PRIVACY:

DISCUSSION PAPER #2

May 1998

TABLE OF CONTENTS

PRIVACY: DISCUSSION PAPER #2

EXECUTIVE SUMMARY

This is the second Discussion Paper on privacy that the Department of Justice has prepared recently. The first one, in July 1996, contained proposals for legislation to protect personal information in the possession of the government of New Brunswick. The Paper was referred to the Law Amendments Committee for public hearings. After those hearings, the Committee approved the proposals in the Paper, but also recommended that a second Discussion Paper should be prepared examining the extension of privacy legislation to the private sector.

This Paper is the result of that recommendation. Its purpose is to help establish whether the privacy of New Brunswickers requires greater protection than the law now provides, and if so, by what means. The Paper consists of "Propositions" for discussion rather than "Recommendations." Like its predecessor, it is to be referred to the Law Amendments Committee for review, so that the public may have a clear opportunity to contribute to the development of policy on this issue.

The Paper is in two Parts. Part I focuses on *Data Protection in the Private Sector.* "Data protection" deals with the establishment of rules to govern the handling of personal information that organizations collect and use in the course of their activities. New Brunswick's recently enacted *Protection of Personal Information Act* is a data protection Act for the public sector. The Paper asks whether data protection legislation is also needed in the private sector, and if so, what it should say.

Part II extends the discussion to *Privacy in General.* Data protection is just one part of the broader law of privacy; questions relating to the need for data protection legislation and what it might say depend in part on what already exists, or what might be established, under privacy law in general. There is also an important connection in terms of the focus of any legislative measures that might be taken to promote privacy interests. Is data protection the only, or the most pressing, area of concern? Examining privacy legislation in general, as well as its data protection sub-component, enables questions like this to be opened up for public debate.

In relation to data protection the Paper suggests that, as things now stand in Canada, the obvious starting point for private sector legislation would be the Canadian Standards Association's *Model Code for the Protection of Personal Information* ("the CSA Code"). The CSA Code is already the basis of New Brunswick's recently enacted *Protection of Personal Information Act.*

The Paper explains what the scope and content of legislation based on the CSA Code would be likely to be. The scope could be broad. The CSA Code is designed to apply to all commercial or non-commercial organizations, and this includes individuals when they collect and use personal information for commercial or other non-domestic purposes. "Personal

information," under the CSA Code, means any "information about an identifiable individual that is recorded in any form." This includes sensitive information as well as non-sensitive information. Every "organization" will almost certainly "collect" and "use" personal information, even if it does no more than maintain membership lists, customer or client information or employee records.

The Paper suggests that the key elements of the CSA Code for legislative purposes would be the Code's ten Principles. The Principles are broadly expressed, as is appropriate to the very wide range of situations to which they would apply.

Principle 1 -- Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Principle 2 -- Identifying Purposes
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 -- Consent
The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

Principle 4 -- Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 -- Limiting Use, Disclosure, and Retention
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

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

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

Principle 8 -- Openness
An organization shall make readily available to individuals specific information

about its policies and practices relating to the management of personal information.

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

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

The Paper discusses these Principles. In a few cases it suggests that small changes of wording would be required for legislative purposes, but the most important parts of the discussion relate to what Principle 2 means when it talks about "identifying purposes," what Principle 3 means by "consent" and "except where inappropriate," and what Principle 9 requires in terms of an individual's right to information. These are all things that the CSA Code describes in the Commentary that it attaches to its Principles. This Paper suggests that legislation, too, would need to deal with some of these things.

A recurring theme of the discussion is whether these Principles are as readily applicable in small organizations as in large ones. The CSA Code is stated as being intended to be applicable across the board, but several of its Principles are expressed in language that is more appropriate to large organizations than to small ones. For purposes of discussion, the Paper starts from the CSA Code's premise that it *should* be all-encompassing, and considers the areas which seem problematic from the point of view of small organizations. An important point for consideration is whether private sector data protection legislation, if adopted, should be as wide-ranging as the CSA Code aims to be, or whether a more focused approach is called for.

The Paper also deals with the enforcement of possible data protection legislation based on the CSA Code. It discusses whether penal remedies (prosecutions and fines), civil remedies (damages, declarations and injunctions) or administrative remedies (which could be of various natures, but would be available from an administrative entity rather than a court) might be appropriate. Contrary to what is often said in relation to data protection legislation, the Paper suggests that administrative remedies are not essential to a data protection Act. However, they are a policy option. Key issues in relation to possible administrative remedies are these. What powers of compulsion, if any, should be given to an administrative entity for data protection purposes? Should the resolution of complaints be the entity's only function?

Part II of the Paper, *Privacy in General*, focuses on the two central legislative options that are available to the Province if it wishes to reinforce existing legal protections for privacy

in New Brunswick at a general level. One is to establish a 'tort' of invasion of privacy. (A tort is a wrongful act which would entitle the person whose privacy had been invaded to go to court seeking the ordinary remedies of damages, declarations and injunctions.) The other is to create non-judicial remedies for infringements of privacy -- remedies that would be available from an agency other than the courts.

As to the tort option, the Paper describes briefly the existing legal remedies by which privacy interests may be protected, and then focuses attention on the *Uniform Privacy Act* prepared by the Uniform Law Conference of Canada. The Paper suggests that legislation establishing a tort of invasion of privacy in New Brunswick would be likely to be substantially similar to the *Uniform Act*. Several provinces have similar legislation already. The Paper discusses the *Act* as a possible model for legislation, and suggests that there are three key issues for public discussion. Should an invasion of privacy be a tort at all? Would legislation based on the *Uniform Privacy Act* adequately describe an invasion of privacy and pose no threat to desirable activities? Does caution dictate that any development of a tort of invasion of privacy should be left to the courts rather than undertaken by legislation?

Finally the Paper examines the possibility of establishing non-judicial remedies for infringements of privacy. The Paper starts by pointing out that there is a difference between the kinds of conduct that might that might amount to a tort, a wrongful act for which damages, declarations and injunctions could be available, and less extreme infringements of privacy. It mentions things such as video surveillance, workplace testing and workplace monitoring as examples of practices which, in some people's view, are symptoms of a progressive loss of individual privacy in today's society. The question is whether non-judicial avenues might be established as a means to addressing some of these privacy issues.

There may be different views on this. Privacy, though a thing that everybody values, is in some people's view best left to be dealt with as an issue in the purely social sphere. On this view, appropriate standards of respect for privacy emerge organically from social interaction; at any given point in time there will be some activities that raise questions about what the appropriate standards are, but in the long run the only true measure of what is acceptable is what persists. Some people may also feel that there is an incongruity in even considering administrative remedies -- a bureaucracy, they might call it -- for the purpose of protecting and promoting privacy.

There are, however, existing models of agencies with a privacy mandate. The Paper mentions examples, and notes that an agency with a broad privacy mandate could include data protection as one of its functions. The Paper suggests that the key issues for public discussion in relation to non-judicial remedies for infringements of privacy in general are much the same as they are in the specific case of data protection. Is a non-judicial avenue needed at all? Should its functions be exclusively complaints-oriented? Should it, or should it not, have compulsory powers? Of course, the answers to these questions might be different in the particular context of data protection as opposed to the broader context of privacy in general.

The items discussed in this Paper are both independent and potentially inter-dependent. Any one, or any two, or even all three of the approaches reviewed might form the basis for legislation designed to promote the privacy of New Brunswickers. On the other hand, some people may feel that there is no need for legislation at all.

The purpose of this Paper is to allow a full public debate on what the appropriate legislative choices should be.

