements alone explain the development of Bill 68.[223] This breaks with the findings of Bennett who does not

find anywhere (e.g. in United States, Britain, Sweden or Germany) "a coherent coalition of interests that has been able to affect the content of the law or the nature of the policy instrument in any significant way."[224] The unique relationship between the media and privacy advocates, however, is perhaps dependent upon the smaller, "village-like" nature of the province. In a bi-directional way, the two elements were able to stimulate public debate and increase public support for privacy issues, which previously were an "Anglo-Canada" concern. State and industry officials eventually had no choice but to look at data protection for the private sector as a serious option. Less influential variables were therefore political culture, the autonomous role of state officials, and economic constraints. This is not to say that they did not play a role; it just means that this role was not as significant as institutional factors and the role of groups and the media.

By contrast, there are absent the salient variables within the national CSA process. There is neither a strong consumer movement nor an activist media at present. Also, industry is well-organised within national sector organisations like the CDMA. In terms of lobbying, industry also has traditionally had the ear of senior officials and politicians in contrast to consumer rights groups. Consumer service associations are also under-funded and almost non-existent.[225]

Another important factor that may have impeded convergence is without question the threat of further economic constraints. With a serious deficit crisis and a climate of deregulation, any arguments propounding further bureaucracy is bound to receive less attention.

There are nevertheless some strong pressures to converge. The first is the development of the Information Highway which must deal with the issue of information privacy if it ever hopes to become a reality. Secondly, the role of public opinion may also be a strong factor in encouraging legislators to look at data protection for the private sector. Thirdly, the economic costs of EC trade barrier's on the transborder flow of personal data may be enough to convince industry that Quebec's model is the way to go. These three factors, and the activism of the Privacy Commissioner, may have already produced a sign of convergence by disrupting the *status quo* and providing the main thrust towards the CSA process.

Chapter Five - Lessons from Québec

Québec's case is interesting because it presents the observer with a noticeable convergence and divergence in comparative public policy. On the one hand, it represents a convergence in terms of world-wide data protection. On the other, it is the only jurisdiction in North America that has regulated the private sector in its use of personal information. Thus, with this exemplar in data protection, what lessons can we learn?

5.1 Lessons for the policy model

The first set of lessons underscore the merits of the Québec regulatory model, and concludes that it is the better policy in assuaging the heady imperatives that drive the tension over personal information. I would venture, however, that the underlying rationality of this model is no coincidence; it is a product of decades of policy-learning and lesson-drawing within the field of data protection. It is thus based on what "works" in the real world of policy-making.

The model's key features are: an independent oversight body or "data commissioner", a reliable enforcement mechanism, an effective form of redress for individuals, legislated "fair information principles", and a constitutional right "to information privacy".

Some analysts, however, would argue that there is one key problem with this model: the constitution. Many commentators posit that Bill 68 could not be applied to the federal level because consumer law is simply a provincial power. (No further discussion. Case closed.) Notwithstanding this, I would still argue to the contrary for a number of reasons. Firstly, the argument that consumer issues must *remain* within provincial jurisdiction loses its power

because it does not reflect present technological realities. As Bruce Phillips sees it, the environment created by information technology in effect makes the federal-provincial question secondary. He charges that "[o]f course there are jurisdictional questions. But electronic communications leap political boundaries. If there is to be free trade in information, we must all sing from the same songbook."[226]

Secondly, there are also some economic trade reasons why the provincial forum should not be the locus for data protection in the private sector. As Flaherty emphasises: " it is especially important that national law on data protection remain the main form for the handling of transborder data flow issues and will continue to remain the place where such problems can be dealt with."[227] If Canadian industries hope to avoid trade tariffs on their information handling practices, they will have to rely on the federal government for a unified and concerted front.

The recent June signing of the *Internal Trade Agreement* may be an indication of such a trend - and it even embodies some of the goals of data protection. This agreement is highly significant because one of its key objectives is to reconcile and harmonise "regulations and standards" that "provide for the free movement of people, goods, services and capital within Canada." This goal applies particularly to consumer protection issues[228]and could easily act as a national platform for a future "omnibus approach" in protecting information privacy.[229]

Fourthly, from an institutional perspective, the *EC Directive* has emerged in the midst of a far more difficult federal arrangement, largely because it is supranational. The point here being that there is no *a priori* reason why, in principle, Bill 68 cannot serve as a template for the

decentralised Canadian federal system. The provinces have certainly been the vanguard for policy reform in the past, and they will continue to be in the future.

However, before we leave the lessons on the policy model, let me make another clarification. The CSA process and the Québec model are not mutually exclusive. The two models are, in practice, artificial distinctions. In real terms, it is quite conceivable that they represent incremental steps in the same direction. The CSA process may be the essential forum where consensus is achieved regarding the nature of the problem and thus the best method to go about addressing it. In this respect, the Québec model may be a legislative precursor of data protection to come.

5.2 Lessons for the policy process

The second set of lessons tempers the prospects of a Québec model appearing on the national stage. The criteria, or specific set of conditions, that brought about Bill 68 within Québec are not overwhelmingly present within the national CSA process. For instance, there is little evidence of a strong, national consumer movement, nor is there a knowledgeable group of media experts within the rest of Canada. These two forces alone could have driven the policy outcome of Bill 68. Also, the sheer size and complexity of the federal policy-making stage perhaps has inhibited the development of a unified consumer lobby. As a consequence, the arguments propounding the merits behind a regulatory model for the private sector have not been heard. For these reasons, and more, it is probably more realistic to predict that the Québec model will be emulated first at the provincial level.

