HOUSE OF COMMONS
CANADA

# PRIVACY: WHERE DO WE DRAW THE LINE?

## Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities

**The Hon Sheila Finestone,**
**Chair**

**April 1997**


Publications Service

# PRIVACY: WHERE DO WE DRAW THE LINE?

## Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities

The Hon Sheila Finestone,
Chair

April 1997

Transcripts of public Committee meetings may be obtained through the Internet at: http://www.parl.gc.ca.

Available from Public Works and Government Services Canada — Publishing, Ottawa, Canada K1A 0S9

HOUSE OF COMMONS

**Issue No. 5 (Meeting No. 44)**

Tuesday, April 22, 1997

**Chair:** The Hon. Sheila Finestone

CHAMBRE DES COMMUNES

**Fascicule nº 5 (Séance nº 44)**

Le mardi 22 avril 1997

**Présidente:** L'hon. Sheila Finestone

*Minutes of Proceedings of the Standing Committee on*

# Human Rights and the Status of Persons with Disabilities

*Procès-verbaux du Comité permanent des*

# Droits de la personne et de la condition des personnes handicapées

RESPECTING:

Pursuant to Standing Order 108(3), A Study of Privacy Rights and New Technologies

INCLUDING:

The Third Report to the House

CONCERNANT:

Conformément à l'article 108(3) du Règlement, Étude du droit à la vie privée et nouvelles technologies

Y COMPRIS:

Le troisième rapport à la Chambre

Second Session of the Thirty-fifth Parliament, 1996-97

Deuxième session de la trente-cinquième législature, 1996-1997

# STANDING COMMITTEE ON HUMAN RIGHT AND THE STATUS OF PERSONS WITH DISABILITIES

**CHAIR**

Sheila Finestone

**VICE-CHAIRS:**

Andy Scott
Maurice Bernier

**MEMBERS**

Sarkis Assadourian
Jean Augustine
John Godfrey
Deborah Grey
Sharon Hayes
Russell MacLellan
Réal Ménard
Georgette Sheridan

**ASSOCIATE MEMBERS**

Chris Axworthy
Mauril Bélanger
Robert Bertrand
Maud Debien
Audrey McLaughlin
Philippe Paré
Svend J. Robinson
Roseanne Skoke
Myron Thompson

(Quorum 6)

**Clerk of the Committee**

Wayne Cole

# ACKNOWLEDGEMENTS

The Committee wishes to express its gratitude to all those who appeared before it in the course of its study of privacy rights and new technologies. In particular, we would like to extend thanks to all those who participated in the townhall meetings held across the country for their great contribution to our understanding of the impact that new technologies are having on Canadians from coast to coast. The Committee thanks especially all those who acted as facilitators during the townhall meetings, for their logistical assistance, their expertise and for sharing their considerable knowledge with us.

The efforts of the Committee staff, especially in the organization of our cross-country hearings were instrumental to the carrying out of this study. We would like to thank especially the Clerk of the Committee, Wayne Cole, who was ably assisted by Roger Préfontaine. Invaluable assistance was provided by the administrative support staff of the Committees Directorate, notably Fiona Bladon, Elizabeth Fex, France Lewis, Kim Nolet, Karen Titley and Linda Tremblay.

The Committee thanks its research staff from the Library of Parliament, Susan Alter, Nancy Holmes and Bill Young for their dedication and professionalism in assisting the Committee. The Committee especially appreciates their assistance in ensuring that the often complex technologies we examined were never permitted to obscure the fundamental rights issues. The draft report they presented for our consideration aided us greatly in arriving at our final statement in this report.

Valerie Steeves, who worked for us on contract as coordinator of the hearings deserves special thanks. Her work both in identifying and inviting witnesses and in assisting in the running of the townhalls was instrumental to their success. We thank her as well for her assistance in the drafting of this report.

The Committee is grateful to Jean-Yves Durocher for his work as media relations officer and for his assistance with the Montreal townhall.

The Committee thanks the many people on the House of Commons staff who provided services and support, particularly those who made possible the teleconferencing sessions and the broadcasting of our hearings.

We would also like to express our appreciation to CPAC for their generosity in agreeing to televise our cross-country hearings and for the professionalism of the staff who were assigned to that task.

Finally, the Chair wishes to thank her colleagues on the Committee for their dedication and commitment in dealing with these important issues.

# CHAIR'S FORWARD

*"We can only be sure of being free from surveillance today if we retire to our basements, cloak our windows, turn out the lights and remain absolutely quiet" — Gerald La Forest, Justice of the Supreme Court of Canada*

Privacy is one of the most comprehensive of all human rights — broad, ambitious and valued around the world. Traditionally understood as the "right to be left alone," in this technological age, privacy has taken on new dimensions. To experts, privacy is the right to enjoy private space, to conduct private communications, to be free from surveillance and to respect the sanctity of one's body. To the average Canadian, privacy is a question of power — the ability to control one's personal information and to remain anonymous by choice.

Privacy, however, is not an inalienable right. Where do we draw the line? Where is the balance between social and economic needs such as crime and fraud prevention, health services and business practices on the one hand, and the protection of our private lives on the other? These questions have become all the more critical because once lost, our personal privacy can never be recaptured.

As a human right, privacy belongs to everyone. The Members of this Committee have listened to as many voices across this country as possible. Canadians have never approved of peeping Toms or unauthorized wire-tapping, and our criminal laws reflect this. We know now that this same disapproval extends, for example, to hidden video cameras in the workplace, genetic testing for insurance purposes and to citizen identity cards.

The dialogue that we began with the Canadian public forms the crux of this report. I am encouraged to hear that this dialogue continues. For example, Jean Augustine, Member of Parliament for Etobicoke-Lakeshore has carried the process further in her constituency.

I wish to thank all of the members of this Committee for their dedication and hard work. I would also like to give special thanks on their behalf to our Clerk, Wayne Cole, our Researchers from the Library of Parliament, Bill Young, Nancy Holmes and Susan Alter, and our Hearings Coordinator, Valerie Steeves, to whom we are all indebted for their commitment and expertise.

# THE STANDING COMMITTEE ON HUMAN RIGHTS AND THE STATUS OF PERSONS WITH DISABILITIES

has the honour to present its

**THIRD REPORT**

In accordance with Standing Order 108, the Committee has conducted a study of Privacy Rights and New Technologies and agreed to report as follows:

# TABLE OF CONTENTS

# INTRODUCTION

For the last several years, the debate about privacy rights in Canada has gone underground. Experts have discussed it at academic conferences; ethicists have promoted their views before consultative bodies; government officials have dealt with it as a pro forma part of their jobs in meeting the requirements of the *Privacy Act*. The provincial and federal privacy commissioners and their staffs have tried to beat the drum to raise public awareness about current threats to personal privacy and the need to revisit privacy legislation that is in some cases, 15 years old. So far, they have not really been listened to either by the legislators or by the population at large. A thorough public airing of the nature of privacy in Canada is long overdue.

That is the reason for this report.

The history behind it began in June 1996, when the members of the Standing Committee on Human Rights and the Status of Persons with Disabilities were a committee of Parliament in search of a subject for study. Like many Canadians, we were curious about the impact of technologies on the broader elements of human existence. What is the impact of new technologies on human rights?

We called together two panels of eminent Canadians who gave us overviews of the impact of biomedical and information technologies on human rights. What we heard was alarming. The view of Jerry Bickenbach of Queen's University was echoed by the others that "technology isn't extraordinary. What's important and what's difficult are the social and ethical consequences of it."[1] Anne Summers, the former head of the Ontario Medical Society's ethics committee, told us that "our current society is totally unprepared" to debate these issues and to make decisions about new technologies in this context.[2] Everyone who provided their views at these roundtables agreed that education must be the basis for choice in determining how, as a society, we want to treat technology.[3]

After a third group of experts discussed the nature of legislative change, it was obvious that human rights protections are evolving at a snail's pace compared to the rapid advances of

---

1 Standing Committee on Human Rights and the Status of Persons with Disabilities, *Evidence* Meeting No. 13, pp. 24-25. (hereafter cited as *Evidence*, 13:24-25)

2 *Evidence*, 13:24

3 13:27

technology. But as Bill Black of the Law Faculty of UBC told us "the challenge... is not to develop new principles but ... to apply those [existing] principles to new areas".[4]

In one way or another, all these roundtables highlighted threats to privacy and made us uncomfortably aware of new forms of technology that seemed to infringe upon individuals' personal lives. We also heard of the benefits that technology can bring. For the federal Privacy Commissioner, Bruce Phillips new technologies "have the power to heal, of course, but they also have the power to enslave. You have to ask yourself whether we're converting ploughshares into swords instead of the other way around."[5] Until the present, however, most privacy initiatives in Canada have revolved around the need to ensure protection of personal information gathered by the public and private sectors. And even this has not kept pace with the times — or the technology.

We felt it was time to broaden the privacy debate beyond this narrow concept of data protection, and explore the role of privacy as a human right and social value. Marcia Rioux of the Roeher Institute summed it up as "a question of ethics, values, standards and principles that one would want to maintain at a national level, at a provincial level, and indeed at an international level."[6] As members of the parliamentary committee responsible for human rights, we strongly believe in the value of discussing privacy in the languge of human rights. We know that this is of critical importance since the language of debate influences the definition of the issues, the policy options, and the decisions for future directions.

We have spent the last 10 months exploring the changing face of privacy. First of all, we asked privacy experts to enlighten us on the state of the debate and the nature of emerging issues. They told us in no uncertain terms that privacy is, indeed both a fundamental human right and a broad assertion of personal freedom. No invasion of this right should occur unless there is overwhelming proof of its necessity. And yet, they observed, privacy is not an absolute right although it remains a core human value, it must also constantly weigh in the balance with competing rights and interests.

Our sense of urgency grew when we began to look at how our emerging technological society is striking that balance. We learned more about the data trails created by new forms of electronic commerce, new surveillance technologies capable of recording conversations through walls, seeing around corners or in the dark and the implications of decoding that most personal source of information, the individual human genome. No doubt new technologies offer valuable advantages, efficiencies and conveniences. But

---

4 *Evidence*, 24:12

5 24:15

6 24:20

must the benefits of these new technologies come with a privacy price tag? Where do we draw the line?

This is why we decided, as a committee of Parliament, that we had to get a sense of what today's citizens think about privacy. This is why we decided to travel across the country and to invite as many voices as we could to join us in our dialogue. We contacted individuals representing the broadest possible cross-section of society: human rights and privacy commissions, advocates, bankers and executives from business, insurance and Crown corporations, people with disabilities, educators, public servants, health care professionals, labour activists, lawyers, media professionals and multicultural organizations, police forces, technology firms, telecommunications and cable companies and students. We asked them to give us their views.

While it is important to remember that processes are only a means to an end, this Committee learned a lot from the very model that we used for our consultations. We cast aside the traditional Committee format where witnesses present briefs and answer questions. Instead, we invited our participants to join us in small, informal group discussions led by experts. The members of the Standing Committee later summarized the groups' findings in an open townhall meeting.

To focus the debate and to identify the social and personal impact of technology in the context of privacy and human rights issues, everyone, as a basis for discussion, used case studies that attempted to illustrate the benefits and detriments of three technologies on peoples' lives.[7] We chose advanced video surveillance, genetic testing and smart cards as examples of technologies on the cutting-edge where real choices will soon have to be made.

Everyone, including members of the Committee, participated fully and freely during these meetings. This created a dynamic environment that encouraged debate and the exploration of differences of opinion. The greatest benefit of the process was the opportunity for people to participate in an informed discussion about important public policy issues. We finished our townhall meetings with the feeling that we had experienced a valuable educational opportunity as legislators that we hope was shared by people who met with us.

Those who attended our townhalls lost no time in setting out their value systems, their ethical priorities and dilemmas and in asking and debating the critical questions: Do Canadians value their right to privacy? Do they believe that privacy is in jeopardy? How far is too far when it comes to trading off the benefits of new — or old — technologies for our sense of personal privacy? In short, is privacy an inalienable right — or a token that can be bartered for social and economic benefits?

---

7 The case studies, as well as backgrounders on the three issues are contained in Appendix I.

While we know that we could never capture the thoughtfulness and eloquence of our participants in this report, we have used their ideas as its core and the foundation for its conclusions. They provided us with a way to formulate an ethical and legislative framework that can enable Canada to navigate the waters of technological change in a manner that is consistent with the most deeply held values of our society.

# CHAPTER 1: PRIVACY MATTERS: RIGHTS, VALUES AND ATTITUDES

> *I've said before that you can have a perfect society and perfect order and perfect control if that is what you want, but what you give up is any vestige of your rights as a free, autonomous, unique human being. We really have to take a hard look at how far we're going to go ...*[1]
>
> *Bruce Phillips, Privacy Commissioner of Canada*

## PRIVACY AS A HUMAN RIGHT AND SOCIAL VALUE

If we were to isolate two concepts that Canadians presented to us as fundamental in our discussions as we travelled across the country, they would be "dignity" and "autonomy". The well-known privacy advocate, Simon Davies, pointed out to us that privacy is central to both these qualities.[2] Bruce Phillips, the Privacy Commissioner of Canada put it another way. "The thing that animates decent societies," he said:

> is observance of the principle of fairness: that we treat each other with a reasonable degree of respect and are not going around behind each other's backs with little pieces of information that we can use against each other. That is not the kind of open, transparent, candid society we want to build.[3]

The Canadians we spoke with were clearly committed to building this kind of candid and open society, and argued that privacy, as a core human right, remains essential to the workings of a healthy, meaningful democracy. In the words of Darrell Evans:

> I think privacy has to be seen as a basic human right. To me, privacy is an essential part of human freedom. Reading through the case studies, the picture I got was that what freedom is there in a society where those kinds of scenarios can play out?[4]

Many considered privacy as the most fundamental of human rights because its existence encourages us to make use of other rights. Committee member John Godfrey in reporting on the discussions in Montreal summarized the discussion in this way:

---

1 Standing Committee on Human Rights and the Status of Persons with Disabilities, *Evidence*, Meeting No. 24, p. 5 [Hereinafter cited as *Evidence*, 24:5]

2 *Evidence*, 22:14

3 24:17

4 34:16

> Privacy is not a free-standing right but it is often associated with other more established rights, as a sort of associated or pre-conditional right. The right to free assembly can be chilled or damaged by excessive knowledge about you, say through video surveillance. If you know that there are going to be cameras picking you out as an individual, depriving you of your anonymity, that might reduce your inclination to assemble, or indeed, your inclination toward free speech.[5]

Certainly, many speakers at the townhall meetings agreed that any debate about privacy highlights the clash between individual protections and societal protections.[6] But at a more fundamental level, Canadians see privacy seen not just as an individual right, but as part of our social or collective value system.[7] As we struggled with the impact of new technologies on our understanding of privacy, we realized that, ultimately, we were talking about what kind of society we want for our future.[8] Canadians view privacy as far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others — either with trust, openness and a sense of freedom, or with distrust, fear and a sense of insecurity. In the words of Committee Vice-Chair Andy Scott, the participants felt that:

> Ultimately, this isn't a technical question. Ultimately, this is a question of fundamental values. . . I believe that our obligation as legislators is to somehow reach into the collective wisdom of the country and citizenry and find out what it is that people believe their laws should reflect.[9]

The concept of privacy in today's high tech world has taken on a broader multitude of dimensions than ever before. To some, it is the right to enjoy private space; to others, it is the right to conduct private communications, to be free from surveillance or to respect the sanctity of one's body. However it is defined, privacy, in the words of Committee Chair Sheila Finestone:

> . . . is a core human value that goes to the very heart of preserving human dignity and autonomy. It is a precious resource because once lost, whether intentionally or inadvertently, it can never be recaptured.[10]

As we conducted our townhalls, we found — unsurprisingly — that privacy is reflected through many lenses. What emerges is a consensus which consists of a rainbow

---

5 *Evidence,* 38:21

6 37:26

7 38:26-27, 30-31, 52

8 33:27-28, 40

9 38:55

10 33:3

of values, interests, knowledge and experiences. Nonetheless, we could not but be amazed by the degree of consensus that emerged in each of our meetings. Union members shared a common concern with their managers; workers in the private sector could make common cause with their public sector colleagues; genetic researchers agreed with advocates — they all believe that privacy matters.

## PRIVACY: PARADISE LOST?

Many of Canadians' fundamental values — including privacy — are undergoing challenges from the profound socio-economic changes that result from the use of new technologies. In many ways, what separates the privacy debate of today from that of 15 years ago is what several participants in our townhall meetings called our obsession with risk reduction and certainty. The benefits of new technologies are often defined by the economic efficiencies that they introduce. Clearly, there are also societal benefits in reducing street crime, fraud and illness. But too often the debate ends there.

In our quest to reduce risk and make society more predictable, we have, as David Lyon argued, "ignored human rights in the most profound sense".[11] Just as introducing video surveillance in shopping malls fails to reduce crime, but merely moves it to other places,[12] our obsession with risk management leads us to create categories of people which may or may not accurately describe who they, in fact, are.[13] For example, our desire to control public funds may lead us to categorize all recipients of social benefits as potential perpetrators of fraud. The possibilities for discrimination based on these categories will have profound implications for the type of society we are building for the future.[14] As Committee member Jean Augustine concluded, "We talked about this being the slippery slope, and the need for guidelines and protocols"[15] to ensure that the most vulnerable members of our society are not the first victims of the loss of privacy.

Many participants in our meetings also expressed concern about a widespread sense of defeatism and technological determinism, where our collective destiny is perceived to be determined by the kinds of technology we are capable of.[16] As Committee member Sharon Hayes reported, participants felt that we will be unable to find the appropriate

---

11 *Evidence,* 33:20

12 27:21

13 33:27

14 33:32

15 37:12

16 34:30; 37:4, 20, 38; 33:15

balance if we "continue to allow technology to be the tail that wags the dog."[17] We should, they argued, take control of the process, and determine not only what we can do with these new technologies but what we should do.[18]

In many ways, the "soul of the issue", as Kate White reported, "seems to be one of trust". Who do we trust to know things about us and take our privacy concerns into account?[19] General discomfort, both from a consumer's and an employee's point of view, greeted the idea to leave these issues to the private sector.[20] On the other hand, many placed their trust in the government to advocate for the best interests of society.[21] But this trust was far from blind. As Marnie McCall reported, the Consumers' Association first made a recommendation regarding privacy protection to the federal government in 1973.[22] Ken Rubin, an Ottawa privacy advocate, first made a submission on privacy to a parliamentary committee in 1982.[23] And Evert Hoogers told us that his union has been asking for the prohibition of employee monitoring in the workplace for the past 15 years.[24]

As much as we found a sense of cautious optimism that it was not too late to protect our privacy, we encountered a clear sense of urgency.[25] People across the country called on the government to act now, or to risk losing the trust citizens have traditionally placed in our legislators to balance our social good with economic and political goals.

### *A. Privacy, Power and Community*

This sense of balance formed a recurring theme in our discussions. Canadians do not see privacy in isolation or as merely an individual right but as part of the fabric which holds our society together. David Lyon summed it up as a belief:

> that we live in a participatory democracy where mutual trust is assured because we deal with each other as people who have disclosed things to each other within those

---

17 *Evidence,* 34:17, 20

18 33:26

19 33:13, 23

20 37:23

21 33:43

22 33:45

23 33:45

24 33:42

25 33:15, 17, 24, 28, 45; 37:22

> relationships of trust... and that's why it's quite different from a residual question of privacy. It's a social question.[26]

Accordingly, many of our townhall participants tied issues of privacy to questions of power and community.

People feared that attitudes toward privacy issues reflect a legacy of fatalism that George Orwell expressed in his discussion of Big Brother in the novel *1984*. We often feel powerless when confronted by new privacy problems and feel that the situation is beyond any control that we might exercise as individuals.[27] In Simon Davies' assessment:

> The public perception is, — well they know everything anyway; there's no hope; anything I do can ultimately be traced. It's almost as if there's this resignation... that there's nothing you can do. So people tend to opt out completely and just say they'll accept that privacy rights have been eliminated.[28]

Opinion polls tell us that this sense of powerlessness is strongest among people who are poorly educated and those who believe that their personal information has been used in a way that invaded their privacy.[29] Our townhall participants felt strongly that the communities least able to resist invasions of privacy, such as people requiring social assistance[30] or those who are functionally illiterate[31], suffer the first hits by the adoption of new invasive technologies.

We heard many stories illustrating the potential repercussions of this vulnerability. For example, the numerical order of figures on the Social Insurance Card indicates where the card was issued and whether the card holder was an immigrant to Canada. This information, in turn, leads to potential for discrimination by the government and by the private sector.[32] In Fredericton, we heard of two pregnant women who faced the possibility of delivering children with disabilities. When they refused to undergo genetic fetal testing, it was strongly recommended that they submit to psychiatric evaluation.[33] In Calgary, we discussed the frightening prospect of eugenics and the removal of classes of people from

---

26 *Evidence,* 33:40

27 *Evidence,* 37:14. David Townsend, for example, argued that it is unlikely that individuals will be able to negotiate their own privacy protections in a technological world.

28 *Evidence,* 22:22; 22:13

29 *Privacy Revealed*, p. 4ff. According to this survey, 60% of Canadians feel they have less privacy than they did a decade ago and 40% deel strongly that their privacy has eroded.

30 *Evidence,* 33:15

31 37:21

32 39:15-16

33 37:18

society through selective abortion.[34] And in Fredericton, we faced the spectre that discrimination against persons with disabilities that is based on economically-driven, private sector decisions will only grow with greater access to genetic information.[35] To ensure an end to this type of discrimination, participants called for governments act immediately to provide vulnerable communities with special protections.

We also need to eliminate the possibility that our sense of responsible citizenship and our 'community-midedness' might be undermined by the false impression that technology is taking care of things. For example, witnesses to an accident could come to rely on a video camera recording the relevant details and feel that they had no obligation to report what they had seen. Instead, they would rely on the anonymous person who views the video recording to do the job that a citizen ought to have done.[36]

The tools we use to protect privacy must be developed within a social context that protects our sense of community. Once again, the privacy prism requires us to evaluate our underlying goals as a society and to take responsibility for the consequences of new technologies.

### *B. Privacy as a Commodity*

As Randy Dickinson pointed out, the use of technology not only affects individuals; it also has an impact on the commercial activity of the community as a whole.[37] Many townhall participants feared that privacy has become a commodity that people are prepared to trade off for either a better level of service or product or the minimization of penalties.[38] Paul-André Comeau, the Privacy Commissioner of Quebec, warned against a debate about privacy that focused solely on the commercial value of information. This was, he said, "the slippery slope we are lured onto by the new technologies in their attempt at putting a dollar figure to each piece of information."[39]

In large part, this issue grows out of what we earlier called an obsession with risk management by those who administer programmes that involve entitlements or benefits.

---

34 *Evidence*, 35:27

35 37:34

36 38:11

37 37:33

38 22:13

39 21:22

But there is also a growing commercial imperative which makes these questions increasingly problematic.[40] M. Comeau also told us that :

> It is dangerous and, at any rate, it could be very harmful for Canadians to see a debate focusing solely on the commercial value of information pertaining to privacy. Of course this information does have a commercial value, but it is first and foremost a question of basic rights.[41]

Many people at our townhalls feared that those who want to violate privacy for their own economic gain exercise too much influence over the nature of privacy legislation[42]. They argued that we will not find the appropriate balance between privacy rights and efficiency if the process of regulating privacy continues to be driven solely by economic and administrative interests. They were concerned that, left to its own devices, private industry will make choices that affect privacy based on self interest rather than the public good.[43] Indeed, the perceived threat to privacy seemed greatest from the private sector[44], particularly as the government hands over many of its traditional activities.[45]

This commericalization of privacy was tied to the question of ownership. As Jean Augustine reported:

> Over and over again, I got the message that people were looking for... some strong indication, guideline, policy direction, some way in which we can control who owns information . . and [assert] the individual's right to the ownership of the information.[46]

Participants argued that Canada lacks clear principles and guidelines about who owns information and who can use that information for economic or commercial gain. If individuals own information about themselves, then the ability to consent to sharing that information is an essential part of ensuring that the individual retains control over his or her privacy.

## MEANINGFUL CONSENT

Generally, people saw consent as a primary tool to protect privacy from technological invasion. But participants distinguished between 'token consent' and 'meaningful

---

40 *Evidence,* 33:27

41 21:22

42 36:16

43 33:41

44 37:16, 23

45 33:45; 39:41

46 38:69

consent'. They feared that informed consent becomes an empty concept when people do not know how information about them is being collected[47], or are forced into giving consent in order to get something.[48]

In many cases, these fears are justified. In order to get or to keep a job, employees will accept serious invasions of their personal privacy and feel powerless to object. For example, if someone cannot get a job without undergoing a particular genetic or drug test, that person does not have a free choice. The same principle governs those who apply for insurance coverage. As Margaret Somerville pointed out, there is a difference between "mandatory" testing and "compulsory" testing. Compulsory testing creates a firm requirement to take the test, as for example, when it is a condition of continued employment. Mandatory testing has the appearance of being voluntary because one's consent to the testing is required. However, as refusal of consent will lead to denial of services or benefits, the test becomes, in reality, quasi-compulsory.[49]

Over and over, we heard that this lack of meaningful consent was an issue of prime concern to the participants in our consultations. Again, the issue of balance was raised. Instinctively or knowledgeably, Canadians organize information about themselves in a hierarchy. To illustrate: People consider privacy to be a right but also recognize that in order to participate fully in society, as citizens or as consumers, they must allow others access to and the use of certain types of personal information. They know that information must be exchanged and that emerging technologies can facilitate personal and social interaction that benefits everyone. At the same time, most people want to see technology used under controlled conditions with considerable sensitivity to the human rights aspects of its use.[50] In other words, we are seeing the emergence of a demand for "informational self-determination."[51]

Each and every one of us is accustomed to requests for, and to providing, certain information about ourselves. Under normal circumstances, we are not particularly sensitive about giving our names or our ages. But we are increasingly cautious about

---

47 *Evidence,* 33:28

48 33:25; 34:16; 36:20; 37:16, 21

49 28:18

50 21:21

51 21:4

providing home telephone numbers, buying habits and especially financial or health information.[52]

Many people approve of advanced technologies, especially when they are applied to obtain such community benefits as crime control. In some circumstances, individuals appear to implicitly enter into a voluntary contract by consenting to abridgement of certain privacy rights in return for certain benefits. The problem arises when this contract is extended by those who collect and control information to other things which most people consider to be absolutely private.[53] In Margaret Somerville's view "We've got to get over the technological imperative... "have technology, must use' ". The issue in the minds of most of those who spoke to us was "How do we decide which technology to use when?".[54]

Experts have expressed concern that privacy interests are at worst, ignored, and at best, not given sufficient weight in determining the balance between privacy and security or privacy and economic interests. As Marc Rotenberg pointed out "because there are one or two instances where the technology has aided in public safety, there's little basis [of support] in restraining or slowing the deployment of the technology."[55] But such instances do not vitiate the need to safeguard privacy and individual ownership of personal information. We must control the use of personal information through the concept of real and meaningful consent, freely given by an individual who has the power to say no without suffering any adverse consequences.[56]

## PRIMARY AND SECONDARY USES OF PERSONAL INFORMATION

The primary use of technology refers to the purpose for which the technology was developed and/or installed. For example, the primary use of video cameras installed on a main street is to protect the public from crime. Secondary use is a term used to describe what happens when the information collected by the technology is used for purposes other than those envisioned by the developers. The example used in the case studies involved a recording made by a main street video camera of a man attempting suicide in his car. The video enabled the police to call 911 and save the man's life, which was in keeping with the primary use of public safety. However, the video was then sold to the media. The sale did

---

52 The 1992 survey showed that information about age caused extreme concern from 8.5% of those who responded. Home phone and name concerned about 24% while 30% worried about buying habits and 44.6% were extremely concerned about financial information. *Evidence,* 30:4

53 *Evidence,* 36:12

54 28:17

55 22:19

56 33:25; 37:16, 21

not promote public safety. Rather, it was a secondary use of the recording, clearly outside the primary purpose for which the tape was made.