In July 1996, the Minister of Justice submitted to the Legislative Assembly, for review by the Law Amendments Committee, a Discussion Paper entitled *A Proposed Privacy Act for New Brunswick.* The Paper made recommendations for the content of legislation to protect the privacy and confidentiality of personal information in the possession of the government of New Brunswick.

The Law Amendments Committee held public hearings in October and November 1996, and reported in February 1997. Its report made two recommendations. The first gave general approval to the proposals in the Discussion Paper. Legislation based on those proposals, the *Protection of Personal Information Act*, was enacted in February 1998; preparations for its proclamation will begin shortly. The Act will be referred to in the remainder of this paper as the *Public Sector Act.*

The Law Amendments Committee's second recommendation was this:

> RECOMMENDATION 2
> Your Committee strongly recommends that the government prepare a discussion paper forthwith, for referral to public hearings, with regard to the extension of privacy legislation to the private sector.

Explaining this recommendation, the Committee stated:

> Your Committee heard from various presenters that privacy legislation should apply not only to government bodies and agencies, but should be extended to the private sector. It was submitted that whether the body controlling personal data is within a government department or a private sector firm, personal information on private individuals must still be protected from inappropriate access.

The present Discussion Paper is prepared in response to the Law Amendments Committee's Recommendation 2.

A threshold question raised by the recommendation is whether the new Discussion Paper should adopt a broader or a narrower definition of its subject-matter. The 1996 paper was concerned with what is often known as "data protection" -- the establishment of rules to govern the handling of personal information that organizations collect in the course of their activities. On a narrow view, examining the extension of privacy legislation to the private sector would simply involve a discussion of private sector data protection legislation comparable to that in the *Public Sector Act.*

On a broader view, however, "privacy legislation" might go much further. A common analysis of privacy nowadays speaks of it as having three main elements: 'personal privacy', which is the privacy of one's body, 'spatial privacy', which is privacy in relation to one's

surroundings, and 'information privacy', which deals with who knows what about you and what they may do with it. Data protection falls largely within the realms of 'information privacy'; it is therefore just one sub-component of "privacy" in a broad sense. Documents such as *Privacy: Where Do We Draw the Line?* a 1997 report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, argue that it is privacy in general, and not just data protection, that is a matter of social concern and should be the subject of legislative action.

Though it might be possible for this Paper to restrict its attention to data protection legislation, it is preferable to consider the broader context of privacy law at the same time. There is an unavoidable connection between the two in relation to the remedies that might be established under data protection legislation; what would be needed would depend in part on what already existed, or might be established, under privacy law in general. There is also an important connection in terms of the focus of any legislative measures that might be taken to promote privacy interests. Is data protection the only, or the most pressing, area of concern? Examining privacy legislation in general, as well as its data protection sub-component, enables questions like this to be opened up for public debate.

This Paper therefore examines "privacy legislation" in a broad sense. It is organized in two Parts. Part I deals with *Data Protection in the Private Sector*. This is the direct and narrow continuation of the 1996 discussion paper and the *Public Sector Act*. This Part invites comment on the question of whether data protection legislation for the private sector is desirable, and to assist in the discussion it sets out the possible content of legislation on the subject. The model used is based on the Canadian Standards Association's *Model Code on the Protection of Personal Information* (hereafter "the CSA Code") and on the *Public Sector Act*, which itself draws heavily on the CSA Code.

Part II, *Privacy in General*, examines existing legal remedies in New Brunswick for invasions of privacy, and asks whether further legislative measures are called for. Two main questions are considered. The first is whether New Brunswick should follow the example of several Canadian provinces (though not all) in establishing legislation which makes an invasion of privacy a specific 'tort' in its own right. A 'tort' is a wrongful act for which an aggrieved individual can seek remedies in the courts; the typical remedies are damages, declarations and injunctions. The second is whether remedies for infringements of privacy might be provided through agencies other than the courts. Various options are mentioned, including the possibility that the mandate of the New Brunswick Human Rights Commission might be expanded to include a role in privacy protection along with the Commission's existing anti-discrimination functions. Both the judicial and the non-judicial options considered in Part II would, if adopted, apply across the board, not only to the private sector but to the public sector as well.

This Paper does not make specific recommendations on the various topics it considers. Instead, it presents a number of propositions for discussion. Many of these are detailed and could provide the basis for legislation if the present consultation indicates that legislation

along those lines is appropriate. At present, however, no decisions have been taken. Options range from enacting no legislation, through various selections or combinations of the items discussed, to legislating on all of them together. This Discussion Paper aims to assist in determining what the appropriate policy choices should be.

I. Data Protection in the Private Sector

This Part of the Paper asks two questions: "Is there a need for private sector data protection legislation?" and "If so, what should it say?" The two questions are closely connected. The more that can be said about the likely content of the legislation, the better informed the arguments for or against it will be.

Conveniently, this Discussion Paper is being prepared at a time when a single document, the CSA Code, dominates the debate in Canada about data protection in the private sector. The Code was developed for the Canadian Standards Association by a Technical Committee made up of representatives of the federal government, industry, privacy commissioners and advocacy groups. The Code was developed as a voluntary one, which private sector organizations could adopt if they chose, and which they could modify to suit their own particular requirements if they saw fit. Subsequently, however, it has attracted attention as the possible basis for legislation, rather than pure self-regulation. The federal gvernment is promoting this position. It has stated its intention to have data protection legslation in place for the federally-regulated private sector by the year 2000, and its recently released consultation paper, *The Protection of Personal Information: Building Canada's Information Economy and Society* (January 1998), places the CSA Code at the centre of the discussion. Several Information and Privacy Commissioners in Canada are among those who have commented favourably on the CSA Code as a basis for legislation.

It is not yet clear, however, that any consensus about the substance of the CSA Code will convert itself into a consensus for legislation based on it. Though industries represented on the CSA's Technical Committee have, in some cases, developed their own industry codes based on the CSA Code, few of them have positively advocated the formalization of the Code into legislation. Even where there is support for legislation in principle, there is a desire to see exactly *how* the CSA Code would be turned into law before that support is made concrete.

This need for clarity makes it convenient that New Brunswick's *Public Sector Act* has been prepared at the particular time that it has. The Act, which is set out in Appendix B, is squarely based on the CSA Code. It therefore provides a specific example of how legislation inspired by the CSA Code might be constructed. It is a model, furthermore, that could easily lend itself to extension to the private sector if the present consultations determine that this is the right course to take.

That, though, is the question at the heart of Part I of this Paper: *whether* extending comparable legislation to the private sector is the right course to take. There is a big difference between the government adopting legal rules to govern its own conduct and imposing similar rules on everybody else. There are many Acts in New Brunswick that create special rules for the operations of the public sector. They deal with things such as hiring practices, purchasing practices, public finances and pay equity, to name just a few. Many of these Acts establish rules that do not *need* to be in legislative form; legislating them is, in effect, a means of giving added weight to a policy commitment. Arguably data protection

rules might fall into this category. Arguably, also, there may be special factors relating to the activities of the public sector, as opposed to the private sector, that make it more important in the public sector that laws, rather than policies, govern the use of personal information. The fact that the *Public Sector Act* is *capable* of being extended to the private sector does not necessarily mean that it *should* be. The appropriate policy and legislative choices for the two sectors may well differ.