There are signs, however, that the public mood is changing in favour of increased data protection, and the press is slowly devoting more coverage to privacy issues. Thus, despite the various constraints within the federal policy-process, a shift and decisive surge of public wrath, possibly triggered by an "event", may overcome even the steepest of hurdles.

Furthermore, the enigmatic nature of the problem may add further impetus for legislators to act. For instance, the international implications and the possible trade threats from the EC may add incentive and convince industry to support enhanced data protection. Also, the ramifications of technological change are breeding a climate of uncertainty, and thus an insecure policy environment. As Bennett's study indicates, uncharted territory in policy-making, especially with technological problems, creates pressures to convergence and not the reverse. With initiatives like the "Information Highway" on the horizon, the CSA Process may represent the beginning of a national convergence.

5.3 Lessons for data protection

Raab notes that learning in the field of data protection is challenging for several broad reasons. He argues that it is "a new and rapidly changing field for the exercise of power, and therefore one in which the main techniques and systems of governance must be tested."[230] Also, very much related, are the "ambivalence of goals to be pursued in data protection." In short, policy-maker's are uncertain where to steer policy.[231]

For these two reasons, it is thus difficult to assess what is good data protection and what is bad. This analysis has nevertheless attempted to do so, using as an example, Québec 's Bill 68.

However, the choice I made was purely for lack of an alternative. With what we know about our changing techno-political environment - the piles of empirical evidence pointing to the accelerated development and widespread application of information technology - even the policy area of data protection has its problems too. Thus, while policy makers should step up the process of "learning" when it comes to data protection, they should also rethink the way information technology is governed.

Bennett suggests that one necessary change is in the way we view these issues. He argues that "privacy should be seen as just one value to be addressed within a more comprehensive 'information policy' for the 'information society'." The problem should thus be viewed holistically, and the unifying concept be shifted to *information*.[232] Bennett points to the "expanding range of concerns to which data protection authorities are having to give attention." By these, he means the *types* of information privacy issues surrounding such events as mandatory AIDs testing and record-sharing, urinalysis, and DNA fingerprinting.

But observers of technology have for decades called for a holistic view for governing technology.[233] In their view, the central problem resides in the functional design of the modern state, which is clearly not conducive to our rapidly changing, technological society. A case in point is the fact that there is little evidence anywhere of a well-developed system for the governance of information - yet we live in an "information society" with "information technology" proliferating in every crevasse of modern life! Raab aptly points out the absurdity of this by noting:

> "where there is 'economic policy', there is yet little or no 'information policy.' Where there is - almost as an inherent part of statehood - great power to effect policy in the one field, in the other there is little."[234]

It is Hoberg's contention that "if political values change or the distribution of society changes" then a traditional policy style is subjected "to a crisis of legitimacy."[235] This is unquestionably the case with any policy field that tries to govern information technology, and may soon be the case for the field of data protection.

Thus it is here where policy-makers need to make the most progress. They need to learn how to innovate structures, mechanisms and institutional processes so that "new problems can continually be confronted and old structures continually discarded;"[236]and importantly, they need to do so in a way that does not infringe our basic human rights. The analysis put forward in this dissertation offers one way of dealing with a changing technological environment that has two parts: first, legislate a plain language law that protects information privacy; and two, establish a dynamic and effective oversight mechanism that can educate the public about important issues as well as monitor and evolve with the changing technological times.

Conclusion: Governance in an Information Polity

The enduring thing about the Industrial Revolution was not the factories, the steam engines or machines, it was the fact that a whole new society was created: one that made unbelievable material and social progress, but also one that had abysmal social problems with child labour and abject poverty.

Similarly, we need to ask ourselves what kind of society the Information Revolution is creating. There will be indeed exciting, positive changes like the chance for modern bureaucracies to "reinvent" themselves; and individuals will have the potential to be empowered with access to more information and knowledge about the world around them than even before in human history. However, with the positive changes are also negative ones. The tension over personal information is an excellent example of both the beneficent and darker sides to information technology, and the techno-political climate in which it coexists. The challenge of governance is to find the appropriate balance for our Information Society. This balance, however, is contigent on which values society deems as being the most important: should efficiency win over democratic notions of privacy, human dignity and self-determination, or the reverse? In light of the strong forces of technology and social change tipping the balance in favour of efficiency, it is crucial that the state intervene on the side of privacy, otherwise Marshall McLuhan's prediction will come true. Technology will destroy privacy, and there will be no place to hide.

[1] This story was related by Pierrôt Péladeau in a telephone interview on September 1, 1994. Mr. Péladeau is currently working as an independent privacy consultant with his company, *Societe Progestacces* in Québec .

[2] This phrase was first coined by Hugh Helco in *Modern Social Politics in Britain and Sweden.* New Haven: Yale University Press, 1974.

[3] This article in particular formed the main inspiration for this thesis. Colin Bennett, "The Formation of a Canadian privacy policy: the art and craft of lesson-drawing", 33 *Canadian Public Administration* : 556.

[4] Christine Bellamy and John A. Taylor, "Introduction: Exploiting IT in Public Administration - Towards the Information Polity?", 72 *Public Administration* (Spring 1994):1

[5] George Hoberg, "The Question of Convergence Across Policy Areas" *mimeo* October 31, 1993: 2.

[6] This insight was derived from Pierrôt Péladeau in a telephone conversation, September 1, 1994.

[7] Chapter 1

Colin Bennett, *Regulating Privacy.* Ithaca, New York: Cornell University Press, 1992: 251.

[8] This is gleaned from Robert Babe's citation of Kenneth Arrow's declaration that "the meaning of information is the reduction of uncertainty" in Robert E. Babe (ed.), *Information and Communication in Economics.* Boston: Kulwer Academic Publishers, 1994: x-xi.