Another theme which was raised throughout the consultation process was the need to restrict or control the uses made of personal information. Participants felt that it was crucial to look at the purpose for which information is collected when determining which uses are or are not appropriate. Many feared that much information being gathered is, indeed, being collected without a specific purpose, and that this should not be tolerated. In addition, they argued that it is essential to test our assumption about the usefulness of the technologies we use to collect information. For example, replacing guards in Ontario jails with video cameras may have cut expenses, by reducing the cost of prisoner surveillance, but it caused a number of other problems in the prison community which far outweighed the initial savings.[57]

In addition, participants wanted controls over the use of information once it is collected.[58] For example, the participants at our townhalls universally considered it unacceptable to sell a videotape of an individual attempting to commit suicide in a public place to the media for public broadcast. Not only was this secondary use of the tape distasteful to the townhall participants; it contravened the implicit contract that street surveillance will only be used to promote public safety.

Similarly, a health worker questioned the uses of video cameras and employee access cards in a New Brunswick hospital. The administration claimed that the technology was in place to protect the employees. However, the cameras pointed not at the public (i.e. those entering the hospital) but at the workers, and the access cards were used to record when employees started and ended their work day, even though their collective agreement prohibited punching a time clock.[59]

To avoid these problems, both the primary and secondary uses of information gathered by new — and existing — technologies should somehow reflect the reasonable expectations of the individuals about whom the information is being collected. Moreover, the person or organization seeking to use invasive technologies should be required to establish that the precise nature of the common good that justifies the invasion.[60]

Once again, people called for an appropriate balance. The challenge put by the participants in the townhalls was summarized by John Godfrey in this way:

---

57 *Evidence,* 33:16

58 36:37

59 37:45-46

60 33:18

> Our first task is to balance the rights and needs and convenience and security of society against the less convenient nature of human rights, which are always awkward and always difficult, but just simply fundamental.[61]

## THE FUTURE IS NOW

In order to meet this challenge, we must address the growing gap between the rapidity of technological change and the slow evolution of human rights.[62] The vast majority of participants did not want to turn the clock back, but, rather as Committee member Sarkis Assadourian noted, "to catch up with technology"[63], so we can control and manage it in a way that protects our privacy rights. Randy Dickinson put it this way:

> We're not against technology. We're just very concerned that it's used to benefit the community and protect the citizens, and not allowed to be misused and abused by people who don't share the same ethical standards as the people who are here [at the Fredericton townhall] today.[64]

In many ways, our case studies underlined the fact that new technologies have not necessarily created privacy conundrums. People have always used personal information to make decisions about access to goods and services, or to enforce public standards of behaviour. However, the fact that the technology is now so efficient at gathering this information, brings these problems to a whole new level of privacy invasion.

With regard to the specific technologies that our case studies singled out, we heard a considerable amount of discussion about the risks that must be understood before any informed decision can be made about where the appropriate balance should lie.

### *A. Genetic Testing*

The relationship between privacy and genetic testing caused some soul searching among those who came to our meetings. Margaret Somerville told us that:

> Genetics requires us to rethink, even reimagine, our assumptions, attitudes, values and beliefs... What we are addressing are the most fundamental, wide-ranging

---

61 *Evidence*, 37:16

62 37:15

63 34:29

64 37:35

> values on which our society is based... We are also adressing — and this is what makes it unusual, because you don't often get these in such close relationship — the most individual, intimate, personal, moral issues.[65]

Generally, people agree that genetic technology has very real and personal benefits in terms of providing medical diagnosis and care. However, both privacy advocates and genetic researchers argued that increasing commercial interest in the information will spur on employers and insurers who can, in fact, already gain access to genetic data by obtaining personal medical files. Accordingly, the potential for misuse of this highly sensitive personal information is very real and has already become a problem.[66] In addition, many people base their caveats and cautions expressed to us on their concern that information generated by genetic testing will be misused for purposes that have nothing to do with the medical well-being of the individuals who have undergone the tests.[67] Instead, uses will grow out of the thirst of the state and of the private sector for personal information.

There are legitimate reasons for genetic testing. For example, the United States military tests the DNA of its members so if one is killed, the remains may be identified. But problems arise when authorities use this information for secondary purposes, such as the U.S. military's passing it on to law enforcement agencies. In essence, this permits the police to conduct a search that would otherwise require appropriate and direct legal approval.

In addition, genetic information does not only provide information about an individual but also about his or her blood relatives as Committee Vice-Chair Maurice Bernier reported:

> When someone goes for genetic testing, that person is not the only one concerned by the results. In other words, not only do we gain information on that person but also on that person's total family. People who have never given any consent might be affected by decisions whose origins they don't even know. This is a serious problem that was emphasized and it should be taken into account.[68]

Given the formidable repercussions these types of choices will have on society as a whole, experts and non-experts alike agreed that genetic information "involves a difference

---

65 *Evidence*, 28:16

66 28:9

67 28:3-4

68 34:12

in kind, not just degree".[69] Universally, the Canadians who we met during this study called for special measures to ensure that genetic data is used in ways which are consistent with our underlying values.[70]

### *B. Smart Cards and Biometric Encryption*

The discussion concerning smart cards once again reflected the need to find a balance between convenience and efficiency on the one hand and personal freedom on the other. Smart cards, as opposed to the more common swipe cards used by automated tellers, for instance, contain a computer chip with enough memory to store a great deal of information. The type of information depends on the function of the card. Our townhall participants recognized that smart cards have advantages; they simplify our lives and promote the efficient administration of public and private funds.[71] But at the same time, people called for measures to ensure that we will be protected from inappropriate secondary uses,[72] and that the technology will only be used by those who genuinely consent to it.[73]

Concerns about secondary uses of the information on a card were strongest when it contained health information. For example, the health card experimentally introduced by the Régie de l'assurance-maladie du Québec in the city of Rimouski contained extremely sensitive medical information including personal and family history, test results and medical diagnoses. As Paul-André Comeau said:

> This type of technology obviously raises important questions: can you imagine who could have access to this information? Could, for example, indiscreet eyes see that information, with obviously very serious consequences? For example, what is voluntary pregnancy termination, abortion, was included on the chip and this became known elsewhere? It doesn't take much imagination to foresee the problems this could cause.[74]

The coupling of biometric technology with smart cards raised further concerns about the relationship between the individual and the collective. Biometric technology is based on the collection of data relating to personal characteristics — for instance, fingerprints and handprints. The technology allows that data to be digitized and then encoded on a card or in a database. Institutions such as banks or immigration authorities can then

---

69 *Evidence,* 28:16

70 33:41; 35:25; 36:14, 20

71 28:13

72 36:12

73 34:20

74 21:11

identify an individual by scanning his or her finger or handprint and comparing it with the digitized picture on the card or in the database.

Cards containing digitized handprints are being used, for example, in the CANPASS project. The CANPASS project is a fully automated immigration and passport control system being pioneered by Canada, in conjunction with the United States. Willing individuals allow their handprint to be scanned and encoded on a CANPASS smart card. Immigration and customs officials are then able to use the card to verify the identify of the cardholder when he or she is entering the country. The project aims to replace a substantial number of passports with smart cards in the next 10 years.

As Simon Davies noted, the use of this technology "raises enormous questions of human identity that need to be addressed now".[75] However, the technology can be used either to invade privacy or to protect it. It is important to remember that the information cards can be encrypted in such a way that the cardholder has total control over who accesses it. Through the use of encryption, we can still obtain the benefits of fraud-proof identification without necessarily invading privacy.[76]

### *C. Video Surveillance*

No longer does surveillance technology fall solely within the ability of national security and law enforcement agencies. Users range from banks to corner stores. The technology itself is inexpensive and easy to use, and the security industry that uses it is generally unregulated.[77] Accordingly, we find more and more cameras monitoring our movements — from the bank, to the office, to the corner store.

Participants felt that this constant monitoring of individuals in public and private places is inconsistent with a free society. Many participants discussed the value of keeping our movements private, not because we have things to hide, but because constant monitoring takes away from our sense of autonomy. Recent advances in surveillance technology have exacerbated the problem. Our understanding of private and public spaces is not in keeping with technologies that can listen in on conversations taking place in cars as they drive by, or peer into buildings over a mile away. People agreed that the reach of surveillance technologies should not exceed our reasonable expectations of privacy, and should be balanced against the value of personal freedom.

People were also uncomfortable with the lack of controls over the use of surveillance technology by the private sector. Our laws have evolved to protect us against invasive

---

75 *Evidence*, 22:11

76 29:5

77 37:35-36

surveillance by the state, but the lack of restraints on other organizations was considered unacceptable. Most of the participants were willing to accept some level of surveillance to protect individuals and property from crime. However, they called for strict control over secondary uses of surveillance tapes, and the development of professional standards for the security industry.

People were also shocked to discover that criminal laws prohibiting the interception of private audio communications do not extend to surreptitious video recordings. The band-aid nature of many laws dealing with privacy reinforced the general feeling that we need some sort of comprehensive framework legislation to ensure that the benefits of new technologies do not override our privacy rights without good cause.

## KNOWLEDGE IS POWER

The Canadians we spoke with agreed that the only way to achieve the necessary balance between individual and societal rights is through open communication and dialogue.[78] To initiate that dialogue, however, we must raise the public's awareness of how technology changes our social relationships. In the words of Darrell Evans:

> I think part of the confusion over the privacy debate is that it hasn't been seen as a fundamental one. It's not rooted in a kind of grassroots feeling. We need a definition, or a firmer idea in the public mind, of what privacy really is, what we mean when we say 'privacy'.[79]

The Privacy Commissioner of Canada provided more evidence of the public's need for information when he told us of the growth in the number of public inquiries to the Commission as a result of the exploding nature of the information world and the growth of technology.[80] Again, scientific sampling by surveys reinforces our observations. Sixty-one percent of those who responded to a 1992 survey indicated that they did not really know where to go if they wanted to deal with an invasion of their privacy. Only one in five had any knowledge of legislation, provincial or federal privacy commissions or private means of redress. Only two percent knew about human rights legislation and less than half of one percent about credit bureaus.[81]

As we held our townhall meetings, we also observed that the level of discussion and debate depended on the nature of the privacy protections that were in place. Concerns

---

78 *Evidence*, 37:26

79 34:16

80 24:6

81 *Privacy Revealed*, p. 25ff. The top ten responses regarding legislation or agencies that help Canadians deal with privacy where: 1. Human Rights Legislation; 2. *Access to Information Act*; 3. *Freedom of Information Act*; 4. *Privacy Act*; 5. *Charter of Rights and Freedoms*; 6. Government; 7. Ombudsman; 8. *Consumer Protection Act*; 9. Privacy Commissioner; 10. Credit Bureau.

about privacy were highest and knowledge of means of redress was lowest in provinces where there was the least privacy protection. In provinces where there is provincial privacy legislation and protection in place, both experts and laypeople were more easily prepared to define the issues and relate them to the requirements for the future. This was particularly the case in Quebec, which has the highest level of privacy protection in North America.[82] In many ways, peoples' attitudes toward privacy reflect their perception of their ability to affect their individual circumstances.

We are convinced that governments and the private sector in Canada must raise the public's awareness of how new technologies are changing our relationships, and initiate an ongoing dialogue between Canadians about the underlying values which fall within the rubric of privacy. Our task requires us to candidly examine these basic values and build a consensus about the kind of society we want for the future. Technology will fulfill its promise only if we, as a society, participate in an informed ethical and policy debate about the importance of privacy as a human right and social value.[83] In the words of Maurice Bernier:

> In conclusion, I would just like to say that the point on which everyone particularly focus is the absolute need to sensitize Canadians about the emergence and impact of new technologies, and to ensure that they are continually well-informed. Sensitization and information can be considered the key to successfully introducing any new technology.[84]

The value of dialogue and consensus building was brought home to this Committee throughout the consultation process. Although stakeholders came to the table with very different perspectives, it was clear that there is an underlying consensus about the primary importance of privacy, and the need for strong measures to protect it from technological innovations. As Sheila Finestone concluded:

> Last, but not least, there was the overall, general sense that there should be a philosophic principle that is value-based, and that the legislation that flows from it needs to be strong and not subject to technological change.[85]

## CROSSROADS

We are at a crossroads in terms of defining fundamental human values and principles. If there are no forward-looking protections or at least a consciousness on the part of the

---

82 Again this is borne out by the findings of *Privacy Revealed*, p. 27 which shows that Quebec residents are twice as likely as residents of other provinces to report awareness of privacy-related legislation or agencies (33% compared to less than 15%). See chapter three for a discussion of the Quebec legislation.

83 *Evidence*, 33:27-28

84 38:9

85 36:18

public put in place soon, it is possible that we will have to "kiss privacy good-bye in the next century."[86] In the words of Darrell Evans:

> I think the vanishing of privacy would be a victory of materialism over the human spirit. I find it very hard to picture what kind of room there would be for creativity on the part of human beings in such a world. I feel the virtual bars closing in faster and faster in a world like that. We are constantly told it is a more secure world, of course, a more efficient world, a world that catches fraud much better, but to me, that is the victory of bureaucracy over human creativity. An old phrase comes to mind here, that we know the price of everything and the value of nothing...
>
> What is our goal in all this? What do we seek for individuals in this? We want to put individuals in a place of causation rather than being a complete effect of technologies and of a gradual erosion of our privacy. If we are to maintain human freedom, I think that's what we have to do.[87]

This is the task of this report. However, before we outline our vision for a comprehensive system of privacy protection, it is necessary to first examine the protective frameworks which are currently in place.

---

86 *Evidence*, 21:22

87 34:16-17

# CHAPTER 2: THE PATCHWORK OF PRIVACY PROTECTION

> *Despite our enthusiasm for international efforts to protect privacy, Canada has done too little to legislate against domestic privacy violations. To date . . . only Parliament and [some] provinces . . . have enacted data protection laws. And even these are not true privacy laws because their scope is limited to controlling their respective governments' collection, use and disclosure of personal information. These laws do not regulate the private sector. Nor do they specifically address such privacy issues as electronic surveillance in the workplace, genetic testing or the use of the polygraph as an employment screening tool.*[1]

Trying to understand the privacy protection for individuals in this country is like viewing the world through rose coloured glasses. Perception and reality are two different things.

## THE PERCEPTION

Certainly, "privacy is a right with a grand tradition"[2]. Thus Canadians cannot be faulted for assuming that given the fundamental human value that they place on it, the right to privacy is adequately protected in this country. This is a logical, if not unjustifiable, conclusion.

In the aftermath of the Second World War, human rights issues, including the right to privacy, reached new levels of international consciousness. The horrifying acts that took place in the 1930s and 1940s served as a catalyst for the adoption of a series of international human rights instruments. The Government of Canada took an active role in orchestrating the development of these documents. Indeed, a Canadian, John Humphrey, was one of the architects of the *Universal Declaration of Human Rights*. Adopted by the United Nations in 1948, the *Universal declaration* sets out the basic rights to which all human beings are entitled and has since become a kind of "Magna Carta" of Human Kind.

Article 12 of the *Universal Declaration* explicitly states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." A similar privacy guarantee was repeated in Article 17 of the 1966 *International Covenant on Civil and Political Rights* to which Canada acceded in 1976.

---

1 Privacy Commissioner of Canada, *Entrenching a Constitutional Privacy Protection for Canadians: A submission to the Special Joint Committee on a Renewed Canada,* 1991.

2 *Evidence,* 22:23

The aftermath of the Second World War also had a profound effect on Canadians at home. They naturally assumed that the same vigilance taken by Canada in the international arena, to ensure the preservation of human dignity and individual autonomy, would be applied domestically. At first glance, this appears to have been the case. Human rights are both entrenched in the Constitution and safeguarded in legislation at the federal, provincial and territorial levels. Numerous court decisions have recognised the existence of a constitutional right to privacy under sections 7 and 8 of the *Canadian Charter of Rights and Freedoms.* Today, privacy acts exist federally and in most of the provinces. Some provinces have also passed laws that provide civil remedies through the courts for privacy invasions.

## THE REALITY

Upon closer scrutiny, however, the privacy picture is neither so rosy, nor so complete. Major pieces of the jigsaw puzzle are missing. A comprehensive and interlocking system to ensure and maintain control over our interactions with each other, with commercial enterprises and with the state is far from a reality in Canada.

Privacy protection in this country is clearly skewed in favour of safegarding personal information. While data protection is clearly a critical part of the spectrum of privacy interest, in a world of increasingly intrusive technologies, it is by no means the only game in town. As we discovered through our examination of video monitoring, genetic testing and biometic identification technologies, other privacy interests are at stake here. Privacy is a wide-ranging right that is currently under siege in a number of ways, and yet Canadians and their governments are still fumbling with tools that are not up to meeting the current, let alone the future, challenges of privacy protection.

### *A. Constitutional Privacy Protection*

While Canada has no express constitutional right to privacy, the courts have interpreted sections 7 and 8 of the *Canadian Charter of Rights and Freedoms* as guarding against unreasonable privacy invasions. Section 7 provides for the right to life, liberty and security of the person and the right not to be deprived of these except through some form of due process. Section 8 protects against unreasonable search and seizure. The privacy value in these rights, however, has largely been recognised in the criminal law context, and

it is for this reason, among others, that calls continue to be made for the entrenchment of an explicit and broad right to privacy in the Canadian Constitution.[3]

Even if the Charter accorded special legal status to the right to personal privacy, there would still be some limitations on its reach. Charter rights are by no means absolute. Section 1 of the Charter allows for reasonable limits on any Charter right when those limits can be demonstrably justified in a free and democratic society. In addition, the Charter only applies to the laws and activities of governments. In other words, Charther rights do not apply directly to the private sector.

While no constitutional documents at the provincial level safeguard the right to privacy, the Quebec *Charter of Human Rights and Freedoms* has attained a kind of quasi-constitutional status within that province. It prevails over other provincial laws unless there is express wording to the contrary. Article 5 of the Quebec Charter guarantees every person the right to respect for his or her private life.

### *B. Privacy of Personal Information*

Until our courts began to grapple with the concept under the *Canadian Charter of Rights and Freedoms* in 1982, the right to privacy enjoyed very low public, and for that matter, governmental profile in Canada. It was often lost amidst human rights or access to information legislation. The federal and provincial governments in this country seemed neither concerned about the impact that new technologies, such as the development of the computer, might have on individual privacy interests, nor were they committed to addressing the situation fully.

Although the federal government did enact the *Privacy Act* in 1982 as a means of regulating the collection, use, disclosure and disposal of personal information that is held by the federal government, the legislation only protects data. It has nothing to do with the concept of privacy in its broadest sense. Moreover, while the Act covers all federal government departments and most federal agencies, it does not extend to every Crown corporation or to the federally-regulated private sector. It requires each government institution, with certain exceptions, to record in a central index the nature and extent of personal information under its control. While the Privacy Commissioner is appointed to receive complaints and investigate non-compliance under the Act, the Treasury Board

---

3 There have been numerous attempts to entrench the right to privacy in the Constitution. Proposals were made by the federal government itself to first ministers in 1979 suggesting the inclusion of privacy as an essential right in the *Canadian Charter of Rights and Freedoms.* Throughout the 1981 debates of the Joint Committee on the Constitution, several recommendations were put forward by the Canadian Bar Association to include privacy in the Charter. The Standing Committee on Justice and Solicitor General in its 1987 report **Open and Shut**, which reviewed the federal *Privacy Act*, unanimously recommended a specific consitutional right to privacy. Finally, the Canadian Privacy Commissioner made a strong argument in 1991 for the constitutional enhancement of the right to privacy to the Special Joint Committee on a Renewed Canada.

Secretariat has general responsibility for co-ordination of the implementation of the Act, and the Department of Justice maintains general responsibility for policy implications.

Interestingly, unlike some jurisdictions where freedom of information legislation has been used to subvert informational privacy laws, Canada has recognised the complementary nature of the concept of privacy and access to information. The federal *Access to Information Act* was proclaimed in force at the same time as the federal *Privacy Act* with the result that information of a personal nature held in government institution databanks is to be kept private, whereas information of a non-personal nature held by a public body is to be publicly accessible.

While the Canadian government was taking a hands-off approach to the dawning of a networked world, the European community was responding to what it perceived as a serious threat to a human right of fundamental importance. Realising the huge potential for massive abuses to privacy from computers that no longer stood alone, but could now talk to one another and exchange information, the Council of Europe enacted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* in 1980. The Convention provided member states with a framework pertaining to the collection, use, access, accuracy, and disposal of personal information. Following on the heels of the European Convention, the Organisation for Economic Co-operation and Development (OECD) released *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980. The OECD's objective was to ensure that all international data flows were not completely blocked by protective measures taken nationally. At the same time, the OECD sought to harmonise the data protection practices of member countries by establishing some minimum standards for handling personal information.

In 1984, Canada joined 23 other industrialised countries in adhering to the OECD Guidelines. In fulfillment of its international commitments, Canada has passed information privacy laws adopting the fair information principles contained in the Guidelines. However, it has done so in a rather haphazard manner. Due to the federal nature of this country, with a division of powers between the federal and provincial legislatures, data protection acts have sprouted up at both the federal, and in some cases, the provincial level in varying intervals.[4] Not only has this given a patchy effect to the Canadian privacy garden, but the lack of careful attention to the landscape as a whole has allowed certain weeds to develop. For example, little in the way of any kind of privacy protection exists in the Atlantic provinces. As the result, these so-called "data havens," like weeds, tend to choke the overall growth and sustainability of privacy rights around them.

---

4 The first provincial privacy legislation came from Quebec in 1982. This was followed by the federal *Privacy Act* which came into force in 1983. Ontario introduced legislation which came into force in 1988 and Saskatchewan's data protection law came into force in 1992. British Columbia enacted legislation in 1992, Alberta in 1994 and several other provinces incorporate fair information principles within their access to information laws.

Essentially, federal and provincial data protection laws do adopt the OECD principles for the collection, use, disclosure of and access to information about an identifiable individual. The weaknesses in the Canadian approach, however, lie with the enforcement mechanisms and general scope of this legislation. For example, while most OECD countries have adopted either a licensing (i.e. Sweden, Denmark, Austria) or a registration[5] (i.e. Germany, Japan, Spain) data protection regime, Canada is one of the few that uses a privacy commissioner as its principal mechanism for safeguarding personal information. The approach to data protection in this country has been much more passive and more narrowlly focused than in Europe. Privacy Commissioners essentially investigate complaints about infringements of the Act; however, they are usually limited to moral suasion or using public embarrassment to ensure compliance. The legislation itself is also usually devoid of any real penalty provisions.

Does this limited approach to data protection indicate the level of commitment to privacy protection in this country? What is the reason for the lack of a comprehensive national data protection system in this country? Does the low profile attached to the issue of privacy, or the fact that Canada as a federal state that constitutionally divides legislative powers between the federal and provincial governments, explain why there is a lack of comprehensive national data protection?[6]

At the federal level, the extent to which the Treasury Board Secretariat, the ultimate supervisor of government personal information and a central agency of government, is the actual informational control keeper is worthy of consideration. From what we could tell, all Treasury Board does is issue data protection guidelines that accord with the *Privacy Act*. It appears to do little else. It does not even follow up on the implementation of their guidelines by monitoring departmental compliance. If it is, the next question is to what extent is its privacy protection agenda politically driven, and how transparent is this process?

Interestingly in choosing the commission approach to privacy protection, the Canadian government was well aware of the data protection regimes chosen by its European counterparts. Canada also recognised that the option existed for the use of an information auditor as a method of securing legislative compliance. We cannot help but ask why Canada seems to consistantly have taken a passive approach to such a critical issue as privacy protection? One wonders about the influence that our neighbour to the south has had on the Canadian decision-making process, for the United States has long downplayed the importance of an independent and proactive data protection regime.

---

5 Basically, personal information is protected by requiring data users to record the details of their activities in a public register. For more information on these systems see Ian Lawson, *Privacy and the Information Highway : Regulatory Options for Canada*, A Study Prepared for Industry Canada, 1995.

6 David Flaherty, *Protecting Privacy in Surveillance Societies,* University of North Carolina Press, 1989, p. 246.

In terms of the scope of our data protection laws, the patchwork effect is perpetuated. While the vast majority of countries in the OECD have enacted data protection legislation that extends to both the private and public sectors, Canadian laws, with the sole exception of Quebec, apply only to the actions of governments and government agencies.

Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*, which came into force in 1994, applies the principles of the OECD Guidelines to all personal information, whatever its form and in whatever medium that it is collected, held, used or distributed by another person, confined mainly to enterprises engaged in an "organised economic activity." It provides a detailed framework for implementing the Quebec *Civil Code's* provisions pertaining to the collection, use and disclosure of personal information. It has been heralded as the first comprehensive regulation of private sector personal data practices in North America and so far, the feared negative impact on Quebec business has not materialized.

While the extension of data protection to the private sector in Quebec has been a positive move within that province, data protection outside of Quebec is considerably weak in comparison. The implications are, for example, that consumers in Quebec enjoy greater privacy protection than their fellow Canadians who reside elsewhere, and businesses everywhere are burdened with the costs and inconveniences of trying to figure out and ensure compliance with a patchwork of information privacy requirements across the country.

Moreover, the private sector vacuum that exists outside of the province of Quebec has, in the spirit of patchwork solidarity, developed in a rather piecemeal fashion. Specific types of data protection legislation has developed, but only in response to limited needs that arose, for example, in the consumer credit and telecommunications sector.[7] Moreove while the federal government, in 1986, attempted to comply with its commitment under the OECD Guidelines by encouraging all private sector corporations to develop and implement voluntary privacy protection codes, this approach has met with very little success.