A. Is there a need for private sector legislation?

Data protection legislation is in large measure a response to the increasing computerization of society. As information can be more and more easily amassed and manipulated, concern is expressed that organizations may have too much information about individuals, with too few controls on what they may do with it. The concerns are expressed differently at different times and in different contexts. The recent federal consultation paper, with its focus on electronic commerce and "making Canada the most connected nation in the world" (p.1), says this:

> The challenge of the electronic age is that with each transaction we leave a data trail that can be compiled to provide a detailed electronic record of our personal history and preferences. The digitization of health, education, employment and consumer records makes it possible to combine information and create an individual profile with data that most of us consider to be extremely personal. This information may be sent across provincial and national boundaries where it can be sold, reused or integrated with other databases without our knowledge or consent. (p.2)

Other descriptions might broaden the perspective to include other forms of information-gathering, not just electronic ones, and other uses to which information can be put, not just consumer profiling.

In response to this, data protection laws attempt to establish a set of 'fair information practices' for organizations to follow. The rules relate to what kinds of personal information organizations can collect, how long they can keep it and what they can do with it. The rules also give individuals a right of access to, and correction of, information about themselves. The general purpose of the rules is to assert the individual's continuing interest in the information that organizations obtain about him or her, and in what they do with it. The aim is to make it clear that the information is not simply the organization's information, to do with as it will.

Data protection legislation applying to both the public sector and the private sector has been adopted in most European states. For members of the European Union such legislation is mandatory under Directive 95/46/EC (hereafter the "EU Directive").

Outside Europe, however, data protection legislation in general is less well established, and private sector data protection legislation particularly so. Legislation from Hong Kong and

New Zealand, applying to both the public and the private sectors, was reviewed during the preparation of this Paper. The Department of Justice is informed that Taiwan and Israel also have such legislation in place. In other countries which have data protection legislation (e.g. Japan, Australia and the United States) the focus is on the public sector.

In Canada, Quebec is unique in having data protection legislation for both the private and the public sectors. Elsewhere (with the exception of Newfoundland and Prince Edward Island) there is public sector legislation alone, though the public sector is defined more broadly in some places than in others. In British Columbia, for example, the legislation extends to bodies such as the governing bodies of self-regulating professions. Manitoba has recently enacted legislation dealing specifically with the handling of "health information," whether in the public or the private sector.

Meanwhile the federal government has committed itself to enacting data protection legislation for the federally-regulated private sector by 2000, and it is encouraging the provinces to develop matching legislation for provincially-regulated activities. The federal government's recent consultation paper mentions that forums such as meetings of Information Highway Ministers and Consumer Affairs Ministers are being used for discussions of the subject. It also mentions that a *Uniform Data Protection Act* is being developed by the Uniform Law Conference of Canada, a conference at which delegations from the various jurisdictions attempt to develop model legislation on matters on which harmonization of provincial laws is desirable.

Among the incentives to the federal government's activity in this area is the EU Directive. Adopted in October 1995, the Directive requires all member states of the European Union to have data protection legislation in force by October 1998 that meets the standards set out in the Directive. One of those standards is that member states must prohibit the transfer of personal information to non-member states unless an "adequate level of protection" for the information exists there (Art.25), or unless, in the absence of that, the person transferring the information "adduces sufficient guarantees," by contractual clauses or otherwise, for the protection of the particular information transferred (Art.26). The recent federal consultation paper says that "This Directive has the potential to make protection of personal information a major non-tariff trade barrier with Canada" (p.8).

The argument in favour of extending data protection legislation to the private sector can conveniently be taken from an address by Allan Rock, then the federal Attorney General, to the International Conference of Data Protection Commissioners in Ottawa in September 1996. When the federal government had first enacted data protection legislation, he noted, it had done so for the public sector alone; at that time government was by far the main collector, storer and user of information on individuals. Subsequently the government had moved to advocating data protection in the private sector too, though by means of voluntary self-regulation. Since then, however, it had reconsidered its view that self-regulation for the private sector was sufficient:

We have done so because it is obsolete. Modern information technology has made it infinitely more feasible for businesses and other private institutions to amass and exchange data -- within and across borders. Advances in computer and networking technology have multiplied and magnified the challenges to privacy.

Meanwhile, Canada has been evolving rapidly from a resource-based economy to one based on information and knowledge. In this environment, more and more private institutions are collecting, using, and exchanging information about our consumption habits and services.

In this situation the Government of Canada takes the position that the protection of personal information can no longer depend on whether that data is held by a public or private institution. This does not mean that the rules governing the collection, use, communication and disposal of personal information need to be exactly the same for every individual and organization. It does mean that they should be based on a common set of principles. And it means that personal information held in the private sector should be protected by law.

There are, however, differing views on this. In Australia the Commonwealth (i.e. federal) Attorney General's Department issued a discussion paper in September 1996 examining the expansion of data protection legislation to the private sector. In 1997, though, it was decided not to take this step. The stated reasons were concern over the compliance costs for businesses, large and small, and the need to reduce the regulatory burden rather than to add new compulsory regimes. Since then there has been consultation in Australia on a national voluntary scheme for self-regulation, leading to the recent release by the Commonwealth Privacy Commissioner of *National Principles for the Fair Handling of Personal Information* (February 1998).

In the United States, too, discussions to date at the federal level have not apparently led to the conclusion that wide-ranging data protection legislation is required. In *Options for Promoting Privacy on the National Information Infrastructure*, a consultation paper issued in April 1997 by the Information Policy Committee of the National Information Infrastructure Task Force, legislated data protection was mentioned as an option, but only as one among several. The paper also referred to arguments that acceptable market standards and practices were evolving and should be left to do so, or that legislative solutions should be applied, in the future as they had been in the past, to particular problem areas as they arose rather than on a comprehensive basis. Wide-ranging private sector data protection legislation for the private sector does not appear to be in prospect in the United States at present.

Here, then, is the background to this first broad question of "Is there a need for private sector data protection legislation?" On the one hand there is concern that, especially with modern information technology, too much personal information is available to too many people, with too few controls over what they may do with it. There is the desire to establish at least a general framework of basic principles that reflect the individual's continuing interest

in the information that organizations possess about him or her, and there is the belief that legislation is the only effective way of establishing a common framework that will be generally respected.

On the other hand there is concern about both the substance of the proposed rules and about their practical impact on the organizations that will have to observe them. As to the substance the concern is that the legislation may create obstacles to desirable activities. As to the practical impact, the complaint is that the legislation may impose excessive administrative burdens and other costs. Doubt is also expressed about whether there is really enough of a problem in relation to the handling of personal information to justify a legislative solution.

These are all issues on which input is required from the general public and from interested parties. It seems unlikely that there will be any major disagreement about the broad principles that private sector data protection legislation would be designed to promote: that personal information should not be gathered or used inappropriately, and that, subject to reasonable limits, individuals should be able to discover and correct what organizations know about them. Opinions may be more varied, however, as to whether legislation is the right way of advancing those principles, as to whether the legislation would actually achieve its objectives and as to whether, on balance, more would be gained or lost by adopting it. Expressions such as "inappropriately" and "subject to reasonable limits" are easy to use in abstract statements of principle. They can become controversial, however, when one ultimately confronts the concrete question of what, exactly, is or is not "inappropriate," or is or is not a "reasonable" limit.

Proposition #1

The general objectives of data protection initiatives are laudable. Key questions for public discussion are

(a) whether legislation is the right way of advancing those objectives,

(b) whether legislation would achieve its objectives, and

(c) whether its benefits would justify the costs and restrictions it imposed.

B What might data protection legislation say?

The mere mention of things like the effectiveness of legislation and its costs and benefits emphasizes the importance of providing the specifics of possible legislation, at least tentative ones, in order to give respondents to this Paper something solid to react to. Fortunately, the combination of the CSA Code and the *Public Sector Act* provide a good framework for a detailed discussion of what private sector data protection legislation might

say. In the current state of the debate in Canada, the CSA Code is the obvious starting point for the development of possible legislation.