[9] OECD, *Trends in the Information Economy.* Paris: OECD, 1986: 9.

[10] Treasury Board of Canada, *Powering Up: A Review and analysis of information technology expenditure trends in the Canadian government 1986-1992.*

[11] Bennett, (1992): 15.

[12] David Lyon, *The Electronic Eye: The Rise of Electronic Surveillance.* Minneapolis: University of Minnesota Press, 1994: 23.

[13] From a letter of correspondence written by Colin Bennett to David Johnson, Chair for the Advisory Council on the Information Highway, Industry Canada on April 11, 1994: 2.

[14] see Harold Innis, *The Bias of Communication* (1951) and *The Empires of Communication* (1950); and Robert E. Babe "Preface" *ibid.,* x-xi.

[15] [*emphasis by author*] Iskender Gokalp, "On the Analysis of large technical systems", *Science, Technology and Human Values* 17 (Winter 1992): 58.

[16] *ibid.*

[17] *ibid.*

[18] see Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information.* Boulder, Colorado: Westview Press, 1994; Iskender Gokalp (1992); David Lyon, (1994).

[19] see Geraint Parry, "The interweaving of foreign and domestic policy-making, 28 *Government and Opposition* (Spring 1993) ; Miriam L. Campanella, "The effects of globalization and turbulence on policy-making processes", 28 *Government and Opposition* (Spring 1993):190-205.

[20] Francisco R. Sagasti, "International cooperation in a fractured global order", *Futures* (May 1990): 419.

[21] Charles D. Raab and Colin J. Bennett, "Protecting Privacy across borders: European policies and prospects", 72 *Public Administration* (Spring 1994): 97.

[22] *ibid.* 98.

[23] René Laperriere, René Côte, Georges A. LeBel , "The Transborder flow of personal data from Canada: International and comparative law issues", *Jurimetrics Journal* 32 (Summer 1992): 565.

[24] See Harvey Gellman, "Strike up the Bandwidth", *Acumen* (June-July 1994): 11-12. Last year the large telephone company, Bell Atlantic, and Telecommunications Inc., the world's biggest cable-television company, made a precedent-setting deal to merge their companies to form "an information-industry conglomerate of unprecedented scale and scope." At the last minute, however, the deal fell through because of resistance amongst Stockholders.

[25] See Paul Kennedy, *Preparing for the twenty-first Century.* New York: Random House, 1993; and Robert Heilbroner, *Twenty-First Century Capitalism.* Toronto: CBC Massey Lecture Series, 1992.

[26] Gokalp, (1992): 64.

[27] Treasury Board of Canada, *Blueprint for Renewing Government Services Using Information Technology.* Ottawa: Government of Canada, 1994: vii.

[28] Bellamy and Taylor, (1994): 5.

[29] Bennett (1992): 86.

[30] Heilbroner, *Twenty-First Century Capitalism* (1992)

[31] Rod Dobell and Steven Rosell, "The Information Society: Some questions concerning Governance", (eds.) David W. Conklin and Lucie Deschenes, Proceedings of a *Conference on Information Technology: Globalization, Diffusion, Innovation and Retraining.* Toronto: The Institute for Research on Public Policy and Canadian Workplace Automation Research Centre, June 7-8 1989: 5.

[32] Lapierrere (1992): 559.

[33] Bellamy and Taylor, 10

[34] OECD *Guidelines on the Protection of Privacy and Transborder Flows of data: Implications for Canada* (1985): 4.

[35] [*emphasis orginial]* Vincent Mosco, "The political economy of communication: lessons from the founders", (ed.) Robert Babe in *Information and Communication in Economics.* London: Kulwer Academic Publishers, 1994: 114-115.

[36] *ibid.*

[37] U.S. Department of Commerce, "Principles for Providing Information" for the Privacy Working Group, National Information Infrastructure Task Force, 1994.

[38] see Jacques Ellul, *The Technological Society;* Lewis Mumford, *Technics and Civilisation.* New York: Harcourt Brace Jahanovich, 1963; and more recently, Langdon Winner, *Autonomous Technology: Technic-out-of-control as a theme in political thought.* Cambridge, Mass.: MIT Press, 1977.

[39] This definition is found in Bellamy and Taylor, (1994): 9.

[40] Mosco, (1994): 107

[41] Bellamy and Taylor, (1994): 5.

[42] Joel Garreau, "The Conspiracy of Heretics", 2 *Wired Magazine* (November 1994): 102.

[43] Lyon, (1994): 61.

[44] Bennett, (1992): 15.

[45] Although very controversial and highly disputed, Lyon maintains that:

> "the 'postmodern condition' is characterised by the 'collapse of metanarratives'. That is to say, modern verities such as the redemptive belief in science, technology, or democracy have fallen into disrepute during the twentieth century..."

Lyon, (1994): 18. Also, see Jean-Francois Lyotard, *The Postmodern Condition.* Manchester: University of Manchester Press, 1984.

[46] Marshall McLuhan and Bruce R. Powers. *The Global Village.* New York: Oxford University Press, 1989: preface.

[47] *ibid.,* 93

[48] See the special issue "The Digital Individual," 10(2) *The Information Society: An International Journal* (April-June 1994).

[49] Mark Poster. *The Mode of Information.* Cambridge, Mass.: Harvard University Press, 1994.

[50] *ibid.*

[51] In a behavioural context, it is Thomas H. Davenport's contention that changing technology only reinforces behaviours that already exist. See "Saving IT's soul: Human-centred Information Management," *Harvard Business Review* (March-April 1994): 120.

[52] Alan F. Westin similarly describes "society, social values and social change in terms of a Newtonian model of action, reaction and dynamic equilibrium" in "The Protection of Privacy in the Public and Private Sectors," (ed.) Bernard Barber, *Effective Social Science: Eight Cases in Economics, Political Science and Sociology.* New York: Russell Sage Foundation, 1987: 129.