Self-regulating codes of fair information practices have emerged on a sectoral basis, in most cases, along the lines of the OECD Guidelines. Most of these "privacy" codes are company, industry or industry association-based. For example, the Canadian Bankers Association's model code guides individual banks in establishing their own privacy guidelines. In the insurance sector, the Canadian Life and Health Insurance Association

---

7 In the late 1970s and early 1980s, some provinces enacted legislation that allowed consumers a right of access and the ability to make corrections to their credit information. Controls were also imposed on the collection, retention and disclosure of credit reports. The Canadian Radio-Television and Telecommunications Commission has recently been given a mandate to respond to the economic and social requirements of users of telecommunications services, including the protection of privacy of individuals. See s. 7(i) of the *Telecommunications Act*.

set out *Right to Privacy Guidelines* and the Insurance Bureau of Canada has adopted its own *Model Privacy Code*. The Canadian Cable Television Standards Council incorporated privacy principles into its *Customer Service Standards* and the Canadian Direct Marketing Association (CDMA) implemented a compulsory code of informational practice in 1993 for its members. Unfortunately, the CDMA could not force non-members, usually the worst offenders, to apply its code to their activities. It has, therefore, taken the unprecedented step, as an industry association, of calling on government to take legislative action in the private sector.

While we applaud these individual initiatives, we believe that Canadians should not become too complacent in their belief that all our privacy interests have been duly considered and safeguarded. Perhaps Colin Bennet best sums up the overall problem when he recently wrote that:

> Privacy codes of practice operate within a complicated and fluctuating set of political, organisational, cultural, technological and economic incentives that vary between and even within business sectors. The entirely voluntary approach always suffers from the perception that the individual's privacy rights are in the hands of those who have the most to gain from the processing of personal data.[8]

Even more disconcerting to this Committee is the fact that much more is at stake here than simply a lack of domestic co-ordination. In 1998, the European Union (EU) will require all member countries to adopt or adapt national data protection laws that comply with the Union's *Directive on Data Protection*. Significantly, in terms of non-member countries, such as Canada, Article 25 prohibits member countries (and businesses within those countries) from transferring personal information to non-members of the EU if that country's laws do not adequately guarantee protection of that information. With the exception of Quebec, Canada will not meet this standard unless appropriate action is taken.

A bright light on the horizon is the Canadian Standards Association's *Model Code for the Protection of Personal Information* that was published in March 1996. A committee of consumer, business, government and labour representatives developed the Code in response to the lack of national data protection standards, particularly in view of the European Union's Directive. Devised under the auspices of the Canadian Standards Association (CSA), the Code sets out privacy protection principles in 10 key areas, including the consent for the collection, use, or disclosure of personal information. These principles have now been approved as a national standard by the Standards Council of Canada.

The Achilles heel of the CSA Model Code system, however, is the fact that to date no enforcement mechanism is in place to ensure compliance with these principles. Some

---

8 "Rules of the road and level-playing fields: The politics of data protection in Canada's private sector", *International Review of Administrative Sciences*, Vol. 62 (December 1996), p. 481-2.

critics even contend that a consensual approach to developing a national standard entails too much compromise, waters down the regulatory regime and therefore is perhaps not desirable when our privacy interests are on the line. Finally, there is the argument that it could prove difficult to keep a set of national standards current or subject to regular review, in a non-legislative regulatory regime.[9]

### C. *Safeguarding the Rest of Our Private Lives*

Other than data protection, privacy protection mechanisms have emerged, if at all, in response to particular interests in specific contexts (e.g., the *Criminal Code*). Not only have these ad hoc developments contributed to the patchwork nature of privacy protection in this country, they have also tended to suffer from a general inability to deal effectively with emerging technologies and tactics.[10]

Just to illustrate the ad hoc way in which the protection of personal privacy has developed, Part VI of the *Criminal Code* currently creates a comprehensive legislative scheme for the invasion of privacy involving the interception of private communications. For example, it is an offence, punishable by up to five years, for anyone to wilfully intercept private communications through the use of a technical device (i.e. "wiretapping" or "bugging" ) without the consent of one of the parties or a warrant. Ironically, there is no such prohibition against secretly taking photographs or videotapes that have no voice recordings. Moreover, only the police need obtain a warrant to surreptitiously videotape people's private activities. No prior authorisation is required for ordinary citizens, such as security guards.

In a similar vein, the rules governing the confidentiality of health records vary according to the actual location of an individual's medical file. For instance, the relevant provincial data protection legislation, if it exists, would apply if the file is located in a hospital. Such protection would not, however, extend to a file with the same information in a doctor's office.

## FROM PATCHWORK TO OVERARCHING PROTECTION

Clearly, Canadians are left with privacy protection that is far from comforting. In reality, Canada has an inconsistent, incomplete and incoherent set of laws, regulations, voluntary codes of practice and policy guidelines pertaining to privacy that add up to a patchwork.

This hodge podge is due in part to the division of legislative powers between the federal and provincial governments, neither of which has exclusive authority over privacy,

---

9 Lawson, p. 34.

10 Lawson, *Privacy and Free Enterprise: Legal Protection of Personal Information in the Private Sector*, prepared for the Public Interest Advocacy Centre, August 1992, p. 526

and the lack of an unequivocal constitutional right to personal privacy in its broadest sense. It also stems in large part from the fact that commercially-driven thirsts for personal information and resultant consumer concerns about "dataveillance" have served to conceptualize privacy in this country as being only about informational privacy.

This Committee believes that what is therefore needed is overarching legislation that would serve as a privacy protection umbrella under which all Canadians, in all circumstances, can seek shelter.

# CHAPTER 3: THE HEART OF THE MATTER: CORE PRIVACY PRINCIPLES

As we outlined in the first chapter, the consistency of viewpoints and degree of consensus among the townhall participants, who represented diverse interests, was quite remarkable. Indeed throughout the entire study process, as the Committee polled the public and canvassed expert witnesses on their views, we found many of the same values and principles were expressed time and time again. The repetition in the dialogue, however, was reassuring rather than tedious. It signalled to us that at the heart of privacy matters, certain principles, which are truly fundamental, are clustered. These principles constitute the core or the ethical foundation upon which we, as a society, must build the systems required to protect privacy.

This chapter presents the Committee's blueprint for this ethical foundation. We are not architects or expert draftspersons; we leave the job of finalizing the blueprint to those who are. But, based on the insightful and impassioned interventions of the witnesses, mindful of the literature we have reviewed and the theories we have tested along the way, we wanted at least to attempt to sketch the foundation — the principles upon which everything else will be built. Before we do so, however, we wish to say a few words about the context or the environment in which this design was shaped.

## ADOPTING THE LANGUAGE OF HUMAN RIGHTS

From the outset of this Committee's study, as the introductory passages of this report attest, one of our main objectives has been to consider privacy issues from a human rights perspective. Why was it critical to approach this study from that perspective? Because experience has shown us that the way you ask the question will often determine the type of response you get. Thus, if we approach privacy issues from a human rights perspective, the principles and solutions we arrive at will be rights-affirming, people-based, humanitarian ones. On the other hand, if we adopt a market-based or economic approach, the solutions will reflect a different philosophy, one that puts profit margins and efficiency before people, and may not first and foremost serve the common good.

Ursula Franklin, Professor Emeritus, University of Toronto, addressed this dichotomy in September 1996, speaking at a conference of privacy commissioners from around the world:

> When human rights informs the language in which the discussion among you and the general public and Parliament takes place, you speak then, rightfully about *citizens* and all that comes with that. On the other hand, if the emphasis is primarily on the

> protection of *data*, one does look at a market model, one does look at an economic model, and all the things you've heard about the new economy. Then it is the language of the market that informs your discourse. ( . . . ) When those who primarily locate themselves in the human rights climate speak about citizens, about the relationship between groups and power, those who are in the market language speak primarily about stakeholders. And when one speaks about rights and obligations, others speak about binding contracts.[1]

## THE HEART OF PRIVACY PROTECTION

Having deliberately taken a human rights approach to its study, the Committee naturally chose also to describe the core principles it identified along the way by adopting the language of human rights, that is, by using a vocabulary that speaks in terms of rights and obligations. These core principles cover the full spectrum of privacy, not simply the field of data protection. They are not solitary, free-standing principles, but are interdependent — overlapping and intertwining, like threads in a tapestry. Furthermore, they do not comprise a closed or finite list. We hope and expect that the list will evolve with time, experience and further public input.

We have tried to limit the core principles to those we found, throughout the study process, to be so fundamental, so basic that they had to be part of the ethical foundation being designed. From this base, additional or second-generation principles can be developed. The core principles are first-generation principles, intended to be a benchmark against which to assess the fairness of governments' and businesses' practices and the adequacy of legislation or other protective measures. They are very general statements of everyone's fundamental privacy rights and obligations and, as such, are designed only to serve as a foundation, nothing more. They form the heart of what we propose in the next chapter should be overarching legislation for protecting privacy rights in Canada — a sort of bill of rights for privacy or a Canadian Charter of Privacy Rights.

## OUR BLUEPRINT FOR THE CORE PRINCIPLES

In the remainder of this chapter, we describe the core principles in a series of statements about rights and obligations. The inspiration for these principles comes from a variety of valuable sources, but mainly the following three: the people who participated in

---

1 Ursula Franklin, *Stormy Weather: Conflicting Forces in the Information Society*, Closing Address at the 18th International Privacy and Data Protection Conference, Ottawa, 19 September 1996 (emphasis added).

our hearings and townhall discussions; the Australian Privacy Charter,[2] which is the first statement we have seen of broad privacy principles as opposed to only data protection principles; and, last but not least, Canada's own CSA *Model Code for the Protection of Personal Information*, which though it only provides data protection principles is a good prototype as far as it goes. The core principles begin with (1) a list of fundamental privacy rights and guarantees, followed by (2) the justification for exceptions, (3) a list of general obligations attaching to the fundamental rights and, finally, they are rounded out with (4) specific rights associated with informational privacy and (5) obligations attaching to these specific rights. In other words, our proposed ethical framework is made up of five parts. Each part, set out below, is followed by comments and observations of the Committee.

### *1. Fundamental Privacy Rights and Guarantees*

**1.1. Everyone is entitled to expect and enjoy:**

- **physical privacy;**
- **privacy of personal information;**
- **freedom from surveillance;**
- **privacy of personal communications;**
- **privacy of personal space.**

**1.2 Everyone is guaranteed that:**

- **these privacy rights will be respected by others adopting whatever protective measures are most appropriate to do so;**
- **violations of these privacy rights, unless justifiable according to the exceptions principle which follows, will be subject to proper redress.**

We listed the bundle of rights comprising privacy rights first, since everything else in this ethical foundation will build upon these basic rights. The fundamental privacy rights are intended to cover the full range of privacy expectations. In other words, they contemplate all the types of intrusive activities that people object to — from invasions of their bodies to unauthorized uses of their personal information, from secret surveillance of

---

2 The Australian Privacy Charter was developed with the encouragement of Justice Michael Kirby, President of the New South Wales Court of Appeal. It contains many elements common to data protection codes, but has greater breadth and puts more emphasis on rights and freedoms. For further information, see Chris Connolly, *Smart Cards: Big Brother's Little Helpers,* No. 66, The Privacy Committee of New South Wales, Sydney, August 1995.

their conduct or performance to eavesdropping on their private telecommunications and encroachments upon their personal spaces.

Accompanying these fundamental rights are guarantees that appropriate steps will be taken to ensure these rights are respected and, if they are violated, that suitable redress will be available. However, since they are simply broad statements of principle or declarations of entitlements, they do not attempt to prescribe specific protective measures or redress mechanisms.

The next principle establishes the threshold that must be crossed to justify infringing on the fundamental privacy rights and guarantees preceding it. The standard that must be met here is similar to section 1 of the *Canadian Charter of Rights and Freedoms*, the "saving provision."

### 2. *Justification for Exceptions*

> Exceptions, allowing the rights and guarantees set out above to be infringed, will only be allowed if the interference with these rights and guarantees are reasonable and can be demonstrably justified in a free and democratic society.

This exceptions principle recognises that privacy rights, like other fundamental human rights, are not absolute and sometimes they may have to be infringed in the name of some other collective benefit. At the same time, it reflects the Committee's opinion that the onus should not be placed on individuals whose rights are infringed to defend them, it should be placed on those who violate these rights to defend their actions. The only acceptable justification for infringing such a right would be concrete proof that the invasion is in the public interest or serves a greater common good; and for it to be reasonable, the benefits achieved would have to outweigh the harm created.

The outcome of implementing this principle would be, for example, to allow those who wish to install surveillance cameras on every street corner to do so only if they can demonstrate that the threats posed to private property and personal safety are so serious that installing cameras would justify monitoring people's activities there. By putting the onus on the invaders, this principle would address the power imbalance which concerned so many townhall participants who felt helpless to challenge the actions of governments or large corporations.

The Committee finds that rights do not exist in isolation, they bring with them corresponding responsibilities. Therefore, accompanying these fundamental privacy rights and guarantees is a series of general obligations or responsibilities.

### 3. *General Obligations*

**3.1 The basic duties owed to others to ensure their privacy rights are adequately respected include:**

- **the duty to secure meaningful consent;**
- **the duty to take all the steps necessary to adequately respect others' privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;**
- **the duty to be accountable;**
- **the duty to be transparent;**
- **the duty to use and provide access to privacy enhancing technologies;**
- **the duty to build privacy protection features into technological designs.**

As we mentioned in Chapter One, "meaningful" consent was consistently raised as a key issue in the townhall meetings. Many people told the Committee they were not given either an opportunity to consent to invasions of their privacy or enough information to make a well-informed decision. In light of this, the Committee believes that those who wish to infringe upon others' privacy must secure meaningful consent, a requirement which puts the onus on them to provide enough information to others to permit a choice to be made that is informed by knowledge of the consequences. We realize that it may not always be possible to secure the consent of every individual affected. In such cases, meaningful consent would have to be obtained in another appropriate way, for example by conducting some type of public consultation, hearing or poll and acting upon the wishes of the majority. We do not believe consent to privacy invasions should ever be implied — there must be a positive obligation on the infringer to seek consent in an appropriate fashion.

The duty to take all steps necessary to adequately respect others' privacy rights is the flip side of the coin guaranteeing that privacy rights will be respected. What would be considered necessary and sufficient measures would be prescribed through secondary principles, whether legislation, regulations, policies or codes of practice.

The duties to be accountable and transparent are intended to answer the public's expectation that an identifiable and independent person be made responsible for monitoring compliance with existing privacy rules. One of the most common complaints was that people did not even know when and how their privacy was being violated. Thus, many of the townhall participants wanted organizations' technologies, systems, services or activities affecting privacy to be revealed to those who are affected, not kept invisible. Implementation of the transparency principle could be as simple as posting signs in a shopping mall that tell people where in the mall they are being monitored by video cameras or providing taxpayers with a list of all government departments with whom Revenue Canada shares or cross-matches the personal information filed with their income tax forms.

The last two obligations set out above recognise that technology can have a marked impact on people's privacy, and given this reality the Committee feels it is important to require, as a matter of principle, that technology be used and designed in ways that serve rather than defeat privacy rights.

In addition to the fundamental privacy rights, set out above, our core principles would include particular rights that flow from the right to privacy of personal information.

### *4. Specific Rights Related to Personal Information*

- **Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable.**

- **Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified.**

As we mentioned in Chapter One, a very thorny issue raised by individuals at our townhall meetings was: who owns my personal information? People did not want to feel that by giving their personal information to someone for one purpose, they forfeited control over its use for other purposes. In other words, they wanted to retain control over it at all times; therefore, they wanted to be declared to be the "owners" of their personal information. In order to make such a right enforceable, it may require special legislation — an analogy, in law, could be made to copyright, whereby the creator of an artistic work owns the right to reproduce it and others must get permission to use it or be subject to penalties under the *Copyright Act*. The Committee believes that the right of ownership over one's personal information must be recognised as a core privacy principle.

The right to enjoy anonymity in relation to one's personal information is an attempt to undo the considerable damage caused to privacy by the fact that personal information linked to an identifiable person has commercial value. The commercial imperative operates against anonymity, thus a rights-based approach to privacy requires that people be entitled to be treated anonymously. The anonymity principle would also ensure that identifying information would be de-identified if it were used for another purpose that did not require the information to be linked to a specific person. For example, a recent issue of *Canadian Forum* reported that Human Resources Development Canada (HRDC) cross-matches its records with those of Revenue Canada to track how many Canadians who return to the workforce after receiving federal assistance continue to support themselves over the long-term.[3] This data matching is done to reveal whether HRDC's assistance programs are saving the government money in the long run. The author does

---

3 Paul Weinberg, "Terminal Case", *The Canadian Forum*, April 1997, p. 17.

not indicate whether personal information is de-identified in the data matching process. It is our view that if the true purpose of this type of data matching exercise were to gauge the success of programs, rather than draw up profiles of suspected "chronic abusers" of the system, then it should not be necessary to identify, by name, that "John Smith" stayed off pogey for only one year.

Last but not least, the core principles set out the obligations specifically associated with informational privacy. These are the responsibilities that go hand in hand with this particular privacy right.

### 5. *Specific Obligations Related to Informational Privacy*

**5.1 The basic duties owed to others to ensure their informational privacy rights are adequately respected include, in addition to the general obligations set out above:**

- **the duty to hold sensitive personal information in trust;**
- **the duty to limit information collection to what is necessary and justifiable under the circumstances;**
- **the duty to identify the purpose for which personal information is collected;**
- **the duty to ensure the information collected is correct and of the highest quality;**
- **the duty to provide the people whose personal data is collected with access to that information and a means to review and, if necessary, to correct it;**
- **the duty to only use and disclose personal information for the purposes identified when meaningful consent was obtained;**
- **the duty to keep personal information only for as long as is necessary and justifiable;**
- **the duty not to disadvantage people because they elect to exercise their rights to privacy.**

With the exception of the first and last duties in this list, all the duties we have stated here are principles now recognised in modern data protection codes like Canada's own CSA Model Code. The first duty in this list recognises that sensitive, personal information, such as medical, genetic or financial records, requires the greatest care when it is handled by others. This principle would require those who collect and handle such

information — such as hospitals, doctors, insurance companies, and banks — to be held to a higher standard of care than those who are custodians of personal information that is not considered sensitive. As so many people reminded us, once sensitive personal information falls into the wrong hands — whether by accident or design — it cannot be recovered. Thus, it is imperative to ensure it is not mishandled in the first place. We feel sensitive information would be better protected if it were held in trust, with all the corresponding duties of "trusteeship" applying.

The last duty listed here would require companies, governments or others to not punish people for choosing to exercise their privacy rights. We learned over the course of our hearings that some companies and agencies have threatened to provide an inferior service, cut off a service or charged more for a service when a client has tried to assert his or her privacy rights. The Committee and Canadians find this type of pressure or blackmail to be offensive. We believe this principle would have precluded telephone companies from ever charging customers for blocking their caller-ID — a reprieve they finally earned only after launching consumer protests and appeals to the Canadian Radio-Television and Telecommunications Commission.[4] Perhaps, also, it would discourage utilities, if they fell under federal jurisdiction, from demanding that customers hand over their social insurance numbers or risk having their services cut off.[5]

## BEYOND THE BLUEPRINT

Bruce Phillips, the Privacy Commissioner of Canada, has repeatedly called for an ethical framework to be charted, setting out the principles that are essential to ensuring privacy is fostered and respected as a human right in our society.[6] We agree that such an ethical base is needed and have responded, as a Committee, with our blueprint of the core principles. We believe these core pinciples reflect the heart or crux of the values system that shapes Canadians' expectations of privacy.

We note, however, that the Privacy Commissioner's protection wish-list includes more than simply defining core values. He has also called for framework legislation, privacy impact analyses of existing legislation, a system for assessing the impact of technologies on society, more public education, access to and use of privacy enhancing technologies, and so on.[7] We agree with him that a set of core privacy principles or an ethical framework is only one piece of the comprehensive strategy that is needed to properly safeguard

---

4 *Evidence*, 30:14-15.

5 30:17-18.

6 24:25.

7 "Notes for an Address by Bruce Phillips, Privacy Commissioner of Canada, to the Standing Committee on Human Rights and the Status of Persons with Disabilities," 21 November 1996, p. 10-11.

privacy rights. Thus, even though it is our view that these core principles are the linchpin of such a strategy, we also know that the job of properly safegarding people's privacy only begins here.

The Committee's motivation in compiling such a comprehensive statement of core privacy principles was to get the ball rolling as quickly as possible, in the right direction — the human rights direction. One of the most common refrains we heard across the country was, "We need a strong legislative framework — basic rules of the road and effective compliance measures — and we need it now." Next, we will map out our vision for a comprehensive privacy protection strategy that starts with an overarching privacy rights framework — a Canadian Charter of Privacy Rights — entrenching the core principes identified here. It then builds from there by devising a number of associated privacy protection measures that accord with the Privacy Charter.

# CHAPTER 4: BUILDING UP PROTECTION: FROM BLUEPRINT TO BRICKS AND MORTAR

## FRAMEWORK AND BEYOND

> *The technology is making it possible to introduce more and more forms of intrusive surveillance of people conducting their lives in ordinary ways. And unless we're prepared to see ourselves being looked at, spied upon, probed and tested, we had better get a grip on this.*[1]
>
> *Bruce Phillips, Privacy Commissioner of Canada*

In the previous chapter, we created a blueprint for the foundational principles upon which a sturdy privacy protection system could be built. Designing them from a human rights perspective, we developed a list of core principles that described basic rights and responsibilities. In this last chapter of our report, we will outline the Committee's proposal for the overarching framework that would incorporate and breathe life into these core principles — a charter of rights for privacy. Once we have roughed out this framework or charter, we will describe the mosaic of measures required to supplement it . At the same time, we will suggest allocations of responsibilities — who needs to do what to ensure the job gets done and gets done well.

As we map out our plan for providing full and fair protection for individuals' personal privacy, we will continue to approach our task from a human rights perspective. To draw on the analogy used by Ursula Franklin, our aim is to propose that the regulation of privacy be treated more like maintaining a garden than managing a production site. When she spoke last September, about how people could live in a technological society, she painted a picture of stark contrasts between a world where justice and rights prevail, portrayed as a garden, and a world where technology rules, pictured as a production site. She concluded by suggesting a way to bridge these seemingly irreconcilable worlds: look for an "adequate" balance.[2]

Finding the right or adequate balance between individuals' privacy rights and all the other interests at play in an increasingly complex, high-tech world is a dynamic process that involves everyone. In terms of processes, it involves public debate, research, education, sensitization, legislation, regulation, codes of practice, privacy enhancing

---

1 *Toronto Star*, 10 May 1996.

2 Ursula Franklin, *Stormy Weather.*

technologies, pilot projects, and more. In terms of players, it requires everyone to join the team: politicians at all levels of government, corporations, educators, the media, privacy commissioners, technology and systems designers, bureaucrats, rights advocates, individual members of the public, and so on. Thus, protecting everyone's privacy rights becomes everyone's responsibility.

But how do we prevent this dynamic and collaborative process from degenerating into chaos? To begin with, the Committee proposes that it be framed by a charter of privacy rights — overarching human rights legislation that would guide the development and implementation of the various measures devised to adequately protect this priceless right.

## THE PRIVACY CHARTER

Everywhere the Committee travelled, participants in our townhall discussions asked that the government create a legal framework to establish ground rules for the protection of privacy. Usually, when people spoke of such legislation, they were in fact referring to a data protection framework. However, some, such as the Manager of Metro Toronto's Privacy Office, Rita Reynolds, summarizing one group's discussion, suggested a broader approach — a genuine privacy protection framework:

> There was a concern very strongly expressed about the fact that existing privacy legislation — federally, provincially, municipally — has no teeth and that rather than trying to go back and build greater strength into these laws, what is needed is overarching umbrella legislation that would give very clear protections to individuals over the collection of genetic information, things like video monitoring, biometric technologies ... [3].

The Committee prefers this broader conceptualization of the overarching framework. We do not believe that Canadians want ground rules to protect only their informational privacy, leaving the rest of their privacy rights to languish in a lawless frontier. Consequently, the protective framework we are proposing here will capture the full breadth of privacy, like a wide angle lens taking in a panoramic view, as opposed to the data

---

3 *Evidence*, 36:16

protection framework toward which the Industry and Justice Ministers are working that focuses, like a close-up lens, tightly on informational privacy rights.[4]

Furthermore, given our human rights perspective, we have chosen a human rights model as the prototype for our overarching privacy protection framework. We considered, but for practical reasons rejected, adopting a constitutional structure for our overarching framework, that is, the one offered by the *Canadian Charter of Rights and Freedoms.* Instead we elected to propose a quasi-constitutional framework, a bill of rights type of model.

The *Canadian Charter of Rights and Freedoms* did not suit our present purposes, for two reasons. First of all, constitutional amendments can be difficult to orchestrate and are unlikely to come about quickly. Considering the pressing need to develop suitable overarching legislation, the *Charter of Rights* did not present a realistic solution. Secondly, since the *Charter* applies only to government actions, even if a swift constitutional amendment to enshrine explicit privacy rights in it were possible, the effect would be to prevent only government policies, practices and legislation from unreasonably infringing on these rights. Policies and practices developed in the federally regulated private sector that adversely affect privacy rights would not have to comply with the *Charter of Rights.* Consequently, more than a *Charter of Rights* amendment would be required in any *event.*

We do not wish our proposal, which discards the constitutional option, to be interpreted as meaning that the Committee does not support entrenching an explicit right to privacy in the *Canadian Charter of Rights and Freedoms.* We wholeheartedly endorse the view expressed 10 years ago by Members then serving on the Standing Committee on Justice and Solicitor General: "When the time arrives to consider amendments to the *Canadian Charter of Rights and Freedoms,* the Committee believes that serious consideration should be given to creating a simple constitutional right to privacy."[5] Indeed, we think such a right should be entrenched.

The advantage of the framework we are proposing, a charter of privacy rights based in ordinary legislation like a bill of rights, is that it would be created through the usual legislative process like any other Act of Parliament, and so could be enacted faster than constitutional amendments. Secondly, as a federal statute, it could be made to apply to the

---

4 Government of Canada, *Building the Information Society: Moving Canada Into the 21st Century,* Supply and Services Canada, Ottawa, 1996, p. 25: "As a means of encouraging business and consumer confidence in the Information Highway, the ministers of Industry and Justice, after consultation with the provinces and other stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector." (This undertaking is part of the federal government's response to the Information Highway Advisory Council's Final Report, *Connection, Community, Content — The Challenge of the Information Highway,* released September 1995.)