Proposition #2

Possible data protection legislation for the private sector should take the Canadian Standards Association's *Model Code for the Protection of Personal Information* as its starting point.

How closely, though, should data protection legislation follow the CSA Code? Some explanation is needed here of the structure of the Code. It consists of ten Principles and six Definitions, with a Commentary on each of the Principles, and in two instances, an explanatory Note. The Notes are important. Their purpose is to explain how the key Principles on "Consent" and "Individual Access" are to be applied when competing imperatives such as the protection of public health or security are at issue. These Notes, the Code explains, are considered to form an "integral part" of the Principle to which they relate (para.3.1.2).

One approach that has been suggested to establishing data protection legislation based on the CSA Code is simply to adopt the Code in its entirety. According to a paper presented at the 1997 meeting of the Uniform Law Conference of Canada, that would be the preference of some of the people who have been involved in the consultations on the subject. The mechanism would presumably be a form of legislative cross-reference, as is done from time to time with CSA technical standards.

This does not appear to be the right approach to general legislation governing the protection of personal information. If there is to be legislation on the subject, it is because there are important social values to assert, and if there are, the Legislature should express them directly rather than by reference to a non-statutory code. This is even more the case if one of the advantages of adopting the CSA Code by cross-reference is, as some proponents of this method apparently suggest, that doing so would make it easier to update data protection standards as the CSA Code is revised and improved with the benefit of experience. The implication is that the CSA's judgments on appropriate standards of data protection over time would become authoritative. It is doubtful that this would be appropriate.

If, then, legislation should not simply adopt the CSA Code by reference, what should it do? Carrying forward the entire text of the Code into legislation does not seem possible. Much of the Commentary, in particular, is expressed in terms of explanation, description and examples, and would be out of place in a legislative text. The result is that data protection legislation that takes the CSA Code as its starting-point must at best be selective, carrying forward into the legislation those parts of the Code that belong there, and leaving other material out.

The ten Principles of the CSA Code, its basic statement of 'fair information practices',

are the central feature of the Code and can be adopted virtually verbatim as the basis of the legislation. This is what the *Public Sector Act* has done. Part of the reason for following the text of the CSA's Principles so closely is that the consensus they represent was apparently a delicate one and was not easily attained. The paper presented to the Uniform Law Conference's meeting in 1997 suggested that the consensus might evaporate if data protection legislation adopted different wording. The CSA Code has also been adopted by the Standards Council of Canada as a National Standard of Canada. Though *some* changes in the wording of the Principles seem to be required if the ten Principles become law, the changes are minor. The details and the explanations are given in the pages that follow.

As for the Commentary, the Notes and the Definitions, these are best viewed as source material in determining what needs to be added to the CSA Principles in data protection legislation in order to give sufficient guidance as to how the Principles are to be interpreted and applied. In the *Public Sector Act*, the ten Principles are placed in Schedule A as a "Statutory Code of Practice," and a Schedule B is added dealing with "Application and Interpretation of the Statutory Code of Practice." Private sector legislation could proceed in similar fashion.

Proposition #3

Data protection legislation should adopt the ten "Principles" of the CSA Code verbatim, as far as possible. The "Definitions," "Notes" and "Commentary" in the CSA Code should serve as source material for data protection legislation, with key elements being adopted as appropriate.

B.1 The scope of data protection legislation

As was noted on p.1 of the Department's 1996 discussion paper, there are two preliminary matters that together determine the scope of a data protection Act: "To whom will the Act apply?" and "What is meant by 'personal information'?"

a. To whom will the Act apply?

In the 1996 discussion paper, this was a relatively straightforward issue. The discussion paper only dealt with the provincial government, so all that had to be decided was how the provincial government should be defined. A listing of "government bodies" was the approach recommended. When one moves beyond the public sector, however, the issue becomes less clear. There are many kinds of organization to which 'private sector' data protection legislation could apply. Commercial enterprises are obviously one. However, non-profit organizations such as charities, churches, political parties and trades unions may also collect and use personal information. They are likely to possess at least such things as membership lists and personnel files, which are 'personal information' that must be maintained in accordance with data protection principles. Even within the strictly commercial

sector, there may be questions as to how or whether data protection legislation should apply to operations such as small family businesses or single person professional practices.

The CSA Code is expressed in terms of what "organizations" must do, and "organization" is defined broadly, as including "associations, businesses, charitable organizations, clubs, government bodies, institutions, professional practices, and unions" (para.2.1). In context that definition is of limited significance. The CSA Code is a *voluntary* one; it only applies to those organizations that choose to subject themselves to it. Nonetheless, a broad definition along these lines seems appropriate, even in a legislative context that *imposes* obligations on anyone who comes within the definition. Most organizations, even small ones, possess personal information, and even in small organizations some of that information may be sensitive and susceptible to misuse. Single-person professional practices such as doctors will possess individuals' medical records. Small businesses like corner stores may possess things such as records of people's video rental habits -- misuse of which led in the USA to enactment of the *Video Privacy Protection Act 1988*. Data protection legislation must be careful not to impose on small organizations levels of obligation that they cannot reasonably be expected to attain -- a point to which this Paper will return periodically -- but at the present stage of this discussion it seems better to proceed on the basis that organizations of all kinds and sizes may be included in the legislation.

One point that the EU Directive makes, though, and seems worth stating, is that data protection legislation does not apply to the activities of "a natural person in the course of a purely personal or household activity." A clarification along these lines seems necessary once one says that data protection legislation might apply to an individual when acting in a business capacity in his or her own right. In such a case one must differentiate the commercial activities of the individual, to which the legislation would apply, from the personal ones, to which it would not. The EU Directive makes the necessary distinction.

Proposition #4

Data protection legislation could apply to all incorporated and unincorporated organizations, and to individuals when they collect and use personal information for purposes other than personal and household ones.

The EU Directive contains the further qualification that, while data protection legislation must apply to all "automatic" (i.e. computerized) processing of personal information, it only needs to apply to "manual" processing where the personal information forms part of a "filing system" -- i.e. "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." Similar to this is the provision in the Quebec legislation that makes 'establishing a file' on a person the triggering point at which the law will begin to apply.

The CSA Code does not differentiate manual and automatic records systems, nor does it expressly adopt a criterion of 'establishing a file' on an individual. On this point the present Discussion Paper will follow the CSA Code. Given that the objective is to explore

the CSA Code as the basis for private sector data protection legislation, it seems more natural to start where the Code starts, and see where that leads. If it turns out that the result is too broad, and that this could be remedied by including some concept of 'establishing a file', that concept could probably be incorporated.

b. What is meant by "personal information"?

The CSA Code contains a definition, and it is a fairly conventional one. Personal information means "information about an identifiable individual that is recorded in any form" (para.2.1). S.1 of the *Public Sector Act* is identical in substance, and adds in s.1(3) the clarification that

> An individual is identifiable for the purposes of this Act if
>
> (a) information includes his or her name,
>
> (b) information makes his or her identity obvious, or
>
> (c) information does not itself include the name of the individual or make his or her identity obvious but is likely in the circumstances to be combined with other information that does.

Two features of a definition of this sort should be underlined. The first is that "personal information," does not have to be sensitive or particularly private information. It merely needs to be "information about an identifiable individual." To that extent the definition, and thus the scope of the legislation, is broad.

It is narrowed, however, by the requirement that the information be "recorded in any form." Personal information would not come within the scope of the legislation unless some form of a record of the information is made. It would be possible, of course, for legislation to be more encompassing than this. Part III of Ontario's (public sector) Freedom of Information and Protection of Personal Information Act, for example, extends data protection principles to personal information which does not exist in a recorded form. Adopting this approach would widen the scope of the legislation. On the other hand, the reference to "files" in both the EU Directive and the Quebec legislation, referred to above, appears to be a little narrower. For present purposes, however, the CSA's definition appears to be relatively standard, and this Discussion Paper will follow it.