[53] Lyon, (1994): 139.

[54] Definition cited in Ralph Oman "Reflections on the changing shape of database protection," 40 *Federal Bar News and Journal* (May 1993): fn. 1 at 237.

[55] *ibid.,* 232.

[56] Frank V. Cespedes and Jeff H. Smith, "Database Marketing: New Rules for Policy and Practice", 34 *Sloan Management Review* (Summer 1993): 9.

[57] *ibid.,* 11.

[58] Interview with Brenda Clarke, president of *Direct Results Marketing* on September 31, 1994 in Vancouver, BC.

[59] Lyon, (1994): 142.

[60] *ibid.*

[61] From an informal interview with a member of Cathay Pacific's marketing division in Vancouver on September 12, 1994.

[62] David McKendry, "Business and consumers conflict over privacy", *Canadian Speeches* (May 1992): 32.

[63] Gandy, (1994): 66.

[64] *ibid.*

[65] For example, Zeller's "Club Z Points" and Save'On Foods' "Select Plus".

[66] Incidentally, all this information was keyed in manually in Taiwan because scanner technology is still too unreliable for reading large quantities of information.

Also in B.C. the Ministry of Health is talking about developing a database called *Pharmanet*, which will house all the pharmaceutical records of British Columbians. The rationales for this database are: (1) adminstrative efficency, like avoiding fraud, and duplication; (2) health concerns such as drug allegeries and side-effect; and (3) for customer service. However, the Privacy Commissioner is raising some important questions about the confidentiality of the data within this database; whether in practice, privateorganisations (e.g. pharmeceutical companies, police) will somehow be able to get access to it.

[67] This is not possible under BC's law which considers it an unreasonable invasion of a third party's personal privacy if "the personal information consists of the third party's name, address or telephone number and is to be used for mailing lists or solicitations by telephone or other means", *The Times Colonist,* June 3, 1994: A2

[68] Lyon, (1994): 153.

[69] Gandy, (1994): 66.

[70] *ibid.*

[71] Lyon (1994): 141.

[72] *The Times Colonist,* (June 3, 1994): A1.

[73] John W. Awerdick, "Who owns the data in the data base?", *39 The Practical Lawyer* (June 1993): 19.

[74] Cespedes and Smith, (1993): 11.

[75] *ibid.*

[76] Paul Wallich, "Trends in Communication: Wired Pirates", *Scientific American* (March 1994): 90-101.

[77] These issues are emerging steadily into public debate. For instance, Mark Forsythe on CBC Radio interviewed Mish Cobey, author of *Information Warfare*, about the increasing prevalence of information abuse within cyberspace. Cobey cited two examples. The first is the frequency of character assassinations through impersonated electronic i.d.'s on the Internet. The second is the use of "EMP bombs" or "radio weapons" that can knock out whole computer systems.

[78] Robert Heilbroner, *21st Century Capitalism.* Toronto: CBC Massey Lecture Series, 1992: 101.

[79] *ibid.*

[80] [*emphasis added]* Alan Westin cited in Colin Bennett, "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s," 16 *Science, Technology and Human Values* (Winter 1991): 59.

[81] Alan Westin in Bernard Barber (1989):

[82] Cespedes and Smith, (1993): 8.

[83] Privacy Commissioner of Canada, *Annual Report 1993-1994:* 5.

[84] *The Vancouver Sun,* April 13, 1994: B7.

[85] Gary T. Marx. "Privacy and Technology," *Whole Earth Review* (Winter 1991): 90.

[86] Cespedes and Smith, (1993): 13.

[87] This is a chapter title from Lyon (1994).

[88] *ibid.*

[89] Gandy, (1994): 1.

[90] see Cathy Goodwin. "Privacy: Recognition of a Consumer Right," 10 *Journal of Public Policy and Marketing* (Summer 1991) 149-166.

[91] Colin Bennett in the *Times Colonist* (April 8, 1993): A5.

[92] *ibid.*

[93] Raab and Bennett, (1994): 98.

[94] Charles Taylor, *The Malaise of Modernity.* Concord, Ont: CBC Massey Lecture Series, 1991.

[95] David Flaherty, *Protecting Privacy in Surveillance Societies.* Chapel Hill: The University of North Carolina, 1989: 9.

[96] Colin Bennett, *Regulating Privacy* (1992): 29-30.

[97] David Lyon, (1994): 171.

[98] *ibid.*

Chapter 2

[99] In Canada, for example, this is evident in the recent CSIS scandal. The United States, also, has pending the *Digital Telephony Bill.* See the *New York Times,* 28 Februrary 1994:D1, "The Push for Surveillence Software."

[100] Lyon, (1994):

[101] Alan F. Westin, *Privacy and Freedom,* New York: Athenaeum (1967): 7 cited in Bennett (1992): 14.

[102] Bennett, (1992): 44.

[103] *ibid.,* 13.

[104] *ibid.*

[105] *ibid.,* 4.

[106] *ibid.*

[107] *ibid.,* 112.

[108] *ibid.*

[109] Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data: Implications for Canada.*

[110] *ibid.*

[111] *ibid.*, 7.

[112] *ibid.*

[113] *ibid.*

[114] Flaherty, (1989): 21.

[115] *ibid.*, 157

[116] *ibid.*, 101.

[117] *ibid.*, 165.

[118] Bennett (1992): 157.

[119] *ibid.*

[120] Table 2.3 also shows another discrepancy over scope which lies over the *types* of personal records covered. West German and Britain protected only automatic records and not manual ones.