5 House of Commons, Standing Committee on Justice and the Solicitor General, First Report, *Open and Shut: Enhancing the Right to Know and the Right to* Privacy, 2nd Session, 33rd Parliament, March 1987, p. 91.

federally regulated private sector and, therefore, have a broader reach than the *Canadian Charter of Rights and Freedoms.* Last but not least, like the *Canadian Bill of Rights* and other human rights codes, this statute would have what is referred to by the courts as "quasi-constitutional status," meaning it would have primacy over ordinary laws.[6]

The purpose of this proposed charter of privacy rights, which we refer to as the Canadian Charter of Privacy Rights, would be similar to Australia's Privacy Charter: to provide a statement of general principles concerning privacy rights and responsibilities in Canada that would serve as a benchmark against which the policies and practices of businesses and the federal government, as well as the adequacy of federal legislation and regulations could be assessed. Our hope would be, that ultimately this Privacy Charter would be adopted, in one way or another, as a guidepost for use, also, in the provinces and territories.

The Privacy Charter would not attempt to prescribe specific measures to protect the rights entrenched in it. It would, however, outline general requirements to ensure appropriate privacy protections are put in place through secondary instruments, whether they be other legislation, regulations, sectoral codes, guidelines, or any other regulatory mechanisms. In conclusion, the Committee believes an overarching legislative framework is needed to protect the full spectrum of privacy rights and the most appropriate model for this legislation would be a quasi-constitutional Act of Parliament.

**RECOMMENDATION 1**

**The Committee recommends that the Government of Canada recognise and act upon its responsibility to respect and protect privacy rights in Canada by enacting a declaration of privacy rights to be called the Canadian Charter of Privacy Rights. This Privacy Charter would apply within federal jurisdiction, take precedence over ordinary federal legislation and serve as a benchmark against which the reasonableness of privacy infringing practices and the adequacy of legislation and other regulatory measures would be assessed.**

**Furthermore, the Committee recommends that the Canadian Charter of Privacy Rights be enacted no later than the 1st of January 2000.**

### *A. The Elements of the Privacy Charter*

The shape, size and contents of the Privacy Charter, ultimately, should be decided through public consultation and with the collaboration of a broad range of Canadians. The

---

6 *Hogan v. The Queen*, [1975] 2 S.C.R. 574 at 579, Laskin, J. stated, "The Canadian Bill of Rights is a halfway house between a purely common law regime and a constitutional one; it may aptly be described as a quasi-constitutional instrument."

Committee does not believe such an important instrument should be cobbled together exclusively by bureaucrats and "stakeholders," working behind closed doors. Our intention, here, is to make recommendations about the basic contents of our proposed Privacy Charter, not to suggest the actual wording that should be employed.

### *1. The Core Privacy Principles*

The first, key inclusion in the Charter would be the core privacy principles set out in the previous chapter of this report. These core principles should be subjected to public scrutiny and comment, revised and refined accordingly, and then be entrenched in the Charter of Privacy. The core principles could be preceded in the Charter by a preamble, declaring the importance of privacy as a human right and recognising the primacy of the Charter over ordinary legislation given its quasi-constitutional status.

**RECOMMENDATION 2**

**The Committee recommends that the Canadian Charter of Privacy Rights declare and entrench fundamental privacy rights and the responsibilities attaching to these rights. These rights and responsibilities would include, but not necessarily be limited to, the following:**

**1. Fundamental Privacy Rights and Guarantees**

**1.1. Everyone is entitled to expect and enjoy:**

- **physical, bodily and psychological integrity and privacy;**
- **privacy of personal information;**
- **freedom from surveillance;**
- **privacy of personal communications;**
- **privacy of personal space.**

**1.2 Everyone is guaranteed that:**

- **these privacy rights will be respected by others adopting whatever protective measures are most appropriate to do so;**
- **violations of these privacy rights, unless justifiable according to the exceptions principle which follows, will be subject to proper redress.**

2. Justification for Exceptions

Exceptions, permitting the rights and guarantees set out above to be infringed, will only be allowed if the interference with these rights and guarantees is reasonable and can be demonstrably justified in a free and democratic society.

3. General Obligations

3.1. The basic duties owed to others to ensure their privacy rights are adequately respected include:

- the duty to secure meaningful consent;
- the duty to take all the steps necessary to adequately respect others' privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;
- the duty to be accountable;
- the duty to be transparent;
- the duty to use and provide access to privacy enhancing technologies;
- the duty to build privacy protection features into technological designs.

4. Specific Rights Related to Personal Information

- Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable.
- Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified.

5. Specific Obligations Related to Informational Privacy

5.1. The basic duties owed to others to ensure their informational privacy rights are adequately respected include, in addition to the general obligations set out above:

- the duty to hold sensitive personal information in trust;

- **the duty to limit information collection to what is necessary and justifiable under the circumstances;**
- **the duty to identify the purpose for which personal information is collected;**
- **the duty to ensure the information collected is correct and of the highest quality;**
- **the duty to provide the people whose personal data is collected with access to that information and a means to review and, if they judge it necessary, to correct it;**
- **the duty to only use and disclose personal information for the purposes identified when meaningful consent was obtained;**
- **the duty to keep personal information only for as long as is necessary and justifiable;**
- **the duty not to disadvantage people because they elect to exercise their rights to privacy.**

### *2. Other Key Elements of the Privacy Charter*

The core principles would obviously constitute the heart of the Privacy Charter. But, in our view, establishing at least five other elements of privacy protection in this Charter is also critical. In particular, it should include declarations (1) identifying the basic measures required to promote proper respect for privacy rights, (2) recognising that proper compliance and enforcement measures must be put in place, (3) recognising also that appropriate remedies to redress violations of privacy rights must be established, and (4) recognising that Privacy Commissioner of Canada is the general overseer and protector of privacy rights in all areas within federal jurisdiction. Finally, the Privacy Charter would impose legislative review requirements on the Minister of Justice. We believe it is important to entrench these elements of privacy protection in the Charter because they signal the basic steps that must be taken to properly protect privacy rights and indicate that privacy protection is not simply the job of the federal government.

From the townhall discussions, the Committee was able to identify at least three steps to achieving proper respect for privacy values: research, public awareness and education, and public consultation. Research must take place on several fronts — for example, from sociological, economic, technological, and legal perspectives — and must be carried out by people in all fields, government, industry and academe. It must also be carried out using practical and innovative techniques, the Rimouski health card pilot project being one

example of such an approach. Public awareness involves raising the consciousness of Canadians about their privacy rights and education involves teaching everyone, from government employees to technology designers and users, how to promote and respect privacy. Education, like research, must take place on all fronts and involve as many people as possible. Finally, in terms of measures to promote privacy, public consultation is critical every step along the way, whether its in developing legislation or policies, preparing a data matching proposal, developing a new product or rolling out a new service.

**RECOMMENDATION 3**

**The Committee recommends that the Canadian Charter of Privacy Rights declare that to achieve proper respect for privacy rights in Canada the following measures are essential:**

- **on-going public discussion and input on matters related to the protection of privacy rights;**
- **research related to privacy rights and their protection;**
- **public awareness and education to sensitise everyone to their rights and responsibilities with respect to privacy.**

By discussing privacy issues with Canadians, the Committee was able to identify the measures which people considered to be fundamental to ensuring that their privacy rights would be properly protected: compliance, enforcement and remedial action. We believe compliance measures should include adopting suitable tools to ensure that policies, regulatory instruments, practices and technologies fall in line with basic privacy values. For example, privacy impact analyses should be introduced to the processes of developing legislation, as well as to the development of government and business policies and practices. Privacy audits should be carried out to determine whether existing policies and practices comply with privacy principles. To govern new practices which could potentially affect privacy, such as data matching or video surveillance, transparent processes must be put in place involving consultation with the public and weighing the evidence to see if the privacy invading practice could be justified. And, in the case of technology, to ensure it complies with privacy values, again, privacy impact analyses should be carried out, preferably at the design stage of new technologies and systems to ensure that privacy issues are adequately addressed from the outset.

With respect to enforcement, the Committee concurs with the people who told us they wanted real incentives and disincentives put in place to reward those who protect privacy and punish those who do not. In particular, we agree sanctions should be introduced for serious violations of privacy rights that are commensurate with the gravity of the infringement. Also, we feel sufficient legal recourse and remedies must be provided

through some kind of independent complaint-resolution mechanism, tribunal or civil action, to resolve situations where administrative or non-judicial solutions cannot be found. Last but not least, we think the time has come to declare in law what has been the de facto situation for years — that the Privacy Commissioner of Canada is responsible for the general oversight and protection of individuals' privacy rights within the federal realm. The proposed Privacy Charter seems to us to be the appropriate place to recognise this important function.

**RECOMMENDATION 4**

**The Committee recommends that the Canadian Charter of Privacy Rights declare that, to ensure the core privacy principles are observed, the following measures must be put in place:**

- **proper compliance, accountability and enforcement mechanisms;**
- **appropriate remedies to redress violations of privacy rights.**

**The Committee further recommends that the Canadian Charter of Privacy Rights declare that the Privacy Commissioner of Canada shall exercise general oversight and protection of privacy rights within areas of federal jurisdiction.**

A final, critical feature of the Privacy Charter would be a provision for the review of legislation to ensure it conforms with the Charter. The Committee believes that, in addition to containing a general declaration that appropriate compliance mechanisms be put in place, the Privacy Charter should impose the specific statutory duty on the Minister of Justice to review existing and new legislative instruments for compliance with the Privacy Charter's principles.

The Department of Justice already reviews proposed legislation and new practices for consistency with sections 7 and 8 of the *Canadian Charter of Rights and Freedoms*. But, as we noted in Chapter 2, these sections address certain expectations of privacy but not necessarily the full spectrum of privacy rights. Indeed, the exact scope of privacy protection under the Charter of Rights is being determined daily, on a case-by-case basis, and Canadians do not yet know the full extent of its reach. The Committee believes that the proposed Privacy Charter could fill this void because it would identify the full range of Canadians' privacy rights and clarify the reciprocal obligations attaching to these rights. Consequently, it would provide an additional benchmark against which to assess federal legislation, legislative proposals and other legislative initiatives. The Privacy Charter should become integral to the Justice Department's legislative review process.

Furthermore, the Justice Minister should be required to notify the Privacy Commissioner of Canada of all new legislation and regulations having a potential impact

on privacy rights. At any one time, a substantial amount of legislation and regulations is before Parliament which has the potential to affect Canadians' privacy rights. By way of example, during the current session of Parliament, more than 50 new laws and regulations with possible ramifications for privacy were before Parliament. The Privacy Commissioner is not systematically informed of each instrument with a potential privacy impact, in spite of past directives from Treasury Board and the Justice Department to federal government departments to provide such notification. The Privacy Commissioner's Office carries out the time-consuming and inefficient process of tracking all new federal legislation and regulations, in order to detect any matters which could affect Canadians' privacy. Given the Privacy Commissioner's important role as the privacy ombudsman for the federal sphere, it is imperative that his Office be officially brought into the legislative loop through a formal notification process. Ideally, the Privacy Commissioner should be consulted at the development stage of legislation; but, at a minimum, consultation must occur once legislation is tabled in Parliament.

**RECOMMENDATION 5**

**The Committee recommends that the Minister of Justice, in consultation with the Privacy Commissioner of Canada, examine existing federal legislation and regulations, bills and draft regulations for consistency with the Canadian Charter of Privacy Rights and report any inconsistency to Parliament. This report shall be referred to the appropriate Parliamentary Committee for consideration and recommendations.**

**The Committee also recommends that the Canadian Charter of Privacy Rights require the Minister of Justice to notify the Privacy Commissioner of Canada of all bills tabled in Parliament and all draft regulations which may have ramifications for privacy.**

To summarize, the overarching legislative framework which this Committee has proposed, the Privacy Charter, would outline everyone's fundamental privacy rights and obligations, set out the ground rules to ensure privacy rights are respected, and measures to protect these rights are complied with and enforced. Also it would require that adequate remedies be put in place to enable people to pursue breaches of their privacy rights, would identify the Privacy Commissioner of Canada as the ombudsman for Canadians' privacy rights, and would make the Minister of Justice responsible for reviewing legislative instruments for privacy implications.

### *B. Leading by Example*

One of the most important functions that the federal government could perform, to safeguard Canadians' privacy rights, would be to become a strong advocate of this

Charter and encourage the provinces and territories to develop and adopt a similar framework for privacy protection in their respective jurisdictions. Clearly, a huge disparity exists across the country among federal, provincial and territorial privacy laws. Quebec's laws are the most advanced, providing extensive privacy protection to people in Quebec. On the other hand, certain Atlantic provinces provide such poor protection to their citizens that they were singled out for criticism:

> I would like to point out to some of your members from Atlantic Canada, by the way — and I happen to be a fifth generation New Brunswicker — that I am very concerned as a Canadian with the existence of data havens in the Atlantic provinces. None of them has even the beginnings, except perhaps Nova Scotia, of adequate privacy protection, never mind the private sector, but also in the public sector. I'm particularly disappointed with the Province of New Brunswick, if I may be so bold as to say so, as an academic. That province has been promoting the information highway, but has been doing nothing for privacy protection in either the public or private sectors.[7]

The unevenness in privacy laws across our country means that only in one province, Quebec, do Canadians have first-class privacy protection. In other jurisdictions, they have either second-class or no privacy rights. The Committee finds this situation appalling. Antidiscrimination laws in this country were harmonized over 20 years ago to ensure that Canadians would be accorded equal dignity and human rights no matter where they live or work in Canada.[8] Canada does not have "havens" or "lawless frontiers" where Canadians can be subjected to racism, sexism or other discrimination without adequate legal protections. Privacy is a human right as well. Canadians should not have different degrees of protection for this right, depending on where in Canada they have the good fortune to live and work. The Committee calls on the federal government to take a leadership role by promoting a uniform approach to privacy protection across all jurisdictions. We note that the starting point or the framework for the harmonization of privacy protections could be the Privacy Charter, which could serve as a guidepost and benchmark across the country.

**RECOMMENDATION 6**

**The Committee recommends that the Government of Canada take a leadership role to ensure that Canadians' privacy rights are accorded equivalent dignity across the country. The Government of Canada should invite the governments of the provinces and territories to work together to**

---

7 *Evidence*, 21:14-15

8 W. S. Tarnopolsky, "Discrimination and the Law in Canada," *UNB Law Journal / Revue de droit de l'UNB*, Vol. 41, 1992, p. 215 at 228: "By 1975, every province in Canada had established a Human Rights Commission to administer antidiscrimination legislation and, in 1977, the *Canadian Human Rights Act* established a federal commission. With minor variations, all the legislation is similar except that Saskatchewan and Quebec have additional protections."

**develop a complementary and uniform approach to privacy protection across Canada that would accord with the Privacy Charter.**

The federal government is a very large employer and handles massive amounts of Canadians' personal information. Also, it has jurisdiction over industries, such as banking, telecommunications, and transportation, which are pillars of our economy. It is the opinion of this Committee, that it is critical that the federal government, in its various capacities — as employer, provider of public programs and services, and industry regulator — set an example for other sectors and employers by becoming a model user of the Privacy Charter. With respect to applying the proposed Privacy Charter to its handling of personal information, the next section of this chapter will suggest a new data protection regime that accords with the proposed Charter's values. However, we are concerned that stronger federal data protection legislation may not address all the privacy issues arising in the federal government's workplaces. As a result, we are calling on the federal government to set a proper example by taking steps to apply the principles of the Charter in this field as well.

**RECOMMENDATION 7**

**The Committee recommends that the Government of Canada, federal agencies and all Crown Corporations identify privacy issues in their respective workplaces and institute appropriate measures that accord with the Privacy Charter to safeguard employees' privacy rights.**

## SECOND GENERATION PRIVACY PROTECTION

Having developed our proposal for a legislative framework to protect privacy, the Privacy Charter, the remainder of this chapter will focus on the second-generation of privacy protections, the specific privacy laws, regulations, sectoral codes, privacy enhancing technologies, research, education, public awareness programs and other protective measures that must be instituted to adequately safeguard privacy.

### *A. Data Protection: A New Regime*

An urgent need for broad data protection legislation in this country is clearly illustrated throughout this report. We heard calls across the country for a comprehensive and uniform set of rules to safeguard our informational privacy. While data protection legislation already exists in the form of the current Privacy Act, as noted in Chapter 2 of the report, it is limited both in terms of its application and enforcement. The Committee believes that these limitations must be eliminated through the enactment by Parliament of a new piece of specific legislation, known as the Data Protection Act. This Act would reinforce the principles set out in our proposed Charter of Privacy Rights by guaranteeing the right of

informational self-determination — the right to control and thereby determine the uses of one's own personal information.

In order to ensure that the security of personal information is taken seriously in the federal domain, the provisions of the Data Protection Act must have as wide an application as possible. The Committee therefore believes that it must extend to Parliament, all federal government departments, agencies, Crown corporation, boards, commissions and other institutions.

Any legislative action in relation to data protection must also extend to the federally-regulated private sector. We heard time and again from participants in our townhall discussions that voluntary compliance with privacy codes of practice does not work. As one participant pointed out, "the profit motive is very strong. Companies in the private sector are not going to act to protect citizens' privacy unless they're absolutely forced to." [9] Moreover, as noted earlier in the report , there is an urgent need for data protection legislation that extends to the private sector in order to meet the requirements of the European Union's Directive.[10]

In determining the best legislative model to adopt in the case of data protection, we are mindful of the Canadian Standards Association's *Model Code for the Protection of Personal Information* (referred to in Chapter 2). We like the fact that the fair information principles contained in this Code have been negotiated openly by industry, consumer representatives and government with the result being a national consensus on the standards of data protection.[11] While we have some concerns about simply legislating these standards into some kind of regulatory regime for the reasons we set out in Chapter 2[12], we still think that this Model Code is a good starting point in the development of a Data Protection Act.

Due consideration must also be given to the data protection approaches taken in other jurisdictions. We are aware, for example, of the Netherlands and the New Zealand approaches which are quite unique, particularly with respect to how they treat sectoral

---

9 *Evidence,* 34:24-25

10 The European Union *Directive on Data Protection* requires all member countries to adopt or adapt national data protection laws to comply with its provisions. Specifically, Article 25 prohibits member countries (and businesses within those countries) from transferring personal information to non-member countries, such as Canada, that do not adequately guarantee protection of that information.

11 Colin Bennett, "Rules of the road and level playing-fields: the politics of data protection in Canada's" *private sector, International Review of Administrative Sciences*, Vol. 62 (December 1996), p. 486.

12 See p. 30 of the text.

codes. For example, the *New Zealand Privacy Act 1993*[13] applies universal information privacy principles to both the public and private sectors, it has strong enforcement provisions, it pays special attention to the issue of data matching[14], and it even deals in an interesting way with codes of practice. The New Zealand legislation requires all public and private sector agencies to designate individuals as privacy officers so as to encourage compliance with the principles set out in the Act, and to co-operate with the Commissioner's requests and investigations.

The *New Zealand Privacy Act* grants strong enforcement powers to a Privacy Commissioner who is mandated to receive complaints, carry out investigations and mediate/conciliate disputes. Complaints may be made to the Commissioner by anyone alleging what is, or appears to be, an invasion of personal privacy. Broad investigative powers are granted to the Commissioner and, where a matter cannot be resolved through the dispute resolution process, appeal may be had to a complaints review tribunal which can grant enforceable remedies and award damages. Interestingly enough, the Commissioner may at any time ask for a declaratory judgement from the courts regardless of whether the matter in question is within the Commissioner's statutory mandate. The Commissioner also has the power to issue codes of practice that modify any of the legislated privacy principles as long as certain requirements are met. These codes become regulations which are enforceable as such under the legislation.

**RECOMMENDATION 8**

**The Committee recommends that the Government of Canada introduce into Parliament comprehensive data protection legislation to be known as the Data Protection Act to replace the current *Privacy Act*. This Act must accord with the Privacy Charter and apply to Parliament, all federal government departments, agencies, Crown corporations, boards and commissions, and other institutions, and to all federally-regulated businesses and industries. The Data Protection Act shall be enacted no later than the 1st of January 2000.**

**A broad and open process of public consultation shall precede the introduction of this legislation and provision shall be made in the Act for comprehensive public review of its provisions and operations within five years of the proclamation of the Act, and at regular intervals thereafter.**

---

13 The following information on the New Zealand legislation is taken from Ian Lawson's, *Privacy and the Information Highway: Regulatory Options for Canada*, A Study Prepared for Industry Canada, 1995, p. 21-22.

14 The New Zealand Commissioner's approval is required for any data matching operations other than some pre-approved government programs. The complaints review tribunal under the legislation can hear appeals where the Commissioner has refused to approve a data matching operation.

**The Government of Canada shall give due consideration to other data protection models, such as the Canadian Standards Association's *Model Code for the Protection of Personal Information* and the New Zealand *Privacy Act 1993,* when developing the Data Protection Act. The Data Protection Act shall recognise the role of federally-regulated industries in the development of their own privacy codes.**

It is evident that we are well into an age where the marketing of personal information has reached new heights. As Privacy Commissioner, Bruce Phillips, told us:

> We are in fact buying and selling large elements of our human personae. The traffic in human information now is immense. There is almost nothing the commercial and governmental world is not anxious to find out about us as individuals.[15]

As we travel along the information highway, most of our every day activities leave an electronic trail that can be stored in numerous databases. Businesses have been only too quick to realise the value of these information holdings and their potential to be tapped into, manipulated and sold without the individual's knowledge or consent. At the same time, governments are seeking leaner, more efficient and cost-effective administrations. As a consequence, we see more and more comparisons and integration of what were once discreet databases. This so-called "data matching" and "data warehousing" is now occurring both within and between governments.

At the federal level, we were astonished to learn that not only are government departments comparing personal information with one another ("data matching"), but that they are even cross-referencing this kind of information between programs within a single department. In terms of intradepartmental information sharing, we are aware that the Department of Human Resources Development Canada has implemented a data matching program with Revenue Canada that uses customs records to catch employment insurance "cheaters" who leave the country while still collecting benefits. Interestingly, when the Department consulted with the Office of the Privacy Commissioner, it received advice not to proceed with the proposed matching program. It was not so much that the Privacy Commissioner did not approve of the data matching per se; it was that persons who gave personal information to Revenue Canada at border crossings were not aware at the time this information was collected that it would be used in the future for purposes other than those for which it was originally presented. It was the violation of this fundamental privacy principle — the right to informed consent to secondary uses of personal information — that concerned the Privacy Commissioner.

Despite the advice of the Privacy Commissioner, the Department went ahead and implemented the matching program. It chose to rely instead on the advice of the

---

15 *Evidence,* 15:12-13

Department of Justice that its program was in compliance both with the *Privacy Act* and with Treasury Board policies and guidelines on data matching.

While we accept that lessening the burden of employment insurance (EI) fraud on the public purse is in the interests of Canadians, we are concerned that people be fully informed in advance, not after the fact, of the uses to which their personal information might be put by government officials. Moreover, we are generally concerned about the negative presumptions that all too often can be drawn from these sorts of matches. As Privacy Commissioner Bruce Phillips once stated:

> Computer matching turns the traditional presumption of innocence into a presumption of guilt: in matching, even when there is no indication of wrong-doing, individuals are subject to high technology search and seizure. Once the principle of matching is accepted, a social force of unyielding and pervasive magnitude is put in place.[16]

Clearly, the current *Privacy Act* contains little in the way of express controls on data matching. Indeed, if one examines sections 7 and 8 of the legislation, it is not difficult to see how departments, such as Human Resources Development Canada, can find legal support for their data matching activities.

The Department of Human Resources Development has also of late been chastised for its "laissez-faire" attitude about handling sensitive personal information and other security measures at its employment offices.[17] We cannot help but wonder how safe is the wealth of personal information (e.g. Income Security Program information, Canada Pension Plan information, Employment Program information, student loan information) contained within this single government institution. Certainly, cross-matching is occurring amongst these departmental programs.[18]

Where are the "firewalls" and the protective barriers against unnecessary intradepartmental and interdepartmental data matching? Where are the standards for acceptable data matching practices? The holes in the federal *Privacy Act* appear big enough to drive a truck through, and little more than bureaucratic assurances and goodwill seem to stand between databases residing within a single institution. To use Simon Davies'[19] analogy, the lack of effective safeguards here is the equivalent to the imposition of a general warrant on all personal information in the hands of the federal government. This practice must be stopped. Data matching in the federal public sector must be justified, and in those cases where it can be justified, there must be strict adherence to the principles of fair information practices that we want to see in a Charter of Privacy.

---

16 Privacy Commissioner of Canada, *Annual Report*, 1985-86.

17 Globe and Mail *article, April 14, 1997.*

18 Privacy Commissioner, *Annual Report*, 1995-1996.

19 *Evidence*, 22:21

**RECOMMENDATION 9**

**The Committee recommends that the Data Protection Act it proposes contain:**

- **strict protections against all unnecessary intradepartmental and interdepartmental data matching;**
- **standards for acceptable data matching practices;**
- **acceptable data matching practices that comply with the Privacy Charter, in particular the principles of informed consent and transparency.**

**RECOMMENDATION 10**

**The Committee recommends that to comply with the proposed Data Protection Act, the Treasury Board Secretariat, a central agency of the federal government must:**

- **create mandatory data matching guidelines;**
- **monitor federal government departments for compliance with the new guidelines;**
- **educate federal departments and employees on what constitutes unnecessary data matching practices.**

While there is a blurring of national and international borders in this informational age, the lines between the public and the private sectors are also becoming increasingly fuzzy. Governments are not only looking at ways to share service delivery with other levels of government, but are also looking to the private sector as well. This is all being done with very little consideration being given to privacy protection. In a shared governmental service delivery system, under which government's privacy protection laws would personal information records fall? What happens to the security currently provided by the *Privacy Act* when personal information is transferred or contracted out to the private sector? Until such time as data protection laws are uniformly extended to the private sector, compliance with the proposed Data Protection Act must be a condition of any privatisation agreement, as is often the case with *Official Languages Act* guarantees. Moreover, all federal government contracts for services should be required to comply with the provisions of the proposed Data Protection Act.

**RECOMMENDATION 11**

**The Committee recommends that the proposed Data Protection Act shall set out the circumstances under which data sharing between the federal and provincial governments is appropriate.**

**The Government of Canada should advise the provinces and territories that upon the enactment of the proposed Data Protection Act, all personal information shall only be shared with those provinces that have adequate data protection in place.**

**RECOMMENDATION 12**

**The Committee recommends that the proposed Data Protection Act must apply to:**

- **any personal information transferred from federal government institutions to the private sector;**
- **any contracts for providing services to federal government institutions.**

Needless to say, a carefully crafted piece of data protection legislation is strengthened by effective implementation mechanisms. As we will elaborate below, we do not see any point in re-inventing the wheel in this regard. As spelled out in the proposed Privacy Charter, the Privacy Commissioner of Canada should exercise general oversight and protection of privacy rights within all areas of federal jurisdiction. This does not mean, however, that responsibility for implementation of the proposed Data Protection Act should rest solely with the Privacy Commissioner. There are other players here that must take an active part in ensuring that data protection is not just pious hope — it must also be a reality.