Proposition #5

Data protection legislation could adopt the CSA Code's definition of personal information: "information about an identifiable individual that is recorded in any form."

B.2 The CSA Principles

The next several pages will analyze the CSA Principles as the possible elements of a statutory code of practice. The discussion will look at each of the Principles in turn. In a few cases minor changes of wording will be suggested, but in all cases the major question will be whether the Principle would need to be supplemented, in data protection legislation, by additional material designed to govern its interpretation and application. Once the Principles have been reviewed, other key elements of a legislative package based on the CSA Code will be examined. Enforcement of the legislation is the major element here. This is something that the CSA Code did not have to deal with, because of its voluntary nature, but which legislation must.

In considering the Principles, the broad definitions of "organization" and "personal information" must be borne in mind. The Principles are designed to apply to all organizations, whether small or large, to light users of personal information as well as heavy ones, and to all kinds of personal information, whether sensitive or not. The Principles therefore set out a broad framework for a wide variety of situations. Their application in specific cases will often require the exercise of judgment by the organization in question.

CSA Principle 1 - Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

The purpose of this principle is to state each organization's responsibility for making the legislation work, and to make sure that in every organization *somebody* is clearly assigned that task. There are, however, some practical issues raised by the way in which the principle is worded. One is that the Principle may leave open the possibility of there being a gap in 'accountability' unless and until the organization takes the positive administrative step of 'designating' somebody. Another is that the Principle applies more naturally in a large organization than a small one. In a small organization (which under Proposition #4 may be no more than a single individual) it will sometimes seem odd to speak of "the organization" as "designating an individual" to be accountable for compliance with the Code.

In the *Public Sector Act* the first problem was dealt with by amending the wording of CSA Principle 1 to make the "chief executive officer of a public body, and his or her designates," accountable for compliance. The second problem did not arise, because "public bodies," though some are actually surprisingly small, all have an organizational structure in which a "chief executive officer" (by whatever official title) can be readily identified.

In the private sector, where organizational forms may be more diverse, a slight variant of this approach is required. The legislation should establish a default position which should apply unless and until the "organization" takes positive steps to alter it. If the organization has an identifiable Chief Executive Officer, that person should initially be accountable for

compliance with the legislation. In organizations with a less clear internal administrative structure, a comparable default position would be to place accountability for compliance with the data protection principles on the person or persons who control the activities of the organization. In most cases it should be obvious who fits this description. Occasionally, though, it may not be. An example might be a three-person partnership where the partners had equal voting rights. In a case such as this it would be the partners collectively who controlled the activities of the organization. Under the suggested default rule, therefore, the partners collectively would be accountable for compliance unless and until they made some other "designation".

Proposition #6

Unless and until a designation is made under CSA Principle 1, the person accountable for an organization's compliance with the data protection principles should be

(a) the organization's Chief Executive Officer, if it has one; or

(b) in an organization without a Chief Executive Officer, the person or persons who control the affairs of the organization.

CSA Principle 2 – Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

The idea that the "purposes" for which personal information is collected should be "identified" is one of the central principles of the CSA Code and of other data protection documents. The identified purposes become key to decisions under CSA Principles 4 and 5 about what pieces of information an organization should collect and what it can do with the information once collected. There are, however, both conceptual and operational challenges connected with the identifying of purposes.

A small point that can be disposed of quickly is the question of whether there are limits on the purposes for which organizations can collect personal information. The CSA Code is entirely open-ended on this. By contrast, the *Public Sector Act* (Sch.B, para.2.1), along with the comparable legislation of other Canadian provinces, specifies that public bodies can only collect personal information for purposes that directly relate to the activities of the public body. A similar restriction should be acceptable in the private sector too.

Proposition #7

The purposes for which an organization collects personal information must be legitimate and must directly relate to an existing or proposed activity of the organization.

More complex are some issues relating to what 'identifying purposes' really involves. Studying the CSA Code suggests that there are really two aspects to this. One is a purely internal process, in which an organization identifies *to itself* why it wishes to obtain personal information. The other is an external process, which relates to what the individual must be told about the purposes of the collection. On the face of things, CSA Principle 2 applies more naturally to the latter. However, the Commentary complicates this. It adds that an organization "shall document" its purposes, thus emphasizing the *internal* aspect of the identification of purposes. It is less categorical, though, about what kind of *external* explanation must be given to the individual. Para. 4.2.3 says that "The identified purposes should be specified at or before the time of collection to the individual from whom the information is collected," but the use of the word "should" is both deliberate and significant. Para. 3.1.3 points out that the use of the word "should" indicates a "recommendation" as opposed to a "requirement."

In the *Public Sector Act* CSA Principle 2 (which is Principle 2 of the Statutory Code of Practice in Schedule A) is considered to be substantially a requirement for an 'external' explanation of purposes, but not necessarily a formalistic one. In the ordinary nature of things, most collections of personal information will be accompanied by at least *some* indication of why the organization wants the information. Perhaps this might be as little as a brief introduction to a conversation or to a letter. A requirement to "identify purposes" in this sense does not seem over-burdensome.

Schedule B of the *Public Sector Act* also contains a requirement that public bodies "document, in relation to any personal records system, the purpose or purposes for which the information in the system is held" (para.2.2). A personal records system is defined as "a computerized or manual records system that contains information about individuals and is structured in such a way as to permit information about specified individuals to be easily recovered" (para.2.3). Under this definition, virtually any organized repository of information about individuals (in the plural) will be a "personal records system". Documenting the purpose for which the information in the system is held effectively attaches that purpose to the use of the information in the system.

Would a similar obligation to "document . . . purposes" be appropriate in the private sector? Its advantage is administrative clarity, especially in large organizations where it would help to establish a shared understanding of what information can be collected and of the uses to which it can be put. In small organizations, however, there is a danger that a general duty to document purposes may merely create an administrative obligation that contributes little to the privacy of the individual. Is it really worthwhile, for example, to require a formal 'documentation of purposes' by an organization such as an individual businessperson when the purposes for which he or she holds personal information are obvious and he or she is the only person who will be using it? Even in large organizations, some people might argue, 'documentation of purposes' will normally occur in practice without the need for a formal requirement to be imposed by the legislation.

Proposition #8

CSA Principle 2 could be supplemented by a requirement that organizations document the purposes for which they maintain personal records systems, but if it is, such a requirement should not apply where documentation would be superfluous to proper administrative controls.

One point which the CSA Code does not deal with is this. What happens if, in particular cases, the internally documented purposes do not match the explanation that is given to the individual? In such a case it would be the explanation that was given to the individual that must prevail. The use that could be made of the information would depend not on the 'documented' purpose that the organization had failed to explain adequately, but on the explanation actually given, and what the individual could properly be considered to have 'consented' to (in the sense described under CSA Principle 3, below) in the light of that explanation.

This would not mean that an organization that is collecting personal information must, in all cases, mechanically recite to the individual the 'internal' purposes as the organization has centrally documented them. Though in some cases this might be relatively straightforward and appropriate, in others it might not. It is likely, for example, that an organization's documented version of its purpose will be expressed in general, and perhaps bureaucratic, language. If so, reciting it may have little explanatory value. In other cases doing so will be merely stating the obvious -- perhaps because the individual's approach to the organization has clearly established the context in which the information is requested and given. More often, perhaps, whatever purpose may be documented internally will be accompanied by some other explanation more directly tailored to the particular contact between the organization and the individual. Perhaps different explanations may be better at different times or for different pieces of information. It does mean, however, that the onus is on the organization to ensure that whatever it identifies internally as being its purposes must be adequately explained to the individual, by whatever means the organization chooses to do so, if it wants to be sure that its 'documented' purpose will actually match what it is permitted to do in accordance with the 'consent' of the individual.