[121] Bennett (1992): 114

[122] Flaherty (1989): 1.

[123] Raab and Bennett, "Protecting Privacy across borders: European policies and prospects", 72 *Public Administration* (Spring 1994): 106.

[124] *ibid.*, 105.

[125] Rabb and Bennett (1994): 106.

[126] David Flaherty, Office of the Information & Privacy Commissioner of British Columbia, *Annual Report 1993-1994.* Victoria, BC.: Queen's Printer (1994): 29.

[127] Raab and Bennett (1994): 95.

[128] Privacy Commissioner of Canada, *Annual Report 1993-1994.*

[129] National Assembly of Québec, *Charter of Human Rights and Freedoms*, Chapter C-12

130 Commission d'accèss à l'information, "Contact: Advice on the confidentiality of personal information", Québec (Québec): March 1994.

131 Lola Fabowalé, "Voluntary Codes: A viable alternative to government legislation?", Ottawa: The Public Interest Advocacy Centre, May 1994.

132 Canadian Standards Association, "The CSA Privacy Initiative Model Code for the Protection of Personal Information". Toronto: CSA, March 1992.

133 See Province of British Columbia, *Credit Reporting Act*, 1979 RS Chapter 78. Also, at the federal level, the new *Telecom Act* (which came into force on October 25, 1993) has section 8 entitled the "Protection of Privacy of Persons." Michael Hennessy argues that in practice this statute does not really confer substantive protection to personal information, but suggests that within the telecommunications sector, the Canadian Radio and Telecommunications Commission (CRTC) might well function as an oversight mechanism over industry for information privacy. Michael Hennessey, all policy advisor for the CRTC, *telephone interview* on September 12, 1994.

134 Joshua D. Blackman, " A proposal for federal legislation protecting information privacy across the private sector", 9 *Santa Clara Computer and High Technology Law Journal* (1993): 446-450.

Chapter 3:

135 Marie Vallée, *telephone interview* on October 13, 1994.

136 Privacy Commissioner of Canada, *Annual Report 1993-1994:* 18.

137 *ibid.*

138 See Blackman's discussion of *Griswold v. Connecticut* at 432; and Colin Bennett's on 66-67.

139 Bennett, "The Formation of a Canadian privacy policy: the art and craft of lesson-drawing", 33 *Canadian Public Administration*: 565.

140 Blackman, (1993): 435.

141 Peter Doresy, Credit Reporting Branch, *telephone interview* on September 10, 1994.

142 Blackman (1993): 436.

143 *ibid.*

144 Mary Gardiner Jones, "Privacy: A Significant Marketing Issue for the 1990s", 10 *Journal of Public Policy and Marketing* (Spring 1991) 139.

145 This document was sent to me by Jacques St. Amant, from the Association coopérative d'économie familiale du Centre de Montréal.

146 Bob Crow of ITAC, *telephone interview* on September 1, 1994.

147 *ibid.*

148 Péladeau, *telephone interview,* October 4, 1994.

149 Richard P. Maurel from the Office of the Privacy Commissioner of Canada. The working paper titled "Québec's Legislation on Privacy Protection in its Private Sector: Analysis."

150 Flaherty, (1989): 11.

151 Flaherty, (1989): 14.

152 Péladeau, *telephone interview* on October 14, 1994.

153 Flaherty, *Protecting Privacy in Surveillance Societies* (1989): 374.

154 Brian Foran, senior policy analyst with the Office of the Privacy Commissioner of Canada, *telephone interview* on October 12, 1994.

155 *ibid.*

156 Cespedes and Smith, (1993): 8.

157 Mosco, (1994): 108.

158 Péladeau, *telephone interview*, September 1, 1995.

159 Flaherty, Office of the Information & Privacy Commissioner of British Columbia, *Annual Report 1993-1994.* Victoria, BC.: Queen's Printer (1994): 29.

160 Murray Long, Senior Policy analyst for SENTOR, *telephone interview* on September 1, 1994.

161 Bennett, (1994): 98.

162 Fabowalé, (May 1994): 1.

163 *ibid.,* 152.

Chapter 4:

164 Title borrowed from Paul-André Comeau, President of the Commission d'accès à l'information du Québec, "The protection of personal information in the private sector: An important step forward by Québec's National assembly", notes for a lecture at *Privacy, Laws and Business*, 6th Annual Conference, Oxford, U.K. (June 38, 1993).

165 National Assembly of Québec, *Charter of Human Rights and Freedoms*, Chapter C-12.

166 There is an "inside story" attached to the revising of Québec's *Civil Code* which escapes the scope of this paper.

167 The changes were so substantial that all Québec lawyers and judges had to attend 90 hours of lectures in order to practice. See Bob Babinski, "Moving from the Napoleonic Age to the Twenty-First Century", *Canadian Lawyer* (May 1993): 22-24.

168 *L'accès*, (March 1994), newsletter to the Commission d'accès à l'information.

169 Pierrôt Péladeau, *telephone interview*, September 12 and 27,1994.

170 Colin Bennett, (1992): 62

171 Péladeau, *telephone interview* on October 14, 1994.

172 *ibid.*

173 There were two noticeable absentees in *La Table:* the Québec section of the *Consumer Association of Canada* and curiously, the Québec *Commission d'accès à l information.*

174 Michel Venne, *Vie privée & démocratie à l'ère de l'informatique.* Insitut Québécois de Recherche sur la culture, 1994.

175 For instance, on September 28, 1994 Radio Canada featured a two and a half hour program on privacy issues on a program analogous to *Morningside* which heard from privacy experts like Pierrôt Péladeau. Similarly, Mr. Péladeau is working in conjunction with *Le Devoir* in putting together a cover story for Industry Canada's Information Highway Report.