To this end, we believe that under the proposed Data Protection Act, the Treasury Board Secretariat, as a central agency of government, should take responsibility for working with, and monitoring the compliance of, all federal government institutions. In the same vein, we believe that Industry Canada should work with, and monitor the compliance of, all Crown corporations and the federally-regulated private sector under the proposed legislation. The Privacy Commissioner would then be responsible under the proposed Act for working with and monitoring the compliance of Parliament, all federal agencies, boards, commissions and other government institutions. The Commissioner would also be ultimately responsible for ensuring the enforcement of the proposed Data Protection Act across the federal spectrum.

**RECOMMENDATION 13**

**The Committee recommends that:**

- **the Treasury Board Secretariat take responsibility for monitoring compliance by federal departments and agencies with the proposed Data Protection Act;**

- **the Minister of Industry take responsibility for monitoring compliance by the federally-regulated private sector with the proposed Data Protection Act; and**

- **the federal Privacy Commissioner be made responsible for ensuring enforcement of the proposed Data Protection Act and that penalties exist in the proposed Act for violations of its provisions.**

## *B. New Technologies and Other Specific Measures*

When the Committee undertook this study, we focused on the threat to privacy posed by three new technologies: genetic testing, smart cards and video surveillance. Our meetings, both the roundtables and the townhalls, revealed to us that these three technologies raise critically important and complex issues. Our consultations also convinced us that each of these three technologies need to be addressed immediately but perhaps treated differently.

We recognise that the federal government does not have complete jurisdiction over the regulation of these technologies. That does not, in our view, excuse the Government of Canada from exercising leadership and foresight in finding appropriate ways to protect the fundamental right of privacy as Canadian governments and the private sector grapple with ways to deal with physical monitoring, biological surveillance and personal identification practices.

It is also important to point out here, that we also believe that technologies can, in fact, be a force for social good. This is not just using existing genetic, video and biometric technologies in an appropriate way. It is also proactively promoting the development of technologies that can empower individuals and protect their privacy.

### *1. Biometrics*

The issue of appropriate personal identification systems has bedeviled business and governments for decades. When the federal government introduced the social insurance number (SIN), issues about its possible abuse were raised but the government felt quite confident that those fears were not well founded. Although in the recent past, the federal government has greatly restricted its own requests for the SIN number, the government's expectations proved to be quite wrong. By then, however, the cat was out of the bag, because the business community and other levels of government already were using the social insurance number of individuals for purposes that its originators had not intended.[20] There still is no prohibition against people, businesses, or non federal institutions or

---

20 *Evidence*, 24:23

governments demanding an individual's SIN number, although a person can refuse if he, or she, wants to — or is allowed to.

Traditional biometric technologies such as digitized handprints that allow access to databases raise serious privacy problems because of the link between the individual to a unique number that is unquestionably that particular person. These are more definitive and indisputable links than even a social insurance number can provide. The dangers of biometric technologies arise with the temptation that they present for data matching especially in the provision of government services.

The Committee believes that the introduction of biometric identification systems to provide access to various services raises enormous questions of privacy and human identity that need to be addressed now. For example, these technologies should be carefully regulated. Such systems should be introduced only for specific purposes and other uses should be strictly prohibited.

We were pleased to have had the opportunity to speak with the Privacy Commissioner of Quebec, Paul-André Comeau, about an experiment with microcircuit, or smart cards in the Rimouski area that was used to store different types of health information: administrative, emergency, vaccination history, medical records and medical information.[21] His cautionary words convinced us of the value of pilot experiments before any large-scale introduction of similar cards within the area of federal jurisdiction.

Our decision-makers do have choices. For example, smart cards do not have to store data but can simply store the key that allows an individual — and no-one else — to gain access to data banks elsewhere. Should there be over-rides that permit others' access in certain restricted circumstances?

**RECOMMENDATION 14**

**The Committee recommends that the Data Protection Act regulate the development, testing (including pilot projects), implementation and application of emerging technologies that have a potential to infringe on the privacy of personal information. These technologies would include, but not be limited to, smart cards and biometric identification systems.**

### 2. *Genetic Testing*

The implications of genetic testing touch the issue of discrimination, and basic justice. The very first concern must be to address the issue of what actions are ethical and which

---

21 *Evidence* 21:11. The smart card experiment in Quebec was launched by the Regie de l'assurance-maladie du Quebec with the collaboration of researchers from Laval University and medical practitioners. It covered approximately 7,500 people, the majority over 60 years of age, pregnant women and babies under 18 months.

are unethical. Genetic testing issues are unique among all the questions related to new technologies that we considered. The personal characteristics that are revealed through DNA testing set it apart in nature and in importance from biometric identification and video surveillance. What distinguishes it is not just the potential for predicting the onset of disease for the individual but its intrusive nature. Any genetic test of an individual provides similar information about his or her children, siblings and parents. The ownership issue is critical and each individual should retain ownership and control of his or her own genetic information.

This Committee shares the strong consensus which emerged from our consultations that an overarching human rights framework must guide all decisions regarding the human genome. We also believe that Canada needs very separate and special protections to regulate the collection, use and ownership of genetic information because of its very private, personal nature and its potential intrusiveness. Privacy legislation is essential but not necessarily sufficient because of the power that genetic information can provide to the holder of the information and the unequal power relationship between the individual and commercial interests, like insurance companies, who may be requiring genetic tests. This Committee believes that insurance companies need to establish a balance between the information that is truly essential for insurance underwriting and the basic equity in society where people are not discriminated against on the basis of susceptibility.[22] Human rights legislation is also necessary to protect individuals against adverse discrimination on the grounds of their genetic inheritance. What is required is a comprehensive approach that involves privacy, human rights and also specific prohibitions against genetic testing except under particular, and well understood circumstances. This Committee tends to share Margaret Sommerville's view that the basic premise should be that there is a basic presumption against genetic testing unless it can be justified under very specific conditions and circumstances.[23]

Other countries are grappling with the same problem. The member countries of UNESCO will be considering a draft declaration on the human genome. We know that the United States Congress and many American state legislatures are dicussing genetic privacy and other protective bills. People with genetic disorders are also protected under the *Americans with Disabilities Act*. In addition, there are model acts proposed in the United States that, for example, hold companies that carry out genetic testing and their staff liable unless they are assured that a genetic test has been carried out voluntarily. Several European countries have legislation that prohibits the use of genetic information for insurance purposes.

---

22 *Evidence*, 28:32

23 28:17

In the United Kingdom an advisory committee on genetic testing has been established. This approach, embodied in a federal/provincial/territorial committee could look into the issue of quality control and the reasonableness of particular genetic tests in the areas of insurance and employment. The structure of human rights commissions might be an appropriate model. There is an important distinction, however, because human rights commissions work reactively and any body with authority to deal with genetic testing model must be proactive and have the power to prohibit any particular test.

The very fundamental question that needs to be addressed is the requirement for different treatment than other health information. This issue must be dealt with in the near future because it will become increasingly difficult to distinguish health data from genetic data. Genetic information cannot be dealt with like health information because it is both qualitatively and quantitatively different.

**RECOMMENDATION 15**

**The Committee recommends that the Government of Canada take immediate action to deal with privacy violations and discriminatory treatment that may result from genetic testing including:**

- **a review of current policies and practices in the employment, health, insurance and criminal justice sectors;**
- **a review of existing reports and existing and proposed legal instruments (including the draft international covenant on the human genome);**
- **consultations with the public;**
- **the development of legislation that is necessary to deal specifically with the privacy and antidiscrimination issues related to genetic testing.**

### *3. Video Surveillance*

This Committee has come to the conclusion that the Government of Canada should move quickly to introduce legislation to protect Canadians from unwarranted, surreptitious video surveillance. Representatives of the private security industry told us that the industry has failed in terms of applying moral, ethical and other standards to itself. The industry is motivated by profits. Obviously, a licencing system to purchase equipment would not be appropriate given that any member of the public can purchase surveillance

technology from catalogues.[24]. In addition, there are no standards and guides on the storage, use and access to videotapes. Video surveillance is one area where a strong consensus about the need for legislative action emerged from our consultations.

Technological developments in the video field permit ever more intrusions into personal pivacy. For example, computerized facial recognition, which is in its infancy, permits video images to be scanned into a computer and whenever the same face is seen by a video camera, it will track the appearances of an individual in a series of locations.

We know that most of the video surveillance systems take place on private property and therefore do not fall within the purview of federal legislation. At the same time, it has gone beyond the purview of dealing with national security interests and law enforcement agencies. Because it is cheap and easy to instal it is being used by employers, commercial interests and service providers. Nonetheless, we believe that it is important that the Government move quickly to amend the *Criminal Code* to provide an enforcement mechanism and penalties to deter abuse wherever possible. The justification for warrants under the *Criminal Code* might be narrowed so that intrusive surveillance by the police can be authorized only where there is a serious national security issue or imminent peril to life and limb. On the other hand, the offence provisions of the Code regarding the interception of private communications must be broadened to cover surreptitious video monitoring.

**RECOMMENDATION 16**

**The Committee recommends that the Government of Canada introduce amendments to the *Criminal Code* that would, to the greatest extent possible, apply the prohibitions against the interception of private communications to surreptitious video surveillance.**

### *4. Privacy Enhancing Technologies*

The Committee believes firmly that technology should adapt to privacy rights and not the other way around. We also know the futility of pretending that our society can stem the pace of technological change — but we can make technologies work for us. One method of ensuring this is the encouragement of privacy enhancing technologies. Like legislation, these take as their starting point the problem of the collection and use of personal data. In order to protect privacy, these technologies must limit or eliminate the collection of personal information and still ensure that personal information can flow without the risk of unauthorized use or interception.

These technologies can, for example, provide an individual with a means of controlling the information that is collected by the use of encryption that can protect

---

24 *Evidence*, 27:23-27

information in sensitive databases. Regarding biometric identification systems, for example, finger patterns are unique but retaining an actual copy or fingerprint is not necessary to develop the access code. Encryption technology allows the conversion of finger patterns to an algorithmic code with no connection with the finger pattern whatsoever. It disguises the number so that it is unreadable without the finger pattern and the fingerprint itself is not stored anywhere in the process. Privacy enhancing technologies can permit personal data to be rendered anonymous. They can, therefore, enhance an individual's privacy without limiting access to information.[25] Technology can also encrypt the data on a smart card so that a finger pattern becomes the key to the information on the card.

The system can protect the privacy of the individuals and at the same time reduce fraud.[26] The problem is to ensure that private enterprise uses privacy enhancing technologies and this might best be achieved in legislation. Abuses of stored personal information can be better dealt with. For example, tracing systems can provide a better way of tracking who has been accessing. But Canada has only a limited opportunity to influence the development of privacy enhancing technologies because much of the technology is foreign-made and imported to Canada from many different countries.

There is a huge task of education ahead with regard to privacy enhancing technologies. Not only does the public need to know what they are and how they can help preserve individual privacy, but also businesses and technology developers and promoters need to understand the potential — social as well as economic — of these developments. Both sides can benefit and privacy enhancing technologies can meet the needs of all three parties.

**RECOMMENDATION 17**

**The Committee recommends that the Government of Canada, in particular Industry Canada, encourage the development and use of privacy-enhancing technologies by:**

- **developing partnerships and creating incentives for research and development into privacy enhancing technologies;**
- **educating the public and businesses (large and small) about the capacity of privacy enhancing technologies to protect the personal information of Canadians.**

---

25 *Evidence*, 29:5

26 29:17-26

## 5. *Public Awareness, Consultation and Education*

A consistent theme of this report from its introduction to its conclusion has been the critical need for public awareness and education with regard to privacy rights and democracy in general, and the implications of new technologies and their impact on human rights and privacy, in particular. During our initial roundtables we heard that the level of knowledge was so low that in itself, it has become a threat to privacy rights. How can we understand our world, if we do not understand the implications of technological development? In reality, this Committee needed no convincing. But it was gratifying to see that our consultation process itself became an educational tool and we believe that the process we undertook needs to continue. Governments at all levels have a role in this; the media have a part to play; the private sector must be involved; privacy commissions need the capacity for outreach; educational institutions have an obligation to teach ethical behaviour to their students.

Education is the only way that individuals can be empowered to make choices. People need to know that they do not have to provide their social insurance number under many circumstances. They are under no obligation to provide personal information on warranty cards. They can refuse to allow businesses to share information about them by filling in an opt-out box. In many ways, education is the major way to restrict the dissemination of personal information and to prevent secondary uses — a major concern raised during our consultations. Businesses need to know that it is to their advantage to respect the wishes of their customers with regard to personal education. There is an opportunity for a competitive edge.[27]

The education function is perhaps one of the most neglected elements related to privacy. The resources of the federal and provincial privacy commissions are very scanty. The Privacy Commissioner of Canada has no budget for this purpose. This Committee has come to the conclusion that obligations to perform this task must be more formalised.

**Recommendation 18**

**The Committee recommends that the Government of Canada undertake ongoing public awareness and education programs about new technologies and their impact on privacy to ensure that everyone is able to make appropriate decisions regarding their personal privacy and the direction of public policy in the future.**

**The Committee further recommends that the Government of Canada should undertake an ongoing public consultation process that examines and**

---

27 *Evidence*, 21:16-18

**makes recommendations about specific legislative and non-legislative measures that are required to ensure that individuals' privacy is protected as technologies are refined or brought into use.**

**The Committee further recommends that the Government of Canada initiate ongoing discussions with the provinces with a view to encouraging a common approach to the treatment of these technologies (particularly genetic testing) within different jurisdictions.**

### *C. Enhanced Role of the Federal Privacy Commissioner*

As noted in Chapter 2 of the report, the title of the current *Privacy Act* is a misnomer. In setting out the minimum standards for the collection, use, disclosure and disposal by federal government institutions of clients' and employees' personal information, the law deals only with data protection. Broader privacy issues, such as genetic testing, electronic surveillance in the workplace and biometric identification are not covered. Any ongoing work on the privacy implications of these new technologies is due to the commitment and, to a large extent, initiative, of the previous and current Privacy Commissioners, and their staff, and not to any suitable legislative mandate.

The *Privacy Act* is not only limited in scope, but also in its application and enforcement provisions. Despite recommendations made in March 1987 by the House of Commons Standing Committee on Justice and Solicitor General in its report *Open and Shut*[28] and undertakings made by the federal government of the day in its response, *The Steps Ahead,* in October 1987, the limitations remain.

In *Open and Shut*, the Standing Committee recommended, among other things, that the *Privacy Act* be amended to include a mandate for public education; that the Act be extended to all government institutions, Crown corporations and their wholly-owned subsidiaries, and the federally-regulated private sector; that the Privacy Commissioner have the power to issue binding orders and that civil remedies and criminal penalties be awarded for breaches of the legislation; that the Act be amended to explicitly deal with electronic surveillance, drug tests and polygraphs and that the Privacy Commissioner monitor developments in these areas. In response to these recommendations, the federal government of the day undertook only to give the Privacy Commissioner a public education mandate and extend the Act to Crown corporations.[29] Neither of these undertakings was implemented.

---

28 Section 75 of the *Privacy Act* required that the administration of the Act be reviewed on a permanent basis by a Committee of Parliament and that this review be undertaken within three years of proclamation of the Act and be completed within a year of that date. The Standing Committee on Justice and Solicitor General was the parliamentary committee that carried out this review in 1986 and 1987.

With respect to the other recommendations, the government of the day felt that there was no justification for additional sanctions in the *Privacy Act* as ample administrative remedies already existed within the legislation. As well, the government felt that it would be inappropriate to amend the Act to deal with topics such as drug testing, electronic surveillance and polygraphs since these issues extended beyond data protection. The then government stated that it would monitor developments in this area.

Finally, a key recommendation, to extend the reach of the *Privacy Act* to the federally-regulated private sector, was not accepted. Since 1987, however, international and commercial pressures, such as the European Union's Directive, have interceded and the current federal Minister of Justice, Allan Rock, has announced that the government aims to have effective, enforceable privacy protection federal legislation in place by the year 2000 and that it will extend to the private sector.[30]

Clearly, privacy in its broadest sense is a widely-accepted fundamental value in this country that is worthy of proper legislative protection. The principles set out in our proposed Privacy Charter must not only be reflected in all federal legislation pertaining to issues of privacy, but also require that a strong, independent mechanism be put in place to oversee and ensure the full implementation of these laws. While this mechanism already exists to some extent in the form of the federal Office of the Privacy Commissioner, we do not feel that it is being utilised to its maximum potential. The mandate of this office must be both broadened and significantly strengthened — to this end we propose that new legislation, to be known as An Act Respecting the Office of the Privacy Commissioner of Canada, replace the current *Privacy Act*.

The Office of the Privacy Commissioner must have the power to deal with all privacy issues within the federal public and private sectors, and it must have adequate enforcement mechanisms at its disposal to carry out this oversight role. We propose that consideration be given to granting the Commissioner powers to enable him or her to react to perceived privacy invasions by means of a complaint investigation and resolution process that would include review mechanisms in the form of an administrative tribunal and the provision for judicial review.

Privacy invasions cannot, however, always be addressed in isolation, on a case-by-case basis. Sometimes a broader, more proactive approach must be adopted. To this end, we believe that the Privacy Commissioner should play a role in assessing the privacy implications of new technologies. This would have the benefit of identifying risks before systems develop, with obvious cost savings. As well, we believe that the Privacy

---

29 *The Steps Ahead,* 1987, p. 15 and 55.

30 Address by the Honourable Allan Rock, Minister of Justice and Attorney General of Canada to the Eighteenth International Conference on Privacy and Data Protection, Ottawa, September 18, 1996.

Commissioner should be able to initiate his or her own privacy investigations through the use of privacy audits.

While it may be necessary in some cases to ensure compliance by means of complaint resolution and coercive measures, these mechanisms are rarely effective in the resolution of human rights issues. Persuasion and education are still the best methods of achieving our privacy objective and this has clearly been the tack taken by Privacy Commissioner Bruce Phillips. We do not wish to diminish these privacy enhancing tools. They are still a vital part of the process. As was recommended in *Open and Shut,*[31] a public education mandate must therefore be accorded to the Privacy Commissioner and this mandate must be spelled out in the new legislation.

In order for the Privacy Commissioner to adequately carry out his or her new duties and responsibilities under the proposed Office of the Privacy Commissioner Act, sufficient resources must be made available. Failure to fund and staff an office that is already stretched to the limit in terms of meeting its current mandate, would only render the proposed powers and responsibilities of the Office of the Privacy Commissioner meaningless.

Finally, the introduction of a new Privacy Act cannot be undertaken without an open and broad public consultation process. The message that we heard loud and clear across this country was that the speed with which we need comprehensive privacy protection legislation should not be used as a reason to run roughshod over the need for public input and collaboration. Moreover, it is vital that this public consultation or dialogue continue after the enactment of new privacy legislation. We therefore believe that a mechanism for regular public review should be contained in the proposed Act.

**RECOMMENDATION 19**

**The Committee recommends that the Government of Canada table in Parliament new legislation that would replace the current *Privacy Act,* to be called An Act Respecting the Office of the Privacy Commissioner of Canada. This Act would broaden and strengthen the mandate and powers of the Privacy Commissioner in relation to all issues of privacy within the federal sector. Specifically, it should contain, but not be limited to, provisions that empower the Privacy Commissioner to:**

- **receive, investigate and settle complaints of alleged privacy invasions;**

---

31 The Committee on Justice and Solicitor General proposed in recommendation 2.1 of *Open and Shut* that for the purposes of clarification, the *Privacy Act* must mandate the Treasury Board and the Privacy Commissioner to foster public understanding of the Act and of the general principles contained therein. It also recommended that education must be directed towards both the general public and the personnel of government institutions and it is in the latter area that the Treasury Board would play a key role.

- initiate his own privacy investigations through the use of privacy audits and technology impact assessments;
- carry out studies relating to privacy and emerging technologies;
- review all government bills, legislation, regulations, delegated legislation, policies and practices that may have an impact on privacy rights and, whenever appropriate, table a privacy impact statement before the House of Commons;
- ensure effective enforcement of the proposed Data Protection Act.

**This Act shall apply to Parliament, all federal government departments, agencies, Crown corporations, boards, commissions and government institutions and to the federally-regulated private sector.**

**This Act shall contain complaint review mechanisms such as an administrative tribunal and the provision for judicial review.**

RECOMMENDATION 20

**The Committee recommends that the introduction of An Act Respecting the Office of the Privacy Commissioner must:**

- be preceded by a broad and open public consultation process;
- provide for a comprehensive public review of its provisions and operations within five years of the proclamation of the Act and at regular intervals thereafter;
- assign a general public education mandate to the Privacy Commissioner.

RECOMMENDATION 21

**The Committee recommends that Parliament provide sufficient resources to the Office of the Privacy Commissioner to adequately carry out its proposed responsibilities.**

## CONCLUDING REMARKS

The Members of this Committee have come to understand that privacy rights in Canada are in danger. The threat is not from a mighty, untameable monster called "technology" but from us, if we blindly join behind the steady march of technological "progress." In Bruce Phillips' words, the potential harm is: "the tyranny of ignorance, of unthinking acceptance of technology without regard to the consequences."[32]

We believe the time has come for governments to exercise greater vigilance to ensure "technology" and "progress" are not contradictory notions — that technological progress and social values develop synchronistically. Technolgy and its impact on privacy rights provide a prime example of a field where this work, this readjustment, must take place immediately.

David Flaherty once wrote: "Privacy is like freedom; we do not realize its importance until it is taken away."[33] The more our privacy erodes, the more high-tech surveillance permeates every facet of our daily lives, the more we come to prize our right to privacy and to understand that, indeed, it is a fundamental human right. Unfortunately, the more privacy we give up, the more we also come to realize the truth in Bruce Phillips' admonition that privacy is not a renewable resource, once lost it cannot be recaptured.

We hope that this report will convey a strong sense of both the urgency and importance of developing suitable means to protect privacy rights in Canada. It offers a useful strategy and realistic ground rules to pull privacy rights out of their downward spiral.

Ultimately, this report is about taking privacy seriously as a human right. To do that, we must invoke recent history and remind ourselves *why* the right to privacy was entrenched in the *Universal Declaration of Human Rights* and subsequent human rights instruments. Otherwise, we may be seduced into believing that privacy is simply a consumer rights issue that can be fixed by a few codes of conduct and some new, privacy enhancing technology.

The stakes are very high. If we lose site of the rights-connection, and if we do not use a rights-based approach to safeguard our privacy, we will embark down a slippery slope that diminishes other fundamental rights, such as the freedoms of association and expression. For, as German law professor Spiros Simitis pointed out to American law students over 10 years ago: "(C)onsiderations of privacy protection involve more than any one particular

---

32 Privacy Commissioner of Canada, *Annual Report 1995-96*, Office of the Privacy Commissioner, Ottawa, 1996, p.1

33 David Flaherty, *Entrenching A Constitutional Right to Privacy for Canadians: A Background Paper* (part of the Privacy Commissioner of Canada's submission to the Special Joint Committee on a Renewed Canada, 1991), p. 2.

right: they determine the choice between a democratic and an authoritarian society."[34]

If we let technology, convenience and efficiency dictate the limits of privacy rights in Canada, we will have a very orderly country. But, in the process, we will lose something fundamental to democracy — individual autonomy and dignity — and "Big Brother" will have triumphed.

34 Spiros Simitis, "Reviewing Privacy in an Information Society," *University of Pennsylvania Law Review*, No. 135, March 1987, p. 707 at 734.

# APPENDIX I

# PRIVACY RIGHTS AND NEW TECHNOLOGIES: CONSULTATION PACKAGE

**PREPARED FOR THE HOUSE OF COMMONS STANDING COMMITTEE ON HUMAN RIGHTS AND THE STATUS OF PERSONS WITH DISABILITIES**

**Susan Alter**
**Nancy Holmes**
***Law and Government Division***

**William Young**
***Political and Social Affairs Division***

**12 February 1997**



**Research Branch**

# TABLE OF CONTENTS

# OUTLINE OF COMMITTEE STUDY

## THE CONCEPT OF PRIVACY

Privacy is a human right with a grand tradition, both nationally and internationally. It is recognised in the *Canadian Charter of Rights and Freedoms* and such international human rights instruments as the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*. Classically understood as "the right to be let alone," privacy in today's high–tech world has taken on a multitude of dimensions. According to certain privacy experts, it is the right to enjoy private space, to conduct private communications, to be free from surveillance and to respect the sanctity of one's body. To the ordinary Canadian, it is about control – the right to control one's personal information and the right to choose to remain anonymous. **Privacy is a core human value that goes to the very heart of preserving human dignity and autonomy.** It is a precious resource because once lost, whether intentionally or inadvertently, it can never be recaptured.

## OUR FINDINGS TO DATE

As Members of the Standing Committee on Human Rights and the Status of Persons with Disabilities, we are taking a decidedly human rights approach to assessing the effects, both positive and negative, that new technologies are having on our right to privacy. In the spring of 1996, we held a series of round table discussions on the impact of new technologies on human rights. During the course of these hearings, expert witnesses repeatedly warned us of the rapid erosion of privacy rights due to modern technological advances. The nature of the current situation was aptly summed up by the Privacy Commissioner for Canada, Mr. Bruce Phillips:

> **The issue of privacy is much broader than merely the traffic in information over electronic systems. It gets into all kind of things, such as biomedical applications in the workplace and surveillance systems. There is almost no aspect of human life these days that does not have a privacy implication in which technology is involved. We're at risk now of losing all of our sense of autonomy and in the process of sacrificing a**

> **fundamental human right. I wouldn't go so far as to say privacy no longer exists, but it's certainly breathing hard to stay alive.**

The concern that the right to privacy is currently suffering from abuse and neglect prompted us to devote our hearings during the fall of 1996 to assess the scope of this right and to ascertain its place relative to the advantages, efficiencies and convenience of new technologies. We were astonished, and alarmed, at how all–encompassing and widespread the monitoring of our personal lives has become. A simple credit card transaction, a secret kiss (caught by a hidden surveillance camera) and a genetic test for medical purposes, while seemingly isolated and private incidents, can easily become public knowledge thanks to advances in modern technology. Indeed, the capturing and commercializing of personal information in our computerized world has become big business. This is no longer the cloak and dagger stuff of government and police spy operations. New technologies are being regularly used by private individuals, employers, and such businesses as banks and insurance companies to monitor, record and track many aspects of our daily lives.

## PRIVACY PROTECTION

There is no comprehensive protective framework for safeguarding privacy interests in the face of these new technological applications. With technological advances rapidly changing the nature of relationships, Canadians must struggle with a complicated and increasingly ineffectual system for safeguarding their privacy interests. They must draw upon international law, constitutional laws, federal and provincial legislation, judge–made law, professional and industry codes, guidelines and personal ethics. Not only are these existing sources of privacy protection complex and diverse (resulting in what is commonly referred to as a "patchwork" effect), but they generally lack the ability to effectively deal with emerging technologies. For example, most federal and provincial privacy legislation deals only with the protection of personal information or data. Moreover, with the exception of Quebec, which deals as well with the private sector, federal and provincial data protection legislation only applies to governments and government agencies. We are pleased, however, to hear that the Ministers of Justice and Industry are currently working with the provinces in an effort to introduce legislation that would protect personal information in the private sector across the country.