Proposition #9

Where an organization's documented purposes do not match the explanation given to the individual, the latter should prevail, in accordance with CSA Principle 3 -- Consent.

CSA Principle 3 -- Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

There are three key issues arising under this principle. The first relates to its wording. The second relates to the issue of "implied consent" as opposed to "express consent." The third relates to determining when a requirement of consent is "inappropriate".

a. Wording

CSA Principle 3 refers to "knowledge and consent" as being required not only for "collection" but also for "use and disclosure". Para.4.3.2 of the Commentary makes it clear that the expression "knowledge and consent" was used deliberately. There is, however, an inconsistency of language with CSA Principle 5, which also deals with "use and disclosure" but which only requires "consent," not "knowledge and consent."

In a legislative text, inconsistencies of this sort should be avoided. The best way of doing this is to remove the words "knowledge and" from CSA Principle 3. In relation to "collection," nothing seems to be lost by doing so, since "consent" is the broader term; it is hard to see that one can "consent" to a collection without having "knowledge" of it. In relation to "use and disclosure," by contrast, it would be problematic if both "knowledge" *and* "consent" were required as separate criteria. One can presumably "consent" to a use without ever "knowing" whether it actually occurs. If "knowledge" here were an *additional* requirement, the result would be to impose an obligation which could be difficult to meet.

Proposition #10

The essence of CSA Principle 3 is "consent." Data protection legislation should not include "knowledge" as a separate and independent criterion which must be satisfied.

b. Express and implied consent

The CSA Code makes it clear that "consent" may be express or implied (para.2.1). The paragraph continues:

> Express consent is consent given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual. (Para.2.1)

The idea of implied consent seems essential to a workable data protection statute. To require express consent for every collection, use or disclosure of personal information would be impossible. When an individual requests a service, for example, there is only an implied consent, not an express one. Consent might also often be implied when an organization took action for the benefit of the individual. Implied consent is especially important to legislation based on the CSA Code. Unusually among the data protection documents that have been reviewed in the preparation of this Paper, the CSA Code does not explicitly allow organizations the flexibility of using information for a purpose that is "consistent with" the purpose that is actually identified to the individual. In the conceptual framework of the CSA

Code it is apparently the notion of "implied consent" that must cover the ground that, in other codes, is addressed through the statutory authorization to act for "consistent purposes."

The CSA Commentary suggests that it is the "reasonable expectations of the individual" (para. 4.3.5) that are the key to determining when "implied consent" exists. This seems an acceptable approach. It rightly focuses attention on what *the individual* should expect to be done with the information he or she provides, rather than on what the organization might consider reasonable from its own point of view.

Proposition #11

Data protection legislation must include the concept of implied consent, based on the reasonable expectations of the individual.

Is it necessary for data protection legislation to explain "implied consent" more extensively than by simply referring to the "reasonable expectations of the individual"? It would be impossible to give an exhaustive definition, but the *Public Sector Act* contains a provision that expands on the idea in two ways. It states that an individual must be "unlikely to disapprove of" an action if consent is to be implied, and it sets out the major factors that a public body should take into consideration. The following Proposition is taken directly from Sch.B, para.3.2 of the *Public Sector Act*, with a few minor changes of expression:

Proposition #12

The actions for which consent can be implied should be those that the individual should reasonably expect the organization to take, and would be unlikely to disapprove of, having regard to

(a) the nature of the personal information in question, including whether it is or is not sensitive or confidential,

(b) any benefit or detriment to the individual,

(c) any explanation that the organization has given of its intended actions,

(d) any indication that the individual has given of his or her actual wishes, and

(e) the ease or difficulty with which the actual wishes of the individual might be discovered.

c. "Except where inappropriate"

Principle 3 requires consent for collection, use or disclosure "except where inappropriate". In its Note to Principle 3 (which "forms an integral part of the principle" -- para 3.1.2) the CSA Code continues:

> In certain circumstances personal information can be collected, used or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate where the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information. (para.4.3)

The concept of "except where inappropriate" is one of the trickiest to set out in legislation. Canadian public sector data protection Acts bear ample witness to difficulty of the task. Over the years they have developed increasingly long lists of permitted non-consensual collections, uses and disclosures. These include some substantial and obvious provisions, such as permitting disclosure to protect the health or safety of another individual. They also sometimes include provisions that raise more questions than they answer, such as disclosure to legal counsel. It seems surprising that disclosure to one's legal counsel should need express authorization under the Act. And if it does, what does this imply about possible disclosures to other professionals or consultants that the Act does not expressly mention? The lists in the existing Acts also normally include a general provision permitting collection, use or disclosure without consent if the public interest clearly outweighs any invasion of privacy that may result.

The *Public Sector Act* makes an effort to shorten the list, and to rely on general statements rather than specific ones. It also adopts a two step approach, so that a public body must satisfy itself not only that it is acting for a specified purpose but also that the action it is proposing is justified in the circumstances. The following Proposition is based on the comparable provisions of the *Public Sector Act* (Sch.B, paras.3.4 to 3.7), with some small changes of terminology, and with the omission of para.3.5, which provides for disclosures in the interest of open government and is specific to the public sector.

Proposition #13

Consent should not be required when an organization collects, uses or discloses personal information

(a) to protect the health, safety or security of the public or of an individual,

(b) for purposes of an investigation related to the enforcement of an enactment,

(c) to protect or assert its own lawful rights, including lawful rights against the individual,

(d) to verify to a government body the individual's eligibility for a program or benefit for which the individual has applied to that body,

(e) for purposes of legitimate research in the interest of science, of learning or of public policy, or for archival purposes,

(f) as required or expressly authorized by law, or

(g) for some other substantial reason in the public interest, whether or not it is similar in nature to paragraphs (a) to (f).

Before collecting, using or disclosing personal information without consent an organization should consider the nature of the information in question and the purpose for which it is acting, and must satisfy itself that in the circumstances that purpose justifies the action proposed.

Any collection, use or disclosure of personal information without consent should be limited to the reasonable requirements of the situation.

Proposition #13 does not, on its face, differentiate between collection, use and disclosure because CSA Principle 3, to which it relates, deals with the three things together. In practice, however, the different elements of Proposition #13 would have different impacts for different organizations, depending on their activities and the particular decisions they had to reach. For example, few private sector organizations would collect information for the purposes of enforcing an enactment; this would not 'directly relate to their activities' under Proposition #7. Similarly, private sector organizations might rarely have a "substantial reason in the public interest" for disclosing personal information, yet it seems important to keep the possibility open -- to ensure, for example, that they could at least disclose the information to the responsible public authority. Use of "personal" information for research purposes is also likely to be unusual, since normally the information could and should be used in an anonymous format and would therefore not be personal information within the meaning of the CSA Code.

CSA Principle 4 -- Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

The *Public Sector Act* sets out the sources from which personal information can be collected. These are (a) from the individual, (b) from another person with the individual's consent, (c) from a source and by means available to the public at large, and (d) from any

source in cases in which, under the *Act's* equivalent of Proposition #13, a public body can collect information without consent (Sch.B, para 4.1). In private sector legislation, too, clarity on these points seems desirable.

The *Public Sector Act* also includes a provision stating that an individual shall not be refused any service or benefit because he or she declines to provide information which is not in fact necessary for a legitimate purpose of the public body (Sch B, para.4.2). The provision reflects para.4.3.3 of the CSA Code.