176 Péladeau, *telephone interview* on September 12, 1994.

177 For instance, when the International Civil Aviation Organisation publicly declared that the bill would negatively effect the operations of its headquarters in Montréal, it was dealt an embarrassing counter-blow by the media and experts who cited their flawed data and inconsistent arguments.

178 OECD, *Guidelines* (1984).

179 *ibid.*

180 Lola Fabowalé, *Voluntary Codes: A Viable Alternative to Government Legislation?* Ottawa: the Public Interest Advocacy Centre, May, 1994.

181 Bennett, "The formation of a Canadian privacy policy" 558.

182 *ibid.,* 560 in fn.31

183 Exceptions have been national programs like CBC's *Morningside* which are devoting time to discussing the problems over information privacy. In the last few months both Bruce Phillips and David Flaherty have been interviewed, and *The Sunday Edition* also ran a long piece on "Personal information out-of-control" on October 21, 1994.

184 Bennett, (1992).

185 Flaherty, (1989):

186 Bennett (1992): 565

187 Statement from a telephone conversation with Eleanor Zasalack from Treasury Board, October 12, 1994.

188 *Focus* (Spring 1992):5

189 Privacy Commissioner of Canada, *Annual Report 1993-1994.* Ottawa.

190 Bob Crow, Senior Policy Advisor, Information Technology Association of Canada (ITAC), *telephone interview* on September 1, 1994.

191 Michel C. Globensky, "Tracking the Future: The Privacy Issue and Information Industry, a Corporate Perspective", Notes for a presentation at the Credit Association of Canada, Ottawa Chapter, May 18th, 1993: 2.

192 Flaherty's research in *Protecting Privacy in a Surveillance Society* (1989) indicates that a strong, pro-active Commissioner is part of a successful data protection regime

193 Privacy Commission of Canada, *Annual Report 1993-1994*: 8.

194 *ibid.,* 9.

195 *ibid.,* 11.

196 *ibid.*

197 Paul André Comeau, (June 28, 1993): 1.

198 Bob Crow, *telephone interview* (September 1, 1994)

199 Canadian Direct Marketing Association, *Communicator: News for Canada's Direct Marketers* (Winter/Spring 1993):1

200 *ibid.*, 7.

201 Peter Hall, *Governing the Economy: The Politics of State Intervention in Britian and France.* New York: Oxford University Press, 1986: 19.

202 Brian Foran, Office of the Privacy Commissioner, *telephone interview* on October 14, 1994.

203 *ibid.*

204 Eric Nordlinger, *On the Autonomy of the Democratic State.* Cambridge, Mass.: Harvard Press, 1981.

205 In the case of Britain, in particular, Bennett found a great deal of this.

206 Eleanor Zasalack, *telephone interview* on October 4, 1994.

207 Verba S. "Comparative political culture," in L. Pye and S. Verba (eds) *Political Culture and Political Development.* Princeton: Princeton University Press, 1965: 513.

208 *ibid.*, 8.

209 Ekos Associates, *Privacy Revealed* (1993): iii.

210 *ibid.*, 27.

211 Ekos Associates (1993): 27.

212 Term borrowed from Schumpeter (1947).

213 Péladeau, *telephone interview* on September 12, 1994..

214 *ibid.*

215 Ekos Associates (1993): 27.

216 Bennett, (1992): 243.

217 CBC Radio, *Morningside* (to be checked.)

218 CTV, *The Sunday Edition* (October 1994).

219 Péladeau, telephone interview on September 1, 1994.

220 Flaherty, (1989): 6 and 314.

221 *ibid.,* 306 and 309.

222 Michael M. Atkinson. "Introduction: Governing Canada," *Governing Canada: Institutions and Public Policy.* Toronto: HBJ, Holt, 1993: 11.

223 Bennett, (1992): 126.

224 *ibid.,* 206.

225 The Vancouver office of the Canadian Consumer Services Association is run by one volunteer and will likely be shut down in the near future. *Telephone conversation on September 1, 1994.*

Chapter 5

226 Privacy Commissioner of Canada, *Annual Report 1993-1994*: 6.

227 David Flaherty, Privacy Commissioner of British Columbia, *Annual Report 1993-1994*: 30.

228 *ibid.,* 13.

229 Government of Canada, Internal Trade Secretariat, "The Draft Internal Trade Agreement" (May 1994, Ottawa).

230 Charles Raab, (1993): 44.

231 *ibid.*

232 Bennett, (1991): 65.

233 See Ursula Frankin, *The Real World of Technology.* CBC Massey Lectures Series. Concord, Ontario: CBC Enterprises 1990; and Jack Barkenbus, "Can Advanced Technology and Open Democracy Co-exist?" *Journal on the Unity of the Sciences* 4(1) Spring 1991 pp.37-57

234 Raab, (1993): 45.

235 George Hoberg, "Environmental Policy: Alternative Styles", in (ed.) Atkinson, *Governing Canada.,* 1993.

[236] Raab, (1993) 44.

References

Awerick, John W. "Who owns the data in the database?" *The Practical Lawyer* 39 (June 1993).

Atkinson, Michael M. "Introduction: Governing Canada," *Governing Canada: Institutions and Public Policy.* Toronto: HBJ, Holt, 1993.

Babe, Robert E. (ed) *Information and Communication in Economics.* Boston: Kulwer Academic Publishers, 1994.

Babinski, Bob. "Moving from the Napoleonic Age to the 21st Century," 17 *Canadian Lawyer* (May 1993).

Banting, Keith and George Hoberg. "Canada and the United States in a changing world," *mimeo* (September 1991).

Bellamy, Christine and John A. Taylor. "Introduction: Exploiting IT in Public Administration," *Public Administration* 72 (Spring 1994): 1-12.