## YOUR VIEWS

As a Committee, we want to hear from Canadians on these issues. We want to know about your value systems and your ethical/moral frames of

reference in relation to privacy. We also want to know where this all fits in with today's high–tech society. It has been asserted that most Canadians are unaware of even the basic steps they can take to safeguard their privacy in this technological age. We want to know if this is the case and, if it is, the extent to which people want to safeguard their rights to privacy. We want to determine whether Canadians are actually aware that their privacy is in jeopardy. Have we all become technologically complacent and therefore blind to erosions of our privacy rights? Or, do we view privacy, not as an inalienable human right, but rather as a luxury that can, and in some instances should, be traded for the sake of other social or economic benefits?

## OUR APPROACH

Since privacy is such a wide–ranging right that is under siege in so many ways, the Committee has decided to focus its inquiry on three basic types of intrusive activities using case studies involving specific technologies:

1) **physical monitoring – video cameras,**

2) **biological surveillance – genetic testing,**

3) **personal identification practices – smart cards.**

In this way, we hope to raise awareness about the risks and benefits of advancing technologies, to stimulate debate about the need for greater privacy protection in this new age, and to test the limits (how far is too far?) of our vested privacy interests against both the present and future promises of new technologies. It is not, however, the Committee's intention to definitively resolve all of the issues raised by the three scenarios. Rather, it is hoped that the case studies will serve as a vehicle for testing our basic values, dealing with underlying trends and common themes, and ultimately developing some workable means of managing divergent interests.

## KEY ISSUES

The following are some basic questions that this Standing Committee would encourage Canadians to respond to:

1. In terms of your personal value system, where do you place the right to privacy? Is it, for example, as important as your right to free speech or your right to a fair trial?

2. Is the present system of privacy protection in this country working? If not, where are the trouble spots?

3. Based on your personal experience, to what extent are we sacrificing our right to privacy for the promises offered by emerging technologies? Is this an inevitable trade–off in a technological age?

4. What is the best method of safeguarding our privacy interests in a high–tech world? Do we need governments to take charge and enact strong and comprehensive privacy legislation, or do we need action taken on a number of fronts such as the development of private sector privacy codes by business and industry, the creation of privacy enhancing technologies, the launching of public education campaigns and the enactment of privacy protection legislation?

5. Are modern technologies being used, in some cases, as a "quick fix" for social or economic problems instead of getting to the root of these problems — for example, the use of video surveillance cameras on public streets to try to reduce the incidence of crime?

6. How should we all become better informed or educated about the impact of modern technologies and practices on privacy rights?

# CASE STUDIES

# VIDEO MONITORING CASE STUDY

## MAIN STREET, GOODTOWN

Goodtown is a small city, with a population just over 75,000. In the past few years, incidents of petty crime in the downtown core have been on the increase — especially vandalism, break–ins, and brawls after the bars close at night. The city has always taken pride in being a peaceful, safe, family–oriented place to live. Many citizens felt Goodtown might be heading for trouble, unless it dealt with the escalating crime problem quickly and effectively. After much debate, the city council decided to install a state–of–the–art closed–circuit television system (CCTV) to monitor Main Street's downtown section. Until that point, the only video surveillance cameras used in the city were set up by private security firms to guard retail stores and government office buildings.

Residents are divided in their support for video surveillance on Main Street. Most people, especially women and seniors, feel much more secure now going to restaurants, movies, and shopping after dark. Some people, however, who have had first hand experience with the long reach of the video cameras, are less than impressed. Take, for example, the experiences of Joan, Paul, Sonia, and Daniel.

## JOAN

Joan is a 16–year–old with boundless creative energy. On Halloween night, armed with a can of red aerosol paint, Joan decided to "paint the town red" — at least a few storefronts off Main Street. She knew enough not to try to leave her mark on Main Street, since the CCTV system would be sure to catch her in the act there. But she didn't realise the state–of–the–art cameras installed on Main Street could pan, tilt, zoom and see down the pitch black, adjacent side streets as clearly as if it were daylight, thanks to their night–vision capabilities. Joan's prank was recorded live by a 911 operator remotely monitoring the street from the central control room several miles away. The police were called, Joan was caught red–handed and is now facing criminal charges.

## PAUL

Paul lives outside Goodtown on a farm. He planned to attend a protest rally in front of the Agriculture Office on Main Street, until he heard about the

city's CCTV cost–recovery program. To recuperate some of the expenses incurred setting up its video monitoring system, the city decided to sell stock footage from its video surveillance cameras to anyone who was interested. Paul heard, through the rumour mill, that government bureaucrats and police officials intended to buy the videotape recordings of the protest rally. The digitised pictures taken of the protesters at the rally could be matched in a matter of seconds against the digitised photographs of licensed drivers held in the Transportation Department's data bank. Thus, most of the protesters would be quickly and accurately identifiable. Paul was outraged by this plan which he considered to be a major affront to both his freedom of expression and his freedom of peaceful assembly. But he didn't want to get into the government's bad books, so he stayed home.

**SONIA**

Sonia worked at the Agriculture Office until last month when she was fired. Her employer had a smoke–free workplace policy, so employees, including Sonia, would stand outside the front doors of their office building when they needed to have a cigarette. Her supervisor accused her of taking upwards of 10 cigarette–breaks each day, but Sonia denied the allegations, explaining that her absences from her desk were due to trips to the photocopier, the library, and other work–related tasks elsewhere in the building. She swore she only took three cigarette–breaks each day, until her supervisor confronted her with evidence to the contrary. He had obtained videotapes from the private security company that guarded the building and which had video cameras trained on the front doors as a security measure. The videotapes disclosed that Sonia spent, on average, one hour each day, not including her lunch hour, smoking outside the front doors of the building. Sonia was fired for taking too many breaks, as well as for lying to cover up her actions.

**DANIEL**

Daniel was laid off when the factory where he worked down–sized several months ago. Having learned his wife was terminally ill, facing no prospect of new employment, and with his unemployment insurance soon to run out Daniel fell into a deep state of depression. One night after having consumed far too many beers at a local tavern, Daniel staggered to his car parked on Main Street and struggled with the locked door. Once inside the car, instead of putting the key into the ignition he took the pocket knife attached to his key chain and slit his wrists. The 911 operator monitoring Main Street that night had tracked Daniel's unsteady stroll to his car and observed him fumbling with the keys. Before he had even slashed his wrists the operator had alerted the police about a

possible impaired driver. When they found Daniel collapsed over the steering wheel, they rushed him to the hospital. In retrospect, he is grateful that they saved his life. But, when the city sold the videotape footage of his suicide attempt to a national, reality–TV show, Daniel was hurt, angry and humiliated. He is contemplating suing the city.

## QUESTIONS FOR DISCUSSION

1. Are closed–circuit television systems (CCTV) an effective tool for deterring criminal activity, or do they simply displace that activity to areas that are as yet unmonitored and perhaps are also lacking in the financial and political clout necessary to secure these types of monitoring systems?

2. To what extent should video surveillance be done live versus taped? For example, should CCTV cameras be permitted to zoom in, tilt towards and record activities at any time, or only when an incident occurs? Who should make decisions to record and upon what basis?

3. Once a video tape is made, who is the owner of the recording and who is entitled to access it? Should practices or policies be in place pertaining to retention periods and the erasing of video footage? If so, who should make these determinations, the tape owner or user?

4. Are video cameras acceptable in public places because they are in essence simply an extension of the naked eye? What about when these cameras have high–tech infrared capabilities that allow them to see clearly in the dark, penetrate walls and zoom in on an individual 300 meters away?

5. If we accept at least a certain amount of surveillance in public places, where is the dividing line between the public and private sphere? What reasonable expectations of privacy should we be able to carry with us in private places (i.e., washrooms located in shopping malls with hidden video cameras to detect shoplifting)?

6. Does the whole question of privacy turn on the location of the invasion, on who is doing the invading, on the purpose for which the invading is being done, or on a combination of all of these factors?

7. How should the balancing of privacy rights with the benefits of new technologies be tackled in the area of video surveillance? Is there a need for overall regulation in this area? If so, how could this be achieved (i.e., a licensing system, an oversight body, a code of practice)?

8. How should we deal with future technological advances in the field of video monitoring? Moreover, how should we handle the heightened commercialization of personal information derived from such surveillance practices?

# GENETIC TESTING CASE STUDY

## THE SITUATION

Frank, a thirty–five year old truck driver for the Inter–city Moving Company, fell and hurt his left arm when he was delivering a load of furniture. The crew that was helping Frank called an ambulance and he was taken to the local General Hospital, a large teaching institution associated with The City University. They also advised Frank's boss, who owned the trucking company.

When Frank was being admitted to the hospital, he signed some forms that allowed the hospital personnel to conduct tests and to provide treatment. At the time, he was assured that these forms were quite routine, although the admitting clerk mentioned that because of the hospital's affiliation with the University, the forms contained a provision that gave consent to having medical information used in ongoing research carried out by the institution. Frank didn't pay much attention to this because he knew that he was there for the treatment of an injury, not an illness.

Because he had lost a considerable amount of blood, the hospital physician on duty, ordered a transfusion and to prepare for this, samples of Frank's blood were sent to the hospital laboratory in order to match his blood type. Because the doctor was conducting research into genetically transmitted illnesses he also ordered a DNA test — genetic screening of Frank's blood — as authorized by the consent form that Frank had signed when he was admitted. The blood samples were identified as Frank's both by name and by his provincial medical insurance number that was put on the requisition form by the doctor.

Frank called his boss and told him that he would be off work for six weeks. In the meantime, the boss had called Inter–city Moving's insurance company to find out what his liability might be. The insurance company, told the owner to ensure that copies of all documentation that related to the accident were forwarded to them. When Frank called to report in, his boss told him to get a copy of his record sent to the insurance company.

Frank was patched up and discharged the following day. Because he lived 300 miles away in Phillipstown, a village of about 2000 people, the

hospital agreed that follow–up care would be provided by his own doctor and by the homecare services there. When he was leaving the hospital, Frank asked the clerk that was handling the discharge to put a note in the computer record that his file should be sent to the insurance company.

The results of the genetic screening were available some time after Frank had gone home. They revealed that Frank had several genes that together might significantly increase his risk of developing heart disease at an early age.

## THE MEDICAL SYSTEM

Because the hospital had no special system to separate out the results of the genetic test, these were automatically entered into Frank's records in the hospital's computerized data bank along with the results of other tests and treatment of Frank's injured arm. Along with the blood sample that the hospital was storing for future research purposes, the data bank was available for use by the geneticists who were conducting research by using information provided by the hospital.

The records clerk at the hospital used his password, called up the file on his computer and distributed the test results as instructed in the file itself. He printed up several copies of the file and E–mailed another copy to the hospital physician. Without reading the file again, the doctor stored the information in his research data base. As a matter of routine, the medical report was mailed to Frank's family physician, who was to look after any follow–up treatment if required and also to the Phillipstown homecare coordinator who assigned a practical nurse, to visit Frank at home in order to change the dressings.

While his family doctor paid no attention to the report beyond looking at what had been done to treat Frank's injured arm, the homecare nurse read Frank's medical report carefully and suggestively told her supervisor — who was the best friend of Frank's wife, Elaine, — to have a look at it sometime.

## THE BANK

Two weeks later, Frank and Elaine, went to their bank to sign the papers applying for a $75,000 mortgage for the new house that they wanted to buy. They knew that they were stretching their financial limits, but the house was a good bargain and would accommodate them and the family they were planning to start. Frank decided that he would get the mortgage life–insured so that Elaine would be free of debt if anything happened to him. At the bank's request, Frank signed a standard form stating that he had no pre–existing

medical conditions that would disqualify him from getting the insurance. But the loans officer knew that Frank was off work due to his injury and asked for assurance that Frank would be back on the job soon and have ongoing employment and a stable income. In order to satisfy the loans officer, Frank volunteered to call his family doctor's secretary and ask her to forward a copy of his medical records to the bank.

A few days later, he opened a letter from his bank. In it, the loans officer explained that the bank had received Frank's file and went on to state that Frank was ineligible for the bank–sponsored, low–cost life insurance on his mortgage because he had a pre–existing medical condition related to his heart. The bank also informed him that it was rejecting his application for a mortgage because he had signed a false declaration.

## THE JOB AND INSURANCE

Later that same week, Frank was called in to see his boss. He was told that he had to look for another job. "I don't have enough work to keep you going," the company owner explained to Frank. In reality, however, the boss had been contacted by his insurance company which had analyzed Frank's medical records and decided that because he might have heart problems in the future, Frank was too high a risk for the company to insure. The boss decided that he would not tell Frank the real reason for the lay–off because he did not want Frank to try to claim disability insurance and possibly jeopardize the reduction in insurance premiums that was given to Inter–city Moving as a small businesses that had a record that was free of claims for five years.

Frank was not too downcast, however, because he had already been asked by another trucking company to consider a job with them. Actually, it paid more and, as he told Elaine when he called her at work to tell her the news, he didn't like his old boss anyway. All Frank needed to do was to get a medical and allow the company access to his medical records.

## THE FAMILY

Then Elaine arrived home, very agitated. She explained that she had had lunch with her friend the homecare supervisor. When Elaine told her friend about Frank's job problems, the friend had commiserated with her and said that she could explain because she had finally read Frank's file. She told Elaine that her husband had a heart condition that was inherited and that any of their children could have the same problem. Furthermore, he could die by the age of fifty and leave her alone with small children to raise. Why, Elaine wanted to

know, had her husband not kept her in the picture? Didn't she have a right to know?

## WHAT NEXT?

Totally bewildered, Frank said that this was news to him and tried to get his family doctor.

When he finally put together the pieces of the puzzle, Frank was angry. How could people get more private information about him than he had about himself? How could they get it without his understanding and consent? Why was he not given the opportunity to present his own personal information to his boss, his bank, his own wife? Frank was left with the knowledge that the information that was in the insurance company's files, in the bank's files and in general medical files (with his medical insurance number on it) was completely out of his control.

## QUESTIONS FOR DISCUSSION

1. Given the extremely personal nature of an individual's DNA, should the regulation of genetic information be treated differently than the regulation of other personal medical information? Should the government have the right and duty to collect genetic information to ensure a healthier society?

2. ° Who should be able to conduct genetic testing?

   - **For what purposes should collection of genetic data be allowed?**
   - **Who should be able to retain samples of DNA, for what purpose and under what conditions?**
   - **When genetic information is used for research purposes what should the obligation of the researcher be?**

3. Given what happened to Frank, should privacy issues arising from the use of genetic technology be dealt with by providing Frank with the opportunity to take legal action, after the fact, against the hospital, the hospital physician, his boss and his bank? Would it be better to provide for Frank's privacy proactively by prohibiting the collection and dissemination of genetic information altogether? Is there a middle road? What can Parliament do?

4. Who should be able to disclose genetic information and to whom? Should Frank's employer and the insurer have access to Frank's genetic profile? What about Frank's wife? What about Frank, himself?

5. To what extent should individual circumstances govern how genetic information is disclosed? For example, should it have made any difference if Frank had been perfectly "normal" as opposed to having an increased risk of a heart problem within the next few years? Would your view change if Frank had a gene that guaranteed the onset of a fatal illness (e.g., Huntingtons)? Should Frank's children be tested for his genetic predisposition even though they are underage? At what age should genetic testing be allowed for children?

6. Should Frank's consent when he was admitted to the hospital be enough to allow the collection of genetic information? What do you think constitutes "informed consent"?

# SMART CARD CASE STUDY

## NEW OCEANIA, 2004

Marie is a hard–working, model citizen of New Oceania who certainly never imagined herself living on "government handouts." In the spring of 2004, however, she found herself collecting unemployment assistance (UA) when her employer suddenly down–sized. Marie files her reports to receive UA benefits and collects the funds owed to her by using a smart card that functions as an ID card and an electronic–banking access card. The unemployment assistance card (UA card) was introduced by the government's Ministry of Work mainly to cut down on fraud and to save on the high cost of administering the old paper–based system.

## THE FINGER SCAN

Instead of filling out forms and mailing them in to receive benefits, which was the practice at the turn of the century, Marie files her request for UA benefits electronically, every two weeks, at a local government services kiosk. The kiosk computer scans her finger and translates her fingerprint pattern into a unique number, called a "digital fingerprint." At the same time, Marie slides her UA card into the terminal, so the computer can compare the number just generated by her finger scan with the digital fingerprint stored in the card. This comparison ensures that Marie, the person to whom the card was issued when she qualified to collect unemployment assistance, and the person filing her request for benefits at the kiosk are one and the same. Marie's digital fingerprint, being a unique number, is used as well to link the information recorded in her card and her full UA dossier which is housed in the Ministry of Work's central computer system.

At first, Marie was uneasy about the finger scanning process because it made her feel a little like a criminal. Now she is more used to it and appreciates that it is essential to verify her identity and to help cut down on fraud.

The UA card's identification technology, which establishes a card holder's ID based on a fingerprint (a physical characteristic which is unique in every individual) is known as "biometric" identification. The government

realised, in introducing its biometric UA card, that the information used for biometric identification purposes is very personal and, therefore, it must not be readily accessible to unauthorised or unscrupulous persons. Since Marie's card is always in her possession, she can control who gets access to it. As for the record of her digital fingerprint held in the Ministry's central computer system, the government protects this information from unauthorised use by keeping it in a separate, limited–access database.

## CASHING BENEFITS

In addition to being an identification card, Marie's UA card is an electronic–banking access card, that works like the magnetic stripe cards once issued by banks. The card gives her access, from any automatic banking machine, to the government's UA account and allows her to withdraw, in cash, up to the full amount of benefits owed to her. She doesn't have to withdraw her full entitlement as soon as it becomes available because the Ministry's central computer and her card both keep a running tally of the balance which she is owed. In this way, Marie and the government both know, at all times, the total of her outstanding benefits.

The UA card also can be used to make direct–payment purchases at any retail outlets which accept electronic–banking access cards. Information on every direct–payment transaction carried out using the card is recorded immediately on her card and simultaneously registered in the Ministry's central computer, to keep her running balance current.

Marie found her UA card to be very convenient and user–friendly. She could file a request for benefits directly and instantly, without having to rely on the post office to ferry her UA reporting forms back and forth; and when she was entitled to receive a UA payment, she could visit any banking machine, anytime, and withdraw the cash she needed. She did not have to wait for her cheque to arrive in the mail and then take it somewhere to get it cashed. She also did not need to carry much cash because she could use her UA card to make direct–payment purchases. Recent events, however, have caused her to question some of the uses made of the card.

## FRAUD CONTROL

First of all, following a trip abroad to look into job opportunities, Marie hit a snag filing her electronic report at the government services kiosk. Unknown to Marie, her digital fingerprint, held in the discreet UA database, had been automatically matched against the same finger pattern digitally scanned at

the airport when she cleared customs using her electronic border crossing card. In the process, the UA system was warned that she had been out of the country for five days. This information exchange was carried out pursuant to an information–sharing agreement between the Ministry of Tax (Customs) and the Ministry of Work.

When Marie tried to file her usual report, which required among other things that she confirm she had been available for work every day during the two–week reporting period, the kiosk computer advised her that she was "deemed" to have been unavailable for work for the five days that she spent outside the country. It then notified her that she had to appear before a Ministry of Work official within 10 days to prove that she had not attempted to file a false claim, which is a punishable offence. The computer also told her that if she could satisfy the official that she had not attempted to commit fraud, then her request for benefits for that period would be processed immediately.

## THE CONSUMER PROFILE

A few weeks later, Marie received a letter from XYZ Company, a private company contracted by the Ministry of Work to provide specialised training to UA recipients. The letter invited her to participate in a workshop called "Living Wisely on a Limited Income." Curious as to why she had been selected as a potential candidate for this training session, Marie telephoned the company and spoke to a representative who told her she probably had been contacted because of her "consumer profile." He went on to explain that the information about her direct–payment transactions, obtained from the UA database, had been compiled into a personal spending profile which showed unnecessary expenses, involving for example tobacco and alcohol.

The data trail left by Marie's direct payments made with her UA card did not accurately reflect her personal consumption habits. Marie had actually made the cigarette and wine purchases for her grandmother for whom she often ran errands. Not wishing to reveal any further details of her shopping habits to this stranger, Marie did not attempt to set the record straight. However, she did ask him whether the company sold her consumer profile to any direct–mail advertisers. (Lately she had received several personally addressed direct–mail advertisements from businesses selling products and services related to the items she often purchased for her grandmother and, in light of her conversation with this representative, she now suspected it was not a coincidence.) He confirmed that this was the company's practice and should she not want her personal information sold or traded, she would have to send him a request, in writing, to that effect.

## THE MURDER INVESTIGATION

The biggest shock, for Marie, came the day a police officer showed up at her door investigating a recent murder in a nearby park. The murder weapon had been wiped clean and discarded in a garbage can several blocks away. The police digitally scanned the fingerprints found on the lid of the can and matched them against a number of government databases, including the UA fingerprint database. Marie's prints were identified in the process and she was asked to account for her whereabouts on the night of the murder. Fortunately, she had spent the evening in question with her grandmother, so she had an alibi.

## THE NEW SUPER–CARD

Today Marie read a newspaper article on the Internet which reported that the Government of New Oceania intends to expand the functions of the UA card and transform it into a universal ID and multi–purpose, government–service card to be called the "universal–card" or "UNI–card." All workers, employed and unemployed, would be issued this card. For those eligible to receive UA, the card would continue to be used for electronic reporting and cashing of benefits. In addition, the card would introduce a host of new applications for employers and employees. For example, the government would give employers access to the card to record information on an employee's earnings and work history — data that would simplify and expedite the application process for persons seeking unemployment assistance. The card also would be used to prove one's citizenship, collect pension benefits, file income tax information and obtain tax refunds. The UNI–card, like the current UA card, would be a biometric identification card and, thus, offer solid proof of the card holder's true identity. As Marie scrolled to the next story, she thought about the unlimited potential of biometric smart cards and wondered whether one day she would need simply one card to conduct all of her personal transactions, with every level of government and all private businesses.

## QUESTIONS FOR DISCUSSION

1. Although Marie was uneasy about having her finger scanned, she had to submit to the process if she wanted to collect UA benefits. Use of the UA card system was made compulsory to maximise the government's savings.

    - **How do you feel about the physical intrusiveness of biometric identification — does it bother you or are you more concerned about how biometric information is stored and used, than how it is gathered?**

- **Given the sensitivity of biometric information, do you think we need clearer rules about who can ask for it, how those who collect it can use it and how it should be protected? For example, should government departments, the police, employers, banks, and insurance companies all be equally entitled to demand this type of information? Would you like to see sanctions, such as fines or imprisonment, imposed on persons who misuse or abuse this information?**

2. Marie's digital fingerprint, stored in the central UA computer, was kept in a separate, limited–access database. This data could have been made more secure with encryption technology, but the system's planners decided not to use encryption. They were confident that housing the biometric information in a separate data bank would provide enough protection. Encryption is a technological process whereby readable data, like a digitised finger pattern, is converted into a form that is indecipherable. Only authorised persons, who have access to the particular encryption program used to disguise the data, would be able to translate it back into a readable form. Technologies, such as encryption, which can be used to improve people's privacy, are called privacy enhancing technologies or PETs.

   - **What role should PETs play in protecting privacy? For example, where information systems handle sensitive personal information, such as biometric identifiers like fingerprints, should the use of PETs be mandatory?**

   - **By adopting a new PET called "biometric encryption," your fingerprint pattern could be used like a high–security lock to protect your personal data files instead of using it in the traditional, unencrypted form as a master–key that can unlock and link several of your data files — would you prefer to see your fingerprint pattern used as a lock or a master–key?**

3. When Marie was "deemed" not to have been available for work because the Ministry of Work was automatically notified that she had travelled outside the country, the presumption seemed to be made that she was trying to cheat the UA system. Some people might argue that this type of data matching is tantamount to executing a general search warrant against everyone who has personal information in the databases being matched.

   - In your opinion, should data matching be allowed to be carried out in a random fashion, just in case some evidence of fraud might be

uncovered? In a democratic society, is it fair and reasonable to search for evidence of wrong–doing in this way?

4. Marie's direct–payment purchases, made with her UA card, left a data trail which XYZ Company used to construct a consumer profile. The Company created the profile using the raw information that the Ministry of Work agreed to share with it. XYZ Company then capitalised on the inherent value of this information by repackaging it and selling it to direct–mail advertisers.

   - In our information society, should more steps be taken to prevent personal information from being shared or commercialised? For example, should people's data trails be made anonymous or should tighter restrictions be placed on information–sharing practices?

5. The phenomenon which privacy advocates call "function creep" occurs with ID cards when they take on extra uses which are above and beyond those originally contemplated by the identification system's developers. For example, many Canadians have experienced function creep in relation to their social insurance number. Retailers, landlords and others commonly request peoples' SIN so they can check their credit ratings at credit bureaus who use the SIN to link individuals to their credit information.

   - Should steps be taken to prevent function creep from happening with respect to smart ID cards? If so, what limits or rules should apply to these cards?

# BACKGROUNDERS

# VIDEO MONITORING BACKGROUNDER

## PHYSICAL MONITORING IN GENERAL

Physical surveillance, or the monitoring of human activity, is nothing new to our society. However, with the emergence of innovative and rapidly advancing technologies, modern surveillance has taken on a whole new character. It has expanded beyond the purview of national security and law enforcement, to include employers, commercial enterprises and service providers. It is no longer labour–intensive, cumbersome and costly. Surveillance technologies now have the ability to penetrate walls, function in the dark and operate from great distances. Moreover, information obtained through these monitoring techniques can easily be aggregated with other sources of information and manipulated with ease.

## CLOSED–CIRCUIT TELEVISION SYSTEMS (CCTV)

Although there are numerous modes of physical surveillance, none to date has surpassed the prevalence of video monitoring. Technical developments have both increased the capabilities and lowered the cost of video cameras, making them an almost regular feature of many city streets, heavily travelled highways, retail stores, banks, hospitals and even private homes. In particular, there has been a boom in the prevalence of closed–circuit television systems (CCTV). The cameras used in these systems are state–of–the–art. They can move in any direction, zoom in on minute objects up to 300 meters away, and bring images up to daylight level even in pitch blackness. The U.K. currently has centrally controlled, comprehensive city–wide CCTV systems tracking the movements of individuals in dozens of cities. In the U.S., police in Baltimore have wired a 16–block area of downtown with enough video cameras to allow them to watch and record activity on every street, sidewalk and alley 24 hours a day.