One thing that the *Act* does not contain is any clarification of what "fair and lawful means" are. The "lawful" part of this is self-explanatory, but while the *Act* was being prepared some thought was given to whether the "fair" element could be clarified. The CSA Commentary says that "The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected" (para.4.4.2). This would certainly be one example of an unfair collection method, but it is doubtful that the idea of 'fairness' should be limited by the legislation to specific situations such as this. 'Fairness', though a general notion, appears to be a clear enough idea that it can stand alone in the legislation without further explanation.

Proposition #14

Data protection legislation should state the sources from which personal information may be collected, and should state that an individual shall not be refused any service or benefit because he or she declines to provide personal information which is not necessary for the identified purpose of the organization.

The requirement that personal information be collected by fair and lawful means does not need further explanation in data protection legislation.

CSA Principle 5 -- Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

a. Wording

There is one point of wording in CSA Principle 5 that seems to need addressing. The Principle refers to uses and disclosures that are "required by law." On a conventional legal reading of the word "required," this would cover uses and disclosures that an organization was legally compelled to make, but would not include situations in which there might be express legislation, or perhaps an express ruling from a court or other legally authoritative agency,

which *authorized*, but did not *require*, a particular use or disclosure. This is a gap that the *Public Sector Act* filled by expanding the phrase "except . . . as required by law" to become "except . . . as required or expressly authorized by law" (Sch.A, Principle 5). The gap is particularly important in the public sector, where many Acts confer discretions on Ministers or other government officials. However, the same gap may exist in relation to the private sector.

Proposition #15

CSA Principle 5 should permit uses and disclosures that are "expressly authorized by law" as well as those that are "required by law."

b. Inter-relation of "purpose", "consent" and "the law"

What is the relationship between the three possible justifications for a use or disclosure that CSA Principle 5 sets out, namely, the purpose for which the information was collected, the consent of the individual, and a legal requirement or authorization? In particular, what is the result when these factors point in different directions?

In principle, the three bases set out in CSA Principle 5 should be seen as alternatives. If any one of them exists, that is sufficient. On this basis one would say, for example, that an express refusal of consent cannot bar an organization from taking an action that the law has expressly authorized the organization to take.

In practice, however, there may be cases in which the relationship between identified purposes, consent and the law may be more subtle. One might be where the individual, while voluntarily providing information, expressly requests that it not be used in one particular way that falls within an organization's documented purposes. If an organization accepted personal information on this basis, it could not then rely on its documented purpose as governing the use of the information. Others might arise where an individual's actual or likely wishes were relevant to the balancing test for non-consensual action described in Proposition #13; those wishes would then partially determine what was "expressly authorized by law." In preparing the *Public Sector Act*, some thought was given to whether it was possible to provide any useful statutory guidance on how the three alternative bases for the use and disclosure of personal information inter-related. The conclusion reached was that it was not. The basic idea that the three were alternatives seemed clear from CSA Principle 5, and the possible subtleties of their inter-relation in specific situations could not be captured in a form that did not cause more confusion than it resolved.

Proposition #16

Data protection legislation need not elaborate upon the relationship between "purposes," "consent" and "the law" as alternative bases for the use or disclosure of personal information.

c. Retention

CSA Principle 5 requires that personal information shall only be retained for as long as is necessary for the fulfilment of the purposes for which it was collected. In many cases compliance with this obligation may lead to the destruction of personal information that is no longer needed. Another way of ceasing to retain *personal* information, however, is to convert it into a form in which the individuals to whom it relates are no longer identifiable. For clarity, it may be wise for data protection legislation to spell out this second alternative.

Proposition #17

Data protection legislation should make it clear that an organization's duty not to retain personal information can be satisfied by converting the information into a form in which the individuals to whom it relates cease to be identifiable.

Another thing that should normally be clarified is how long the acceptable retention period is. This is more easily done in relation to personal information in "personal records sytems" than other personal information. So far as "personal records systems" are concerned, part of the process of establishing the system should include taking a decision on how long the information will be needed, and what will be done with it when it has served its purpose. Some kind of time-lag is likely to be necessary so that personal information is not disposed of too soon. Both for the organization and the individual there may be a need for information to be retained for some time after it has been used.

Outside "personal records systems" -- in places such as policy or product development files where "personal information" will sometimes appear incidentally -- a more flexible approach to retention and destruction seems to be appropriate. To attempt to purge all incidental "personal information" from such files would be a laborious task, and these kinds of files are, in the long run, quasi-anonymous. Once the file is closed, any personal information it contains is relatively inaccesible. Of course, if the 'non-personal' file is later re-opened, any use or disclosure of the personal information that remains there would still be subject to the legislation.

Proposition #18

Organizations should not be required to purge all personal information from 'non-personal' files in which the personal information appears incidentally.

CSA Principle 6 -- Accuracy

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

This Principle is self-explanatory. The main point that the CSA Commentary makes on it is that "An organization should not routinely update information, unless such a process is

necessary to fulfil the purpose for which the information was collected" (para.4.6.2). The Principle should not, therefore, be mis-read as imposing a general obligation to keep personal information up-to-date: an appropriate degree of "accuracy" is only really called for when information is "used." This, though, seems clear enough from the relative terms in which CSA Principle 6 is expressed.

Proposition #19

CSA Principle 6 is self-explanatory. Data protection legislation would not need to provide additional guidance on its application and interpretation.

CSA Principle 7 -- Safeguards

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

a. Wording

The *Public Sector Act* removed the word "security" from CSA Principle 7. The reason was that this word seemed to under-represent the scope of the Principle. The CSA Commentary says that the safeguards must protect the personal information from "loss or theft, as well as unauthorized access, disclosure, copying, use, or modification" (para.4.7.1). It also mentions that the methods of protection should include physical, organizational and technological measures, as well as making employees aware of the importance of maintaining the confidentiality of personal information (paras.4.7.3 and 4.7.4). Though the word "security" catches some of the flavour of this, it diverts attention from the idea that one of the principal safeguards against "unauthorized . . . disclosure [or] . . . use" will be a proper appreciation of what kinds of use and disclosure are in fact "authorized". Viewed in this broad sense, what CSA Principle 7 amounts to is placing an obligation on organizations to take the necessary steps internally to make the legislation work. Including the word "security" in the Principle seems to narrow its scope.

Proposition #20

The word "security" should be removed from CSA Principle 7 so as not to narrow its scope.

b. What kinds of safeguards?

As noted above, the CSA Commentary specifically mentions various kinds of measures as being intended to be included in the broad expression "safeguards." For clarity, it seems appropriate that data protection legislation should do the same. On the further question of what kinds of safeguards will be, in the language of CSA Principle 7, "appropriate to the sensitivity of the information," consideration has been given to whether any further legislative explanation could be given of what will make a safeguard "appropriate." It seems, though, that the simple statement in the Principle is as satisfactory as a more detailed formulation is likely to be.

Proposition #21

Data protection legislation should specify that the safeguards to be implemented include training and physical, technical, administrative and other measures, as appropriate in the circumstances. It should not attempt to define what will make a safeguard "appropriate to the sensitivity of the information."

c. Transfers to third parties

An important sub-issue that arises in relation to safeguards is this: what kinds of safeguards, if any, should an organization put in place when it transfers personal information to another body?

The guiding principle here is that an organization is responsible for personal information under its control (CSA Principle 1), and that this responsibility continues to exist at least until the time when the personal information is transferred. The organization must ensure, therefore, that the transfer is authorized by law, by consent or by the purpose of the original collection (CSA Principles 3 and 5), and under the Safeguards Principle it must take appropriate steps, commensurate with its responsibility under CSA Principle 1, to protect the personal information.