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

----------. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca, New York: Cornell University Press, (1992).

----------. "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing," *Canadian Public Administration.* 551-570.

----------. "Playing the Privacy Card," *The Ottawa Citizen* (May 6, 1993).

----------. "Major Flaws in BC Privacy Bill," *Times-Colonist* (April 8, 1993).

----------. "The Information Age: It's time to put privacy on the agenda," *The Ottawa Citizen* (June 21, 1993)

----------. "Quebec sets impressive new standards," *The Ottawa Citizen* (August 6, 1993).

----------. "Progress for Privacy," *The Ottawa Citizen* (January 2, 1994).

Blackman, Joshua D. "A proposal for Federal Legislation Protecting the Information Privacy across the Private Sector," *Santa Clara Computer and High Technology Journal* 9 (1993): 431-469.

Boehmer, Robert G. and Todd S. Palmer. "The 1992 EC Data Protection Proposal: An Examination of its Implications for US Business and US Privacy Law," *American Business Law Journal* 31 (1993): 265-311.

Canadian Direct Marketing Association. *Communicator* (Winter/ Spring 1993).

Canadian Standards Association (CSA). "Proposal for a Model Privacy Code," March 1992.

Cespedes, Frank V. and Jeff H. Smith. "Database Marketing: New Rules for Policy and Practice," 34 *Sloan Management Review* (Summer 1993): 7-22.

The Change Corp. "Doing Business on the Information Highway," *Electronic Commerce Research Project* (1994).

Comeau, Paul-André. "The Protection of Personal Information in the Private Sector: An Important Step Forward by Quebec's National Assembly," Notes for the Sixth Annual Conference of *Privacy, Laws and Business* in Oxford, UK (June 28, 1994).

Commission d'accèss à l'information, "Contact: Advice on the confidentiality of personal information," Québec (Québec): March 1994

----------. *L'accès*, (March 1994), newsletter to the Commission d'accès à l'information.

Davenport, Thomas H. "Saving IT's Soul: Human-centered Information Management," *Harvard Business Review* (March-April 1994): 119-131.

Dobell, Rod and Steven Rosell. "The Information Society: Some Questions Concerning Governance," Proceeding's from the Conference on *Information Technology: Globalization, Diffusion, Innovation and Retraining* (eds.) David W. Conklin and Lucie Deschenes. Toronto: The Institute for Research on Public Policy and the Canadian Workplace Automation Research Center (June 7-8, 1989).

Ekos Research Associates. *Privacy Revealed: The Canadian Privacy Survey.* Ottawa: Ekos Research, 1993.

Equifax Canada. "Consumer and Information Privacy: The Equifax Perspective," Montreal: Equifax Canada, Public Affairs (October 1993).

Fabowalé, Lola. *Voluntary Codes: A Viable Alternative to Government Legislation*? Ottawa: the Public Interest Advocacy Center, May, 1994.

Flaherty, David F. *Protecting Privacy in Surveillance Societies.* Chapel Hill: The University of North Carolina, 1989.

----------. Office of the Information & Privacy Commissioner of British Columbia, *Annual Report 1993-1994.* Victoria, BC.: Queen's Printer, 1994.

Franklin, Ursula. *The Real World of Technology.* CBC Massey Lectures Series. Concord, Ontario: CBC Enterprises, 1990.

Gandy, Oscar J. *The Panoptic Sort: A Political Economy of Personal Information.* Boulder, Colorado: Westview Press, 1994

Garreau, Joel. "The Conspiracy of Heretics," *Wired Magazine* 2 (November 1994): 100-158.

Globensky, Michel C. "Tracking the Future: the Privacy Issue and Information Industry, a Corporate Perspective," Notes for a presentation at the Credit Association of Canada, Ottawa Chapter, May 18th, 1993.

Gokalp, Iskender. "On the Analysis of large technical systems," *Science, Technology and Human Values* 17 (Winter 1992): 57-77.

Goodwin, Cathy. "Privacy: Recognition of a Consumer Right," 10 *Journal of Public Policy and Marketing* (Summer 1991): 149-166.

Government of Canada, Treasury Board. *Powering Up: A Review and Analysis of Information Technology Expenditure Trends in the Canadian Government 1986-1992.*

Hall, Peter. *Governing the Economy : The Politics of State Intervention in Britain and France.* Oxford, UK: Oxford University Press, 1986.

Heilbroner, Robert. *21st Century Capitalism.* Toronto: CBC Massey Lecture Series, 1992.

Hoberg, George. "Environmental Policy: Alternative Styles," in (ed.) Atkinson, *Governing Canada.* (1992).

---------. "The Question of Convergence: Comparison Across Policy Areas," *mimeo* (October 31, 1994).

Information Technology Association of Canada (ITAC), "The Information Industry in Canada: The First National Survey of an Emerging Industry," Toronto: ITAC, (April 1992).

Jones, Mary Gardiner. "Privacy: A Significant Marketing Issue for the 1990s," *Journal of Public Policy and Marketing* 10 (Spring 1991): 133-148.

Laperriere, René and René Côte, Georges A. LeBel , "The Transborder flow of Personal Data from Canada: International and Comparative Law Issues," *Jurimetrics Journal* 32 (Summer 1992)

Lyotard, Jean-Francois. *The Postmodern Condition.* Manchester: University of Manchester Press, 1984.

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

Markoff, John. "The Push for Surveillance Software," *The New York Times* (February 28, 1994: D1).
Marx, Gary T. "Privacy and Technology," Whole *Earth Review* (Winter 1991): 90-95.

McKendry, David. "Business and consumers conflict over privacy", *Canadian Speeches* (May 1992).