In Canada, the closed–circuit surveillance camera business is estimated to be somewhere between $65 and $90 million annually and growing. Not only are video cameras being used openly in public places by some municipalities and businesses, but retailers, employers and private individuals are taking advantage of low cost technological advances to conduct

surreptitious monitoring. Ironically, while it is illegal under the Criminal Code to intercept private conversations (i.e., "wiretapping" and "bugging"), there is no such prohibition against secretly taking photographs or videotapes that have no voice recordings. Moreover, only the police need obtain a warrant to videotape people's private activities. No prior authorisation is required for ordinary citizens, such as security guards.

## THE FUTURE OF VIDEO SURVEILLANCE

The future of surveillance camera technology appears awesome. Computerised facial recognition systems have been created that can take the image of a face caught by a surveillance camera and convert it into a computerised numerical sequence that can then be matched with facial images already held in computer databases. A company in Florida, for example, has developed powerful computing technologies that can scan a crowd at a rate of twenty faces a second, convert the faces into an electronic code and match them against identities already stored in a database. In Massachusetts, this technology has been used to develop a state–wide database containing the digitised photographs of 4.2 million drivers. One can only imagine the result were these technologies linked to a CCTV system.

Other examples of future technologies include hand–held devices (called Forward Looking Infrared Radar) that can look through walls to determine activities inside buildings with the accuracy and clarity of a video camera. Already passive millimetre wave detectors, a form of radar, can scan beneath clothing to assist law enforcement and customs officials in detecting concealed objects even within human body parts, such as the stomach.

## KEY ISSUES

So, in terms of video monitoring, there is more at issue than simply a question of whether our public and personal safety is ensured by having overhead video cameras tracking events in public places. The fear is that once the technology is in place, it opens the door to greater risks to privacy than were ever originally contemplated. Most of us would agree that there are definite benefits to be derived from some forms of physical monitoring. **The issue is where do we draw the line?** While this may be difficult, it may none the less be crucial given that with the current onslaught of technological developments, the ability to spy on one another will only become more effective, cheaper and pervasive.

## FOR FURTHER INFORMATION:

- House of Commons, Standing Committee on Human Rights and the Status of Persons with Disabilities, *Evidence*, 2nd Session, 35th Parliament, 3 December 1996. (Topic of discussion: Video Surveillance)
- Privacy Commissioner of Canada, *The Privacy Act – An Office Consolidation and Index*, Ottawa, 1995.
- Parts VI and XV of the Criminal Code.

# GENETIC TESTING BACKGROUNDER

Genetic information, a sub–set of health information is of increasing interest to public health care managers, to the insurance industry, and to employers. Apart from using it as forensic evidence in criminal investigations, there are several uses to which genetic technologies might be put:

1. genetic screening of a broad range of the population for a particular gene or combination of genes (e.g., cystic fibrosis, breast cancer, heart disease) to identify the presence of a single gene or combination necessary for a genetic illness

2. genetic testing (where evidence indicates the probability of the presence of a gene) to verify the likelihood of an individual developing a genetic condition (e.g., Huntingdon's disease)

3. genetic monitoring to ensure that individuals who are working in high–risk occupations (e.g., with chemicals) are not affected by their work environment

As the cost of gathering genetic information decreases, the pressure towards its more widespread use will increase. In the past, the high cost of DNA analysis has been as one of the constraints in more widespread use of this technology. But as the costs of carrying out this analysis decrease, some observers have pointed out that applied genetic research will make — or save — some businesses or institutions a lot of money. Insurance companies, private employers, governments and educational institutions all have an immediate, or potential, interest in promoting large–scale genetic screening to identify individuals carrying disease–associated genes. Economic pressures to apply genetic tests to broad sections of the population may increase as biotechnology companies develop and sell genetic testing products and services.

Because things are moving quickly in this area, it is time to consider possible consequences — such as discrimination — that might result from real or perceived differences from the 'normal' in a person's genetic makeup. This might occur in the workplace, in access to social services, insurance underwriting and the delivery of health care. American studies have uncovered cases where new, renewed or upgraded insurance policies were unobtainable

even if individuals labelled with genetic conditions had no evidence of — or assurance of — developing a disease associated with this genetic abnormality. People who are poor and uneducated, or those with fears about their job security, may not be willing or able to negotiate the complexities of the current legal and regulatory systems to secure their rights. Other individuals who are currently healthy may — consciously or unconsciously knowing the implications — refuse a genetic test and thereby suffer adverse consequences.

Data protection and privacy are serious concerns with regard to the collection and use of genetic information. This concern stems from the differences between genetic information and other personal information:

- Knowing about an individual's genetic makeup also provides information about relatives.
- All DNA information is contained in nearly every body cell.
- Genetic information not only provides certain knowledge about personal identifiers (height, build, skin colour, intelligence) but also information about possible behaviours.
- Individual genetic information cannot be altered.
- Genetic information can indicate what will (or may) happen to health in the future.

When the Standing Committee on Human Rights and the Status of Persons with Disabilities held Roundtables on genetic technologies, several questions, technical and practical, were raised:

- What can the science of genetics predict versus what it cannot predict? What is the level of understanding about the variable nature of many genetic conditions? (Some individuals with a genetic abnormality may never develop a disease, others may only develop the mildest form of a disease.)
- What is the difference between the predictive ability of genetics when dealing with a single gene disorder versus a multiple gene disorder?
- How many single gene disorders are there, compared to multiple gene disorders?
- What is the interaction between genetic factors and environmental and behavioural factors?

- What is the difference between treating an individual with a genetic condition (for example, Huntington's chorea) differently from an individual with a non–genetic predisposition to contracting an illness such as diabetes?

Though hundreds of diseases, for example Huntington's and haemophilia, are caused by a single faulty gene, each of these diseases is quite rare. Even if these genes were eliminated, some estimates put the effect on the world's 'disease burden', at less than two per cent.

With regard to most diseases, the contribution of faulty genes is less clear. A gene, for example, might be a necessary but not a sufficient cause of a disease. Sometimes an environmental factor might be needed to trigger the disease. Sometimes, more than one gene may need to be faulty for a disease to develop. In other cases, some forms of a disease might be genetic while other forms may not be (e.g., breast cancer).

Experts have pointed out that the very presence of a genetic technology "ups the ante" for the individual who may be subject to the test. Social or peer pressure, for example, to take such a test can result.

In his 1995–1996 Annual Report, Bruce Phillips, the Privacy Commissioner, stated that he believed that it was important to ensure than a DNA database does not become subject to what he called 'function creep.' By this, he meant resisting the pressure to keep adding to the list of offences for which testing is allowed. The same has been said of genetic screening and genetic testing. "The pressure to do just that is present in our society, a product of the very existence of technology and the belief that technology can solve all our woes, if only we let it." In addition, Mr. Phillips proposed that DNA samples be discarded to prevent unrelated secondary uses such as looking at genetic links to crime. This is also a concern in terms of genetic information entering large–scale data banks now used to store personal health–related information. Individuals' health profiles, which can include genetic conditions, may be available privately and may be accessed in a manner analogous to credit checks.

## FOR FURTHER INFORMATION:

- House of Commons, Standing Committee on Human Rights and the Status of Persons with Disabilities, *Evidence*, 2nd Session, 35th Parliament, 4 June 1996. (Topic of discussion: Human Rights and Biomedical Technologies)

- House of Commons, Standing Committee on Human Rights and the Status of Persons with Disabilities, *Evidence*, 2nd Session, 35th Parliament. (Topic of discussion: Privacy and Genetic Testing)

- Privacy Commissioner of Canada, *Genetic Testing and Privacy*, Ottawa, 1992.

- Privacy Commissioner of Canada, *The Privacy Act – An Office Consolidation and Index*, Ottawa, 1995.

# SMART CARDS BACKGROUNDER

## THE NEED FOR PERSONAL ID

The need for individuals to prove their identity to others is as ancient as civilisation itself. Over the centuries, as this need has grown, identification methods have become increasingly more sophisticated. The anonymity of today's large cities and the complexity of our daily transactions have made personal identification systems a necessity of modern life. The ability to accurately and reliably identify individuals is especially critical to governments, businesses, and other service providers, so they can operate efficiently, control fraud, and provide better quality services.

Simon Davies, who has written extensively on the topic of personal identification, notes that three basic methods of identification are used today: (1) identification by an object, such as a card or papers; (2) identification by something you know, like a personal identification number (PIN) or a password; and (3) identification by something that is part of your physical makeup, like your photographic image, fingerprint, voice or eye pattern. The latter form of identification, which relies upon an analysis of a physical characteristic of a person, is known as biometric identification. It is considered to be the most reliable of the three types of identification. At least two, and sometimes all, of these methods of identification are combined in the various advanced identification cards being developed and tested today.

## SMART CARDS

Smart cards are one example of an emerging high–tech card. They are being used and field–tested for a variety of applications in North America and appear, at this point, to have the potential to be adopted widely for personal identification purposes. A smart card is a card housing a micro–processor and memory storage space; thus, it is essentially a credit–card–sized, portable personal computer. It can calculate, encrypt, and record data. It can operate as a self–contained information system or interface with computer networks and centralised data banks.

Smart cards have a number of applications, including acting as: access cards or keys to buildings and equipment; stored–value cards which

serve as electronic cash; and personal data storage cards which can function as portable records systems, one example of which would be a patient's health smart card. A smart card may combine any or all of these three applications.

Contrary to a popular misconception, smart cards are not the same thing as magnetic stripe cards. The magnetic stripe card, the best known form of which is the credit card, can carry only a limited amount of information, such as the cardholder's account number, name and the card's expiry date, whereas a smart card can hold the equivalent of two to 20 pages of typescript or 50 times that volume if data compression techniques are used.

## WHAT MAKES PEOPLE UNIQUE

Personal identifying information is needed to establish or authenticate one's identity; it is a critical ingredient of all identification cards. Personal identifying information is what makes each person unique and distinctive. It may include, for example, one's date of birth, age, sex, height, weight, eye colour, address, DNA makeup, fingerprints, blood type, religion, or ethnic origin. The risk that someone, without proper authority, could access, disclose or use such confidential information is the most serious privacy concern associated with advanced identification cards. Ultimately, the success or failure of advanced card technology experiments may depend on whether the public can be persuaded that these cards can properly safeguard the highly personal information contained in them. For example, in the case of health smart cards, most cardholders probably would want to be certain that the confidential health records which they contain will only be accessible to the appropriate health care providers for medical treatment purposes and not be disclosed to outsiders, such as insurance companies or employers. Without proper assurances, people might resist voluntarily adopting the technology.

## SENSITIVE INFORMATION

Society's conviction that sensitive personal information warrants special protection from abuse is reflected in various data protection laws around the world. Strong and enforceable data protection legislation can offer an important degree of security; but legislation, alone, may not be sufficient to prevent abuses of the personal identifying information collected, generated, or disseminated using advanced card technology. Additional protection could be provided by other measures, such as raising public awareness about privacy rights and protections, encouraging the development of privacy enhancing technologies, building privacy considerations into the design and implementation of such technology, or conducting formal, independent privacy impact audits of new advanced card technologies.

High–tech, high–quality identification systems offer the potential to reduce fraud and promote greater administrative efficiencies — goals which are in everybody's interest. On the other hand, the identification systems that can best achieve these goals tend to be physically invasive and to depend on collecting very personal information. Most people probably would agree that this type of information warrants stringent protection. Therefore, the challenge, in the case of high–tech ID cards, is to make them ever more accurate and effective while guarding and preserving the confidentiality of the personal information they use. The question is how best to meet this challenge.

**FOR FURTHER INFORMATION:**


- House of Commons, Standing Committee on Human Rights and the Status of Persons with Disabilities, *Evidence*, 2nd Session, 35th Parliament, 10 December 1996. (Topic of discussion: Advanced Identification Cards)

- Rita Reynolds, "Privacy and Technology," Address at Technology Pathways to the Future — Bell and Government Connecting Canadians, 17 October 1996.

- Privacy Commissioner of Canada, *Privacy Framework for Smart Card Applications — A Discussion Paper*, Ottawa, July 1996.

- Privacy Commissioner of Canada, *The Privacy Act — An Office Consolidation and Index*, Ottawa, 1995.

- Ken McQueen, "After SIN: National Identity Numbers?" *The Gazette*, Montreal, 2 February 1997, p. A1 and A5.

# APPENDIX II

# List of witnesses

| Associations and Individuals | Issue | Date |
|---|---|---|
| **Access to Information Commission of Quebec**<br>Paul-André Comeau, Chairman | 3 | October 22, 1996 |
| **Adsum Consulting**<br>Charles Hitchfeld | 4 | March 11, 1997 |
| **Advanced Card Technology**<br>Catherine A. Johnston, President | 4 | March 12, 1997 |
| **Advocacy Resource Centre for the Handicapped**<br>Patty Bregman, Executive Director | 4 | March 12, 1997 |
| **AIDS Foundation of Canada**<br>Nathan Ganapathi, President | 4 | March 10, 1997 |
| **AIDS New Brunswick**<br>Elaine Sussey | 4 | March 13, 1997 |
| **Alberta Civil Liberties Association**<br>Rick Bennett, President<br>Brian Edy | 4 | March 11, 1997 |
| **Alberta Committee of Citizens with Disabilities**<br>Robyn Joffe | 4 | March 11, 1997 |
| **Alberta Community Development**<br>Joseph Forsyth, Director, Freedom of Information and Privacy | 4 | March 11, 1997 |
| **Alzheimer's Society**<br>Linda Leduc | 4 | March 12, 1997 |
| **Argenta Systems**<br>Don Specht | 4 | March 10, 1997 |
| **Assembly of First Nations (AFN)**<br>Alexandra Mackenzie | 4 | March 6, 1997 |
| ***Association coopérative d'économie familiale du centre de Montréal***<br>Jacques Santamant | 4 | March 14, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| ***Association des enseignantes et des enseignants francophones du Nouveau-Brunswick*** | | |
| Ronald LeBreton, General Director | 4 | March 13, 1997 |
| **Atlantic Association of Chiefs of Police** | | |
| Les Chipperfield, Deputy Chief | 4 | March 13, 1997 |
| **Atlantic Canada Opportunities Agency (ACOA)** | | |
| Claudia Gaudet | 4 | March 13, 1997 |
| **Bank of Canada** | | |
| Colleen Leighton, Corporate Security and Chief, Executive and Legal Services | 4 | March 6, 1997 |
| **B.C. Health Association** | | |
| Darren Kopetsky | 4 | March 10, 1997 |
| **B.C. Human Rights Coalition** | | |
| Peter Beaudin | 4 | March 10, 1997 |
| **B.C. Nurses' Union** | | |
| Leslie Burke | 4 | March 10, 1997 |
| Frank Gillespie | | |
| **B.C. People with Disabilities** | | |
| Tom McAulay | 4 | March 10, 1997 |
| Mary Williams | | |
| **B.C. Tel** | | |
| Vern Lillies, Corporate Security Director | 4 | March 10, 1997 |
| **Black White Communications Inc.** | | |
| Kate White | 4 | March 6, 1997 |
| **British Columbia Association for Community Living** | | |
| Joe Dickey | 4 | March 10, 1997 |
| **British Columbia Children's Hospital** | | |
| J.M. Friedman, President, Canadian College of Medical Geneticists | 4 | March 10, 1997 |
| **British Columbia Civil Liberties Association** | | |
| John Westwood | 4 | March 10, 1997 |
| Kay Stockholder | | |
| **British Columbia Federation of Labour** | | |
| Dennis Blatchford, Director of Community and Social Affairs | 4 | March 10, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **British Columbia Freedom of Information and Privacy Association** | | |
| Darrell Evans | 4 | March 10, 1997 |
| Els Mol, President | | |
| **British Columbia Human Rights Commission** | | |
| Mary-Woo Sims, Chief Commissioner | 4 | March 10, 1997 |
| **British Columbia Information Services** | | |
| Chris Norman, Director | 4 | March 10, 1997 |
| **British Columbia Public Interest Advocacy Centre** | | |
| Tim Timberg | 4 | March 10, 1997 |
| **British Columbia Transit** | | |
| Chris Harris, Director | 4 | March 10, 1997 |
| ***Bureau du protecteur du citoyen (Quebec)*** | | |
| Micheline McNicoll, Avocate déléguée du protecteur | 3 | December 10, 1996 |
| **Calgary Herald** | | |
| Catherine Ford | 4 | March 11, 1997 |
| **Canada Post Corporation** | | |
| Antoinette Deguida, Privacy Protection Officer | 4 | March 6, 1997 |
| **Canadian AIDS Society** | | |
| Rodney Kort | 4 | March 6, 1997 |
| **Canadian Association for Community Living** | | |
| Connie Laurin-Bowie | 4 | March 12, 1997 |
| **Canadian Banker's Association** | | |
| Margaret Eckenfelder, Regional Director | 4 | March 10, 1997 |
| David McInnes, Director of Government Relations | | March 12, 1997 |
| **Canadian Cable Television Association** | | |
| Bev Kirshenblatt | 4 | March 6, 1997 |
| **Canadian Civil Liberties Association** | | |
| Kenneth Swan | 3 | December 3, 1996 |
| | 4 | March 12, 1997 |
| **Canadian College of Medical Geneticists** | | |
| Peter Bridge | 4 | March 11, 1997 |
| **Canadian Council of Rehabilitation and Work** | | |
| Carl Schuler, Executive Director | 4 | March 11, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **Canadian Cystic Fibrosis Foundation** | | |
| Cathleen Morrison, Executive Director | 3 | December 5, 1996 |
| **Canadian Imperial Bank of Commerce** | | |
| Norman Howey, Director, Compliance and Privacy | 4 | March 12, 1997 |
| **Canadian Labour Congress** | | |
| David Onyalo | 4 | March 6, 1997 |
| **Canadian Life & Health Insurance Association** | | |
| Charles Black, Senior Advisor, Insurance Operations | 3 | December 5, 1996 |
| | 4 | March 12, 1997 |
| **Canadian Medical Association** | | |
| John Williams | 4 | March 6, 1997 |
| **Canadian National Institute for the Blind** | | |
| Debb Finn, CNIB National Office – Ottawa | 4 | March 6, 1997 |
| **Canadian Teachers' Federation** | | |
| Maria Moll, Head of Research and Technology | 4 | March 6, 1997 |
| **Canadian Union of Postal Workers** | | |
| Bob Curran | 4 | March 13, 1997 |
| Evert Hoogers, National Union Representative | | March 6, 1997 |
| Herb Moore | | March 13, 1997 |
| John Porter | | |
| **Canadian Union of Public Employees (CUPE)** | | |
| Richard Balnis | 4 | March 6, 1997 |
| Gordon Black | | March 13, 1997 |
| Adrian Charette | | |
| Terry Mullen (Local 865) | | |
| Margot Young | | March 6, 1997 |
| **Carleton University** | | |
| David Sutherland, Computing and Communications Services | 2 | June 11, 1996 |
| | 4 | March 6, 1997 |
| ***Chambre de Commerce du Québec*** | | |
| Michel Audet, Président | 4 | March 14, 1997 |
| **Children Hospital of Eastern Ontario** | | |
| Judith Allanson, Division of Genetics | 4 | March 6, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **City of Calgary** | | |
| Peter Copple | 4 | March 11, 1997 |
| Cal Johnston, Police Department | | |
| Murray Stooke, Police Department | | |
| ***Collège de Chicoutimi*** | | |
| Marcel Mélançon | 4 | March 14, 1997 |
| **Community Legal Assistance Society** | | |
| Frances Kelly | 4 | March 10, 1997 |
| **Consumer's Association of Canada – Alberta** | | |
| Wendy Armstrong | 4 | March 11, 1997 |
| **Consumers' Association of Canada – National Office** | | |
| Marnie McCall | 4 | March 6, 1997 |
| **Council of Canadians with Disabilities** | | |
| Diana Brent | 4 | March 11, 1997 |
| **Department of Justice** | | |
| Michael Zigayer, Criminal Law Section | 4 | March 6, 1997 |
| Fred Bobiasz, Criminal Law Section | 3 | December 3, 1996 |
| | 4 | March 6, 1997 |
| **Electronic Privacy Information Centre (EPIC)** | | |
| Marc Rotenberg, Director | 3 | October 24, 1996 |
| **Equality for Gays and Lesbians Everywhere (EGALE)** | | |
| Lawrence Aronovitch | 4 | March 10, 1997 |
| **Ethnocultural Council** | | |
| James Kafieh | 4 | March 12, 1997 |
| ***Fédération des Travailleurs du Québec*** | | |
| Émile Vallée | 4 | March 14, 1997 |
| ***Fédération nationale des associations de consommateurs du Québec*** | | |
| Marie Vallée, Telecommunication Analyst | 3 | December 12, 1996 |
| | 4 | March 14, 1997 |
| **Globe and Mail** | | |
| Jack Kapica | 4 | March 12, 1997 |
| **Government of Manitoba** | | |
| Gail Perry, Office of the Ombudsman | 4 | March 11, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **Government of New Brunswick** | | |
| Ellen King, Ombudsman | 4 | March 13, 1997 |
| Glenys McLaughlin, Information Technology Consultant, Corporate Information Management Services | | |
| Rebecca Moore, Department of Education | | |
| Claire Pitre, Office of the Ombudsman | | |
| Judy E. Ross, Information Technology Consultant, Corporate Information Management Services | | |
| Connie Taylor, Information Technology Consultant, Corporate Information Management Services | | |
| **Government of Nova Scotia** | | |
| Darce Fardy, Review Officer | 4 | March 13, 1997 |
| **Hamilton-Wentworth Regional Police** | | |
| Tim Fletcher | 4 | March 12, 1997 |
| **Health Law Institute** | | |
| Tim Caulfield, Research Director | 4 | March 11, 1997 |
| **Health Sciences Association of Alberta** | | |
| Elizabeth Ballermann, President | 4 | March 11, 1997 |
| John Vanderkaay, Director, Labour Relations | | |
| ***Hôpital Ste. Justine*** | | |
| Louis Dallaire, Department of Pediatrics | 4 | March 14, 1997 |
| **Hospital for Sick Children** | | |
| Joe Clarke, Department of Genetics | 4 | March 12, 1997 |
| **Human Rights & Employment Equity Consultants** | | |
| Bart Sackrule | 4 | March 12, 1997 |
| **Huntingtons Society of Canada** | | |
| Mary Shea | 4 | March 12, 1997 |
| **IBM Canada Ltd.** | | |
| Wayne Scott, Government Programs | 4 | March 12, 1997 |
| **Immigration and Refugee Board** | | |
| Larry Kearley | 4 | March 6, 1997 |
| **Industry Canada** | | |
| Stephanie Perrin, Special Policy Advisor, Long Range Planning and Analysis | 4 | March 6, 1997 |
| **Information and Privacy Commissioner of British Columbia** | | |
| David Flaherty, Commissioner | 3 | October 22, 1996 |
| Celia Francis | 4 | March 10, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **Information and Privacy Commissioner of Ontario** | | |
| Ann Cavoukian, Deputy Commissioner, Privacy | 1 | April 30, 1996 |
| | 3 | October 22, 1996 |
| | 4 | March 12, 1997 |
| Tom Wright | 4 | March 12, 1997 |
| **Information and Technology Access Office** | | |
| Eric Partridge, Corporate Strategies and Information | 4 | March 10, 1997 |
| **Insurance Corporation of British Columbia** | | |
| Steve Heather, Manager, Information and Privacy | 4 | March 10, 1997 |
| **Intercon Security Inc.** | | |
| Alan Bell, Manager, Corporate Resource Group | 3 | December 3, 1996 |
| Richard Chenoweth, Corporate Vice-President | | |
| **Law Society of British Columbia** | | |
| Kuan Foo | 4 | March 10, 1997 |
| ***Le GÉNÉTIQ*** | | |
| Marcel Mélançon, Director, "Groupe en génétique et éthique du Québec (Canada)" | 2 | June 4, 1996 |
| **Life Underwriters Association of Canada** | | |
| Edward Rothberg, Assistant General Counsel | 4 | March 12, 1997 |
| **Manitoba Association for Rights and Liberties** | | |
| Valerie Price | 4 | March 11, 1997 |
| **McGill University** | | |
| Dr. Abby Lippman, Department of Epidemiology | 2 | June 4, 199 |
| | 4 | March 14, 1997 |
| Trudo Lemmens, Researcher, Biomedical Ethics Unit | 3 | December 5, 1996 |
| Margaret Somerville, Professor, Faculty of Law | | |
| Sunny Handa, Centre for Medicine, Ethics and Law | 4 | March 14, 1997 |
| Marie-Claude Premont, Faculty of Law | | |
| **Media Awareness Network** | | |
| Jan D'Arcy | 4 | March 6, 1997 |
| **Ministry of Natural Resources** | | |
| John Boufford | 4 | March 12, 1997 |
| **Municipality of Metropolitan Toronto** | | |
| Rita Reynolds, Manager of Corporate Access and Privacy | 3 | December 10, 1996 |
| | 4 | March 11, 1997 |
| **Mytec Technologies Inc.** | | |
| George Tomko, President | 3 | December 10, 1996 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **National Anti-Poverty Organization** | | |
| Mike Farrell | 4 | March 6, 1997 |
| **National Computer Security Association** | | |
| Michel Kabay, Director of Education | 4 | March 14, 1997 |
| **National Federation of Nurses' Unions** | | |
| Kathleen Connors, President | 4 | March 6, 1997 |
| **NBTel** | | |
| Greg Belley | 4 | March 13, 1997 |
| **New Brunswick Aboriginal Peoples Council** | | |
| Sandra Splude, President | 4 | March 13, 1997 |
| **New Brunswick Federation of Labour** | | |
| Tom Steep | 4 | March 13, 1997 |
| **New Brunswick Human Rights Commission** | | |
| Janet Cullinan | 4 | March 13, 1997 |
| Constantine Passaris | | |
| Karen Taylor | | |
| Francis Young | | |
| **New Brunswick Information Highway Secretariat** | | |
| Bill Hall | 4 | March 13, 1997 |
| **New Brunswick Medical Society** | | |
| David Balmain | 4 | March 13, 1997 |
| Janet Maston | | |
| **Newfoundland/Labrador Human Rights Association** | | |
| Gerry Vink | 4 | March 13, 1997 |
| **North York General Hospital** | | |
| Anne Summers, Genetics Programme | 4 | March 12, 1997 |
| **Nova Scotia Human Rights Commission** | | |
| Mary MacLennan | 4 | March 13, 1997 |
| **Office of the Information and Privacy Commissioner** | | |
| Robert Clark | 4 | March 11, 1997 |
| John Ennis, Portfolio Officer | | |
| Frank Work, Director | | |
| **Office of the Privacy Commissioner** | | |
| Lorraine Dixon, Executive Director | 4 | March 10, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **Office of the Privacy Commissioner of Canada** | | |
| Ann Goldsmith | 4 | March 6, 1997 |
| Eugene Oscapella, Policy Advisor | 3 | December 5, 1996 |
| | 4 | March 6, 1997 |
| Brian Foran | | |
| **OMERS** | | |
| Claude Vaillancourt, Vice-President | 4 | March 12, 1997 |
| **Ontario Human Rights Commission** | | |
| Selwyn McSween | 4 | March 12, 1997 |
| **Ontario Medical Association** | | |
| Dr. Anne Summers, Former Chair, Committee on Bioethics | 2 | June 4, 1996 |
| **Ontario Nurses Association** | | |
| David Nicholson | 4 | March 12, 1997 |
| **Ontario Provincial Police Association** | | |
| Jim Drennan, C.E.O. | 4 | March 12, 1997 |
| **Ontario Teachers' Federation** | | |
| Wendy Matthews, President | 4 | March 12, 1997 |
| **Osmose Pentox Inc.** | | |
| Alex Gabanski | 4 | March 14, 1997 |
| **Ottawa Public Library** | | |
| Brian Clément | 4 | March 6, 1997 |
| Jean Martel | | |
| **Parent Finders of Canada** | | |
| Jim Kelly | 4 | March 10, 1997 |
| **Premier's Council for the Disabled** | | |
| Randy Dickinson | 4 | March 13, 1997 |
| **Price Waterhouse** | | |
| David McKendry, National Director, Consumer Affairs Reporting | 4 | March 6, 1997 |
| **Prince Edward Island Council of the Disabled** | | |
| Jessie Campbell, President | 4 | March 13, 1997 |
| **Privacy Commissioner of Canada** | | |
| Bruce Philips | 2 | June 11, 1996 |
| | 3 | November 21, 1996 |
| **Privacy International (U.K.)** | | |
| Simon Davies, Director General | 3 | October 24, 1996 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| ***Progesta Communications Inc.*** | | |
| Pierrôt Péladeau | 4 | March 6, 1997<br>March 14, 1997 |
| **Public Interest Advocacy Centre** | | |
| Andrew Reddick, Director of Research | 3 | October 12, 1996 |
| **Public Works — Alberta** | | |
| Sue Kessler, Director, Information Management and Privacy Branch | 4 | March 11, 1997 |
| **Quebec Human Rights Commission** | | |
| Daniel Carpentier | 4 | March 14, 1997 |
| **Queen's University** | | |
| Jerry Bickenbach, Department of Philosophy | 2 | June 4, 1996 |
| David Lyon, Department of Sociology | 4 | March 6, 1997 |
| ***Régie de l'Assurance-Maladie du Québec*** | | |
| Jean-Paul Fortin | 4 | March 14, 1997 |
| **Revenu Canada** | | |
| Stuart MacPherson, Manager, Programme Development Division, Travelers Directorate, Custom Border Services Branch | 3 | December 10, 1996 |
| **Roeher Institute** | | |
| Marcia Rioux, Executive Director | 2 | June 11, 1996 |
| Miriam Ticoll | 4 | March 12, 1997 |
| **Rogers Cablesystems Limited** | | |
| Pamela Dinsmore, Director, Regulatory Affairs | 4 | March 12, 1997 |
| **Royal Bank** | | |
| Christina Walpert, Manager, Human Resources | 4 | March 12, 1997 |
| **Royal Canadian Mounted Police** | | |
| André Thouin, Privacy Coordinator | 4 | March 6, 1997 |
| **Royal Ottawa Health Care Group** | | |
| Cathy Kerr, The Rehabilitation Centre | 4 | March 6, 1997 |
| **Saint Paul University** | | |
| Greg Walters, Centre for Techno-Ethics | 4 | March 6, 1997 |
| **SHL Systemhouse Inc.** | | |
| Rick Charland, Vice-President, Emerging Markets Canada | 4 | March 6, 1997 |
| **Simon Fraser University** | | |
| Ian Wojtowicz, Student | 4 | March 10, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| ***Société des Acadiens et Acadiennes du Nouveau-Brunswick*** | | |
| Micheline Doiron, General Director | 4 | March 13, 1997 |
| **St. Thomas University** | | |
| Andrea Bear Nicholas, Chair, Department of Native Studies | 4 | March 13, 1997 |
| Ron Byrne, Atlantic Human Rights Centre | | |
| Sheila Laidlaw, Third Age Centre | | |
| Josephine Lyman, Third Age Centre | | |
| **Stentor Resource Centre Inc.** | | |
| Bill Fisher, Manager – Smart Card Project | 4 | March 11, 1997 |
| **Sysnovators Ltd.** | | |
| Peter Brandon, President | 4 | March 6, 1997 |
| **Technology Industries Association** | | |
| David Hughes | 4 | March 10, 1997 |
| **Telus Communications** | | |
| Anne Coles, Regulatory Analyst, Regulatory Affairs | 4 | March 11, 1997 |
| **The Canadian Press** | | |
| Stephen Ward, Chief of Bureau | 4 | March 10, 1997 |
| **The Nizkor Project** | | |
| Ken McVay, OBC Director | 1 | April 30, 1996 |
| **The Province** | | |
| Joey Thompson | 4 | March 10, 1997 |
| **Treasury Board Secretariat** | | |
| Mary Ann Stevens, Senior Policy Officer, Information, Communications and Security | 4 | March 6, 1997 |
| **UNB Librairies** | | |
| Elizabeth Hamilton | 4 | March 13, 1997 |
| ***Université de Montréal*** | | |
| Bartha Maria Knoppers, Public Rights Research Centre | 2 | June 4, 1996 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| ***Université du Québec à Montréal*** | | |
| Pierre MacKay, Professor, "Département des sciences juridiques" | 1 | April 30, 1996 |
| René Laperrière, Professor, Département des sciences juridiques | 3 | November 26, 1996 |
| **University of British Columbia** | | |
| William Black, Faculty of Law | 2 | June 11, 1996 |
| Barb Arneil, Political Science Department | 4 | March 10, 1997 |
| Dr. Patricia Baird, Department of Medicine Genetics | 2 | June 11, 1996 |
| | 4 | March 10, 1997 |
| Richard Rosenberg, Department of Computer Science | | |
| **University of Calgary** | | |
| Gregor Wolbring, Department of Biochemistry | 2 | June 4, 1996 |
| | 4 | March 11, 1997 |
| Edna Einsiedel, Faculty of Social Sciences, 320 | 4 | March 11, 1997 |
| **University of New Brunswick** | | |
| Liz Burge, Netlearn Project | 4 | March 13, 1997 |
| Kirby Keyser, Computing Services | | |
| Mike MacDonald, Fredericton Freenet, Faculty of Computer Science | | |
| Rorey McGreal, Department of Advanced Studies | | |
| John McEvoy, Professor, Faculty of Law | | |
| David Townsend, Faculty of Law | | |
| **University of Ottawa** | | |
| Andrea Chia, Student | 4 | March 6, 1997 |
| Ronald Crelinsten, Department of Criminology | | |
| Geoffrey Gurd, Department of Communications | | |
| Genie Lyon, Student | | |
| Perez Nyamwange, Research Associate, Human Rights Research and Education Centre | | |
| Iffet Ozkut, Department of Criminology | | |
| Karen L. Rudner, Human Rights Research and Education Centre | | |
| **University of Toronto** | | |
| Jutta Treviranus, Manager, Adoptive Technology Support Group | 1 | April 30, 1996 |
| Calvin Gotlieb, Professor Emeritus, Department of Computer Science | 4 | March 12, 1997 |
| Liz Hoffman, University Ombudsperson | | |
| **University of Victoria** | | |
| Colin Bennett, Political Science Department | 4 | March 10, 1997 |