Mosco, Vincent. "The political economy of communication: lessons from the founders," in (ed.) Robert Babe, *Information and Communication in Economics.* London: Kulwer Academic Publishers, (1994):

Maurel, Richard P. From the Office of the Privacy Commissioner of Canada. The working paper titled "Québec's Legislation on Privacy Protection in its Private Sector: Analysis."

Nordlinger, Eric. *On the Autonomy of the Democratic State.* Cambridge, Mass.: Harvard Press, 1981.

Organisation for Economic Co-operation and Development (OECD). *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data: Implications for Canada.* Paris: OECD, 1981.

Oman, Ralph. "Reflections on the changing shape of database protection," 40 *Federal Bar News and Journal* (May 1993): 232-239.

National Assembly of Québec, *Charter of Human Rights and Freedoms*, Chapter C-12.

---------. *An act respecting the protection of personal information in the private sector.*

Poster, Mark. *The Mode of Information.* Cambridge, UK: Polity Press

Privacy Commissioner of Canada, *Annual Report 1993-1994*

Raab, Charles D. and Colin J. Bennett. "Protecting Privacy across borders: European policies and prospects," 72 *Public Administration* (Spring 1994): 95-112.

Raab, Charles D. "Data Protection in Britain: Governance and Learning," 6 *Governance* (January 1993): 43-65.

Safire, William. "Peeping Tom Lives," *The New York Times* (January 4, 1993).

Sagasti, Francisco R. "International cooperation in a fractured global order", *Futures* (May 1990).

U.S. Department of Commerce, "Principles for Providing Information" for the Privacy Working Group, National Information Infrastructure Task Force, (1994).

Venne, Michel. *Vie privée & démocratie à l'ère de l'nformatique.* Insitut Québécois de Recherche sur la culture, 1994.

Verba, S. "Comparative political culture," in L. Pye and S. Verba (eds) *Political Culture and Political Development.* Princeton: Princeton University Press, 1965: 512060.

Wallich, Paul. "Trends in Communication: Wired Pirates", *Scientific American* (March 1994): 90-101

Weber, Max. *From Max Weber: Essays in Sociology.* New York: Oxford University Press, 1958.

Westin, Alan F. *Privacy and Freedom.* New York: Athenaeum (1967)

----------. "The Protection of Privacy in the Public and Private Sectors" in Bernard Barber (ed), *Effective Social Science: Eight Cases in Economics, Political Science and Sociology.* New York: Russell Sage Foundation, 1987.

Interviews

Bennett, Colin J.
Professor at the University of Victoria and privacy advocate/consultant. (May 26, 1994)

Clark, Brenda.
President of *Direct Results Marketing.* (September 20, 1994).

Crow, Bob.
Senior Policy analyst for the Information Technology Association of Canada (ITAC). (September 1, 1994).

Dorsey, Peter.
Credit Reporting Bureau, Vancouver BC. (October 24, 1994).

Flaherty, David.
Freedom of Information and Privacy Commissioner of BC. (April 28, 1994).

Foran, Brian
Senior policy analyst, Privacy Commissioner of Canada. (October 12, 1994).

Globensky, Michel.
Vice-President, Equifax Canada. (October 3, 1994).

Hennessey, Michael.
Analyst with the Canadian Radio and Telecommunications Council (CRTC).

Long, Murray.
Senior policy analyst for the STENTOR group. (September 1, 1994).

Péladeau, Pierrot.
Quebec privacy consultant and advocate. (September 1, 18; October

Parker, Micheal.
Cathay Pacific, Marketing Division. (September 19, 1994).

Plamondon, Madeleine. Quebec Consumer Aid Services

Valleé, Marie.
Quebec Consumer Aid Services

Venne, Michel.
Journalist with *Le Devoir* and author.

Zasalack, Eleanor.
Treasury Board Secretariat, Information Security Branch,

Appendix 1:
Safeway's *AirMiles* Application Form

02

Sign up and start collecting.

Yes, I want to join AIR MILES™ and fly free*!
For questions please call **1-800 563-4108.**

Complete this form and mail to: AIR MILES, P.O. Box 1055 - Station B, Toronto, Ontario M5T 3E4. Or drop off at your local Safeway store.

PLEASE PRINT CLEARLY

Mr. ☐ Mrs. ☐ Ms. ☐ Dr. ☐

First name **Middle Initial**

Last name

Address

Apt. #

City

Prov. **Postal code**

Number of people in household

Home Telephone (very important)

Language preference Eng. ☐ Fr. ☐

Business Telephone (optional)

Collect travel miles faster! **Get a supplementary card for another member of your household *free!* (Issued in the name of the principal Collector.)** ☐ ***Yes!*** **Please send me a supplementary card.**

The following information is to help us develop a general profile of AIR MILES Collectors. Answers to the following questions will be kept confidential.

Annual Household Income

Up To $35,000 ☐ **$35,000 to $50,000** ☐ **$50,000 to $75,000** ☐ **over $75,000** ☐

Date of birth (of principal Collector)

D D M M Y Y

By enrolling in the AIR MILES program, you agree to receive activity summaries and other mailings from AIR MILES and its participating Sponsors.

Printed in Canada

"I certify that the above information is correct, and ask that you enroll me as a Collector in the AIR MILES™ Program. I agree to be bound by the Terms and Conditions that you will send me."

In four to six weeks you'll receive your personalized AIR MILES Collector Card and your AIR MILES Collector Guide with full details on collecting AIR MILES travel miles: booking procedures, redemption eligibility, terms and conditions, and all other aspects of the AIR MILES Reward Program.

This brochure prepared for use in Western Canada.
Effective date: 08/25/94 BOM code: 5037427(4/92)

SS-25