| Associations and Individuals | Issue | Date |
|---|---|---|
| **Vancouver Police Department** | | |
| Bob Rich, Sergeant | 4 | March 10, 1997 |
| **Vancouver Sun** | | |
| William Boei | 4 | March 10, 1997 |
| **Veteran Affairs** | | |
| Donna Cawley, Coordinator ATIP | 4 | March 13, 1997 |
| **Workers' Compensation Board** | | |
| Heather McDonald, Coordinator, FOI & Protection of Privacy | 4 | March 10, 1997 |
| **Youth Connexions Jeunesse** | | |
| Ivan Corbett | 4 | March 13, 1997 |
| **Yukon Human Rights Commission** | | |
| Richard D'Aeth, Commissioner | 4 | March 10, 1997 |
| **As Individuals** | | |
| Rob Botterell | 4 | March 10, 1997 |
| Arthur Cordell | 1 | April 30, 1996 |
| Roz Currie | 4 | March 10, 1997 |
| Lewis Eisen | | March 14, 1997 |
| Tim Falconer | | March 12, 1997 |
| Sarah Funston-Mills | | March 12, 1997 |
| Elliott Goldstein | | March 12, 1997 |
| Kelly Janssens | | March 13, 1997 |
| Colin Laughlan | | March 11, 1997 |
| Ian Lawson | 3 | November 26, 1996 |
| June Lewis | 4 | March 10, 1997 |
| Glennis Lewis | | March 11, 1997 |
| Murray Long | | March 6, 1997 |
| Mairi S. MacDonald | | March 12, 1997 |
| Camilla MacDougall | | March 13, 1997 |
| Michael Markwick | | March 10, 1997 |
| David Masse | | March 14, 1997 |
| Ron McKeown | | March 13, 1997 |
| Don McNaughton | | March 13, 1997 |
| Ken Rubin | | March 6, 1997 |
| Steven Skurka | 3 | December 3, 1996 |
| Antoine Soucsse | 4 | March 14, 1997 |
| Joan Vanstone | | March 10, 1997 |
| Frank White | | March 12, 1997 |

# APPENDIX III
# RECOMMENDATIONS

**RECOMMENDATION 1**

**The Committee recommends that the Government of Canada recognise and act upon its responsibility to respect and protect privacy rights in Canada by enacting a declaration of privacy rights to be called the Canadian Charter of Privacy Rights. This Privacy Charter would apply within federal jurisdiction, take precedence over ordinary federal legislation and serve as a benchmark against which the reasonableness of privacy infringing practices and the adequacy of legislation and other regulatory measures would be assessed.**

**Furthermore, the Committee recommends that the Canadian Charter of Privacy Rights be enacted no later than the 1st of January 2000.**

**RECOMMENDATION 2**

**The Committee recommends that the Canadian Charter of Privacy Rights declare and entrench fundamental privacy rights and the responsibilities attaching to these rights. These rights and responsibilities would include, but not necessarily be limited to, the following:**

**1. Fundamental Privacy Rights and Guarantees**

**1.1. Everyone is entitled to expect and enjoy:**

- **physical, bodily and psychological integrity and privacy;**
- **privacy of personal information;**
- **freedom from surveillance;**
- **privacy of personal communications;**
- **privacy of personal space.**

**1.2 Everyone is guaranteed that:**

- **these privacy rights will be respected by others adopting whatever protective measures are most appropriate to do so;**

- violations of these privacy rights, unless justifiable according to the exceptions principle which follows, will be subject to proper redress.

2. Justification for Exceptions

Exceptions, permitting the rights and guarantees set out above to be infringed, will only be allowed if the interference with these rights and guarantees is reasonable and can be demonstrably justified in a free and democratic society.

3. General Obligations

3.1. The basic duties owed to others to ensure their privacy rights are adequately respected include:

- the duty to secure meaningful consent;
- the duty to take all the steps necessary to adequately respect others' privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;
- the duty to be accountable;
- the duty to be transparent;
- the duty to use and provide access to privacy enhancing technologies;
- the duty to build privacy protection features into technological designs.

4. Specific Rights Related to Personal Information

- Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable.
- Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified.

5. Specific Obligations Related to Informational Privacy

5.1. The basic duties owed to others to ensure their informational privacy rights are adequately respected include, in addition to the general obligations set out above:

- the duty to hold sensitive personal information in trust;
- the duty to limit information collection to what is necessary and justifiable under the circumstances;
- the duty to identify the purpose for which personal information is collected;
- the duty to ensure the information collected is correct and of the highest quality;
- the duty to provide the people whose personal data is collected with access to that information and a means to review and, if they judge it necessary, to correct it;
- the duty to only use and disclose personal information for the purposes identified when meaningful consent was obtained;
- the duty to keep personal information only for as long as is necessary and justifiable;
- the duty not to disadvantage people because they elect to exercise their rights to privacy.

RECOMMENDATION 3

The Committee recommends that the Canadian Charter of Privacy Rights declare that to achieve proper respect for privacy rights in Canada the following measures are essential:

- on-going public discussion and input on matters related to the protection of privacy rights;
- research related to privacy rights and their protection;
- public awareness and education to sensitise everyone to their rights and responsibilities with respect to privacy.

RECOMMENDATION 4

The Committee recommends that the Canadian Charter of Privacy Rights declare that, to ensure the core privacy principles are observed, the following measures must be put in place:

- proper compliance, accountability and enforcement mechanisms;

- appropriate remedies to redress violations of privacy rights.

**The Committee further recommends that the Canadian Charter of Privacy Rights declare that the Privacy Commissioner of Canada shall exercise general oversight and protection of privacy rights within areas of federal jurisdiction.**

**RECOMMENDATION 5**

**The Committee recommends that the Minister of Justice, in consultation with the Privacy Commissioner of Canada, examine existing federal legislation and regulations, bills and draft regulations for consistency with the Canadian Charter of Privacy Rights and report any inconsistency to Parliament. This report shall be referred to the appropriate Parliamentary Committee for consideration and recommendations.**

**The Committee also recommends that the Canadian Charter of Privacy Rights require the Minister of Justice to notify the Privacy Commissioner of Canada of all bills tabled in Parliament and all draft regulations which may have ramifications for privacy.**

**RECOMMENDATION 6**

**The Committee recommends that the Government of Canada take a leadership role to ensure that Canadians' privacy rights are accorded equivalent dignity across the country. The Government of Canada should invite the governments of the provinces and territories to work together to develop a complementary and uniform approach to privacy protection across Canada that would accord with the Privacy Charter.**

**RECOMMENDATION 7**

**The Committee recommends that the Government of Canada, federal agencies and all Crown Corporations identify privacy issues in their respective workplaces and institute appropriate measures that accord with the Privacy Charter to safeguard employees' privacy rights.**

**RECOMMENDATION 8**

**The Committee recommends that the Government of Canada introduce into Parliament comprehensive data protection legislation to be known as the Data Protection Act to replace the current Privacy Act. This Act must accord**

with the Privacy Charter and apply to Parliament, all federal government departments, agencies, Crown corporations, boards and commissions, and other institutions, and to all federally-regulated businesses and industries. The Data Protection Act shall be enacted no later than the 1st of January 2000.

A broad and open process of public consultation shall precede the introduction of this legislation and provision shall be made in the Act for comprehensive public review of its provisions and operations within five years of the proclamation of the Act, and at regular intervals thereafter.

The Government of Canada shall give due consideration to other data protection models, such as the Canadian Standards Association's Model Code for the Protection of Personal Information and the New Zealand Privacy Act 1993, when developing the Data Protection Act. The Data Protection Act shall recognise the role of federally-regulated industries in the development of their own privacy codes.

RECOMMENDATION 9

The Committee recommends that the Data Protection Act it proposes contain:

- strict protections against all unnecessary intradepartmental and interdepartmental data matching;
- standards for acceptable data matching practices;
- acceptable data matching practices that comply with the Privacy Charter, in particular the principles of informed consent and transparency.

RECOMMENDATION 10

The Committee recommends that to comply with the proposed Data Protection Act, the Treasury Board Secretariat, a central agency of the federal government must:

- create mandatory data matching guidelines;
- monitor federal government departments for compliance with the new guidelines;

- educate federal departments and employees on what constitutes unnecessary data matching practices.

RECOMMENDATION 11

**The Committee recommends that the proposed Data Protection Act shall set out the circumstances under which data sharing between the federal and provincial governments is appropriate.**

**The Government of Canada should advise the provinces and territories that upon the enactment of the proposed Data Protection Act, all personal information shall only be shared with those provinces that have adequate data protection in place.**

RECOMMENDATION 12

**The Committee recommends that the proposed Data Protection Act must apply to:**

- any personal information transferred from federal government institutions to the private sector;
- any contracts for providing services to federal government institutions.

RECOMMENDATION 13

**The Committee recommends that:**

- the Treasury Board Secretariat take responsibility for monitoring compliance by federal departments and agencies with the proposed Data Protection Act;
- the Minister of Industry take responsibility for monitoring compliance by the federally-regulated private sector with the proposed Data Protection Act; and
- the federal Privacy Commissioner be made responsible for ensuring enforcement of the proposed Data Protection Act and that penalties exist in the proposed Act for violations of its provisions.

RECOMMENDATION 14

**The Committee recommends that the Data Protection Act regulate the development, testing (including pilot projects), implementation and**

application of emerging technologies that have a potential to infringe on the privacy of personal information. These technologies would include, but not be limited to, smart cards and biometric identification systems.

RECOMMENDATION 15

The Committee recommends that the Government of Canada take immediate action to deal with privacy violations and discriminatory treatment that may result from genetic testing including:

- a review of current policies and practices in the employment, health, insurance and criminal justice sectors;
- a review of existing reports and existing and proposed legal instruments (including the draft international covenant on the human genome);
- consultations with the public;
- the development of legislation that is necessary to deal specifically with the privacy and antidiscrimination issues related to genetic testing.

RECOMMENDATION 16

The Committee recommends that the Government of Canada introduce amendments to the Criminal Code that would, to the greatest extent possible, apply the prohibitions against the interception of private communications to surreptitious video surveillance.

RECOMMENDATION 17

The Committee recommends that the Government of Canada, in particular Industry Canada, encourage the development and use of privacy-enhancing technologies by:

- developing partnerships and creating incentives for research and development into privacy enhancing technologies;
- educating the public and businesses (large and small) about the capacity of privacy enhancing technologies to protect the personal information of Canadians.

**Recommendation 18**

**The Committee recommends that the Government of Canada undertake ongoing public awareness and education programs about new technologies and their impact on privacy to ensure that everyone is able to make appropriate decisions regarding their personal privacy and the direction of public policy in the future.**

**The Committee further recommends that the Government of Canada should undertake an ongoing public consultation process that examines and makes recommendations about specific legislative and non-legislative measures that are required to ensure that individuals' privacy is protected as technologies are refined or brought into use.**

**The Committee further recommends that the Government of Canada initiate ongoing discussions with the provinces with a view to encouraging a common approach to the treatment of these technologies (particularly genetic testing) within different jurisdictions.**

**RECOMMENDATION 19**

**The Committee recommends that the Government of Canada table in Parliament new legislation that would replace the current Privacy Act, to be called An Act Respecting the Office of the Privacy Commissioner of Canada. This Act would broaden and strengthen the mandate and powers of the Privacy Commissioner in relation to all issues of privacy within the federal sector. Specifically, it should contain, but not be limited to, provisions that empower the Privacy Commissioner to:**

- **receive, investigate and settle complaints of alleged privacy invasions;**
- **initiate his own privacy investigations through the use of privacy audits and technology impact assessments;**
- **carry out studies relating to privacy and emerging technologies;**
- **review all government bills, legislation, regulations, delegated legislation, policies and practices that may have an impact on privacy rights and, whenever appropriate, table a privacy impact statement before the House of Commons;**
- **ensure effective enforcement of the proposed Data Protection Act.**

**This Act shall apply to Parliament, all federal government departments, agencies, Crown corporations, boards, commissions and government institutions and to the federally-regulated private sector.**

**This Act shall contain complaint review mechanisms such as an administrative tribunal and the provision for judicial review.**

RECOMMENDATION 20

**The Committee recommends that the introduction of An Act Respecting the Office of the Privacy Commissioner must:**

- **be preceded by a broad and open public consultation process;**
- **provide for a comprehensive public review of its provisions and operations within five years of the proclamation of the Act and at regular intervals thereafter;**
- **assign a general public education mandate to the Privacy Commissioner.**

RECOMMENDATION 21

**The Committee recommends that Parliament provide sufficient resources to the Office of the Privacy Commissioner to adequately carry out its proposed responsibilities.**

# REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the Government table a comprehensive response to the Report within one hundred and fifty (150) days.

A copy of the relevant Minutes of Proceedings (*Issue No. 5, which includes this report*) is tabled.

Respectfully submitted,

The Hon. Sheila Finestone,
*Chair*

# Dissenting Report to the Report on Privacy Issues produced by the Standing Committee on Human Rights and the Status of Persons with Disabilities

Reform considers it essential for the government to be part of the growing debate over the impact of modern technology on privacy rights and was glad to participate in the recent review performed by the Standing Committee on Human Rights and the Status of Persons with Disabilities.

The opportunity the Committee afforded for Canadians to engage in the public debate was important. Reform, however, is compelled to dissent to the final report issued by the Committee on this study because of the lack of recognition given to the scope of opinion submitted by Canadians from across the country.

Many Canadians recognize the value of some form of regulation or legislation that recognizes the competing interests involved in this complex issue. Many groups, including Industry Canada, recommended a "multi-pronged" approach where responsibility is shared between the government and other interested parties. This would likely include a measure of self-regulation by businesses in the privacy domain.

Instead the government, in standard fashion, has chosen the most narrow and heavy-handed approach by opting to recommend consolidating all power in the federal government, and in particular, under the Privacy Commissioner, greatly expanding the role and responsibilities of the Privacy Commissioner without any apparent consideration of the costs involved or the efficiency of the process.

The Canadian Human Rights Commission (CHRC) seems to mirror many of the functions of the proposed expanded Privacy Commission, but has been ignored as either a source of experience or a possible mechanism for the regulatory process.

According to the government, privacy rights are not congruent with those rights addressed by the CHRC since they do not represent historically-defined discrimination.

However, if the government adjusts this qualification on the definition of the rights addressed by the CHRC, the Commission could then focus on real and present rights' violations. This would facilitate a more equitable approach to rights violations. And if privacy is an "inalienable human right" as it maintains, it could be included in the Commission's portfolio.

Another recommendation of the Committee has potentially serious ramifications on the constitutional distinctions between federal and provincial jurisdictions. In what appears to

be a very heavy-handed approach to enforcing privacy rights, the committee has recommended that federal governments cease data sharing with provinces unless the provinces implement reforms to privacy protection that meet the approval of the federal government. Thus legislation and regulation intended for application in the federal government and federally-regulated organizations will have much farther reaching implications.

The government's interest in enforcing privacy rights also rings hollow in view of its opposition to respecting property rights. With years of pressure and continuing inattention to the area of property rights, why is there now a will to exclusively pursue the related area of privacy?

Several bills illustrate "regulatory creep" and the government's disregard for property and privacy rights:

Bill C-68 significantly weakens Canadians' protection from search and seizure measures, increasing the ease of access of police officers to private property.

Bill C-71 also permits search and seizure without a warrant. While these two bills still maintain a measure of protection regarding dwelling places, Bill C-76, the *Drinking Water Safety Act*, of all pieces of legislation, goes even further. This bill, concerned with the regulation of bottled water, includes provisions for permitting access even to a person's home without a warrant. Little by little, the government is abandoning the historical rights and freedoms of Canadians while trying to claim the high ground by appearing concerned about new, complex issues that are more difficult to define.

Extreme proposals advanced in some circles on behalf of so-called children's rights have also found a friendly ear in some corners of the Liberal government. Such proposals, including the repeal of Section 43 or the privacy rights of children over and above the rights of parents, threaten the protection afforded to children and their families in the private sanctuary of the home. Such infringements threaten to destroy institutions and relationships Canadians have long taken for granted.

The violations of privacy made possible through more and more Liberal legislation sends a contradictory message to the recommendations proposed by the Committee on the limited scope of privacy issues addressed by the Committee. It suggests that the government lacks a comprehensive underlying philosophy that takes into account the priorities of Canadians and reflects the expected level of respect for their rights.

The Reform Party supports the involvement of the government in the public debate over privacy issues. The purpose of public debate, however, is to inform the government of the views and concerns of Canadians.

In consideration of the government report however, the Reform Party recommends greater responsibility and freedom be extended to individuals and businesses to choose and implement standards and measures that also respect the expectations of Canadians.

We recommend a re-examination of the singular proposal to use a greatly expanded Privacy Commission as the structure for the regulatory body.

Finally, we express our reservations over the rush in which the final report was produced which should have allowed more opportunity for careful examination of its proposals and their consequences. The Reform Party trusts that the public consultation proposed by the recommendations will produce results that do indeed represent the wishes and expectations of the broadest possible spectrum of Canadians.

# MINUTES OF PROCEEDINGS

TUESDAY, APRIL 22, 1997 (Meeting No. 44)

[*Text*]

The Standing Committee on Human Rights and the Status of Persons with Disabilities met *in camera* at 11:45 o'clock a.m. this day, in Room 208, West Block, the Chairman, Sheila Finestone, presiding.

*Members of the Committee present:* Jean Augustine, Maurice Bernier, Sheila Finestone, John Godfrey, Sharon Hayes, Russell MacLellan, Andy Scott and Georgette Sheridan.

In accordance with Standing Order 108(3), a study of Privacy Rights and New Technologies (*See Minutes of Proceedings of June 13, 1996, Issue No. 2*).

*In attendance: From the Research Branch of the Library of Parliament:* Susan Alter, Nancy Holmes and Bill Young, Research Officers. *Consultant:* Valerie Steeves.

It was agreed,—That the report be entitled: "Privacy: Where do we draw the line ?"

Il est convenu,—Que le titre du rapport soit: "La vie privée: où se trouve la frontière ?"

It was agreed,—That the report be adopted and that the Chair table the report in the House.

Il est convenu,—Que le rapport soit adopté et que la présidence le dépose à la Chambre.

It was agreed,—That the Committee request that the Government table a comprehensive response to the report within 150 days, in accordance with Standing Order 109.

Il est convenu,—Que le Comité demande au gouvernement de déposer une réponse globale dans les 150 jours suivant la présentation du rapport, en conformité avec l'article 109 du Règlement.

It was agreed,—That the Chair, in consultation with the research staff, be given the authority to make stylistic, grammatical and typographical changes to the report which do not affect the substance.

Il est convenu,—Que la présidente, de concert avec le personnel de recherche, reçoive l'autorisation d'apporter des changements stylistiques, grammaticaux et typographiques au rapport, sans en modifier la teneur.

It was agreed,—That 1,000 copies of the report be printed and that the report be prepared in alternate format.

Il est convenu,—Que 1 000 exemplaires du rapport soient imprimés et que le rapport soit préparé dans les formats de substitution.

It was agreed,—That the Committee hold a press conference following the tabling of the report and that the Chair and at least one member of each party participate.

Il est convenu,—Que le Comité tienne une conférence de presse à l'occasion du dépôt du rapport et que la présidence et au moins un représentant de chaque parti soient autorisés à y assister.

At 12:46 o'clock p.m., the Committee adjourned to the call of the Chair.

Wayne Cole
*Clerk of the Committee*