What those steps will be will depend on the circumstances. In many cases compliance with CSA Principles 3 and 5 will be sufficient. This will be the case if the receiving organization is also subject to the legislation, since the receiving organization's use will be limited to the legitimate purpose for which the transferring organization is disclosing it. In other cases the receiving organization may be under a professional or contractual obligation of confidentiality which the transferring organization can rely on as making additional safeguards unnecessary. In some cases, however, there may be no such context of legal protection for the information, and the transferring organization may have to take steps to ensure that the terms of the transfer are consistent with the organization's responsibilities.

Can data protection legislation go further than this, and spell out what those steps should be? This seems doubtful. Contractual terms may sometimes be effective, particularly in the context of an ongoing relationship between the organizations in question, but it would be very difficult to identify particular situations in which a transferring organization *must* put contractual measures in place. Unless the legislation were prepared to identify those situations, it would effectively be leaving the decision to the organization, and this, in turn, would amount to little more than the general statement that the transferring organization must put in place 'appropriate safeguards'.

Proposition #22

Data protection legislation should make it clear that "appropriate safeguards" may be required when an organization transfers personal information to another organization, but it should not require specific forms of safeguards.

CSA Principle 8 -- Openness

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

Like others among the CSA Principles, Principle 8 seems to apply more naturally in large organizations, which are likely to have formalized "policies and practices," than in small ones. Even in small organizations, however, it seems possible to give the Principle an intelligible meaning. The individual can ask what the "policies and practices" are. The organization, in reply, must explain whatever the true state of affairs is. All organizations should presumably be able to do this much.

Proposition #23

CSA Principle 8 is self-explanatory. Data protection legislation need not attempt to clarify its meaning.

CSA Principle 9 -- Individual Access

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

a. Wording

CSA Principle 9 is the second of the two Principles that are acommpanied by a Note -- which is an "integral part of the principle" (para.3.1.2). The Note explains why the right of access cannot be unqualified.

> Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege. (para.4.9)

Data protection legislation elsewhere regularly includes exceptions along these lines. In the *Public Sector Act*, the words "except where inappropriate" were added at the end of the first sentence of CSA Principle 9 to indicate that the individual's right to information is not unqualified. The same addition would seem to be called for in private sector legislation.

Proposition #24

The words "except where inappropriate" should be added to the right to information in CSA Principle 9.

b. The nature of the right

Though CSA Principle is headed "Individual Access," it actually appears to include two elements: a right to "be informed" as well as a right to be "given access." In practice, the right to *information* may well be more used than the the right to *access*, which is in effect a right to documents. The organization's obligation under the Principle is triggered by a request from the individual. In most cases it seems likely that the individual will simply ask for information, and a straightforward reply will satisfy CSA Principle 9.

There may be cases, of course, in which an individual specifically requests access to documents. In this case, assuming that it is not unduly onerous or expensive to allow the request (see *c. Exceptions to access*, below), and that none of the other substantive exceptions apply, the documents should be made available. In some cases, perhaps, *documents* may be withheld on the basis of one of the exceptions, but *information* as to at least part of their contents should still be provided in order to meet the organization's obligation under this Principle.

In the *Public Sector Bill* there was no need to clarify this relationship between "information" and "access," since the matter is dealt with by the *Right to Information Act*. In private sector legislation, however, the relationship should be made clear.

Proposition #25

Data protection legislation should make it clear that, under CSA Principle 9, providing *information* is sufficient unless access to documents is specifically requested.

c. Exceptions to access

Under the *Public Sector Act* the *Right to Information Act* is relied upon to provide the exceptions to the individual's right to information. Most "public bodies" are subject to that Act already. Private sector legislation, however, should spell out its own list of exceptions.

Part of the list would be a counterpart of the one in Proposition #13, which describes when it is appropriate to collect, use or disclose personal information without consent. In several of the situations described, non-disclosure to the individual would be equally appropriate. There are also, however, some grounds for non-disclosure that are specific to the context of 'individual access'. There is also the question of whether the list should include a general provision to deal with situations not foreseen by the specific items listed, and of whether, if information is withheld, an organization might nonetheless be expected in some cases to provide some explanation of the substance of the information.

Proposition #26

An organization should not be required to disclose personal information to the individual

(a) where disclosure would be harmful to the health, safety or security of the public or an individual, including the applicant;

(b) where disclosure would be prejudicial to an investigation related to the enforcement of an enactment;

(c) where non-disclosure is required or expressly authorized by law, or where the individual would have no right to obtain the information in legal proceedings;

(d) where the information was provided by another person in confidence, or is confidential in nature;

(f) where the information requested is inextricably linked to the personal information of another individual;

(f) where the information requested would be unduly expensive or onerous to provide.

Consideration should also be given to authorizing non-disclosure when there is some other legitimate and substantial reason for not providing the information requested.

Non-disclosure should be limited to the reasonable requirements of the situation. If it is practicable to explain the substance of the information withheld without prejudicing the reason for withholding it, the organization should do so.

c. Procedure

CSA Principle 9 says nothing about the procedure by which individuals may obtain the information, materials or corrections to which they are entitled. By inference, it leaves it up to each organization to establish its own procedures.

This appears to be acceptable. CSA Principle 9 covers many possible scenarios, ranging from entirely informal requests, which organizations may readily and easily respond to, to situations which may become adversarial. To establish a statutory procedure for all of these would not be easy; it would also risk bureaucratizing the process. If data protection was silent on the question of access procedures, it would operate on the premise that the individual has rights and the organization must respect them. Implied in this would be that the organization must deal with the individual's request within a reasonable time, and that anything less than a genuine attempt to permit the exercise of the individual's rights will be a violation of the Principle.

Proposition #27

Data protection legislation could be silent on the question of access procedures under CSA Principle 9.

d. Corrections

Broadly speaking, the idea that an individual should be able to "challenge the accuracy and completeness of the information and have it amended as appropriate" seems self-explanatory and self-operating. An organization will presumably have little interest in having inaccurate or incomplete information in its files. The problem of implementation that seems most likely to arise under this element of CSA Principle 9, therefore, is that the individual and the organization may disagree as to whether personal information is incorrect. If this occurs, the organization should not be required to alter the information it possesses, but it should note that the individual disputes its accuracy. It seems likely that this would occur in the ordinary course of events, even without legislative reinforcement, but since CSA Principle 9 is silent on the question of disagreements between the parties, legislative clarification is probably appropriate.

Proposition #28

When the individual has challenged the accuracy or completeness of personal information, but fails to convince the organization, the organization should make a note that the individual disputes the information in question.

CSA Principle 10 -- Challenging Compliance

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

This Principle, it must be noted, is concerned with an *internal* review of compliance by the organization itself; issues relating to *external* review by some other body are dealt with below, under the heading Enforcement.

In an internal review process the main issue is maintaining the credibility of the process. In all cases the organization is reviewing its own conduct, and in some cases, especially in small organizations, the person conducting the review may well be the very person whose decision is being questioned. This is unavoidable. What legislation *can* attempt to do, however, is emphasize that the review process must be a genuine one. No doubt this is implicit in CSA Principle 10, but for clarity, there is value in setting out in data protection legislation both the organization's obligation to investigate in good faith and its duty to take appropriate measures if it finds the complaint to be justified.

Proposition #29

An organization should be required to investigate in good faith the complaints it receives and to take appropriate measures when a complaint is found to be justified.

B.3 Other Issues Arising

In Part 2 of the federal government's 1998 consultation paper two main issues that are not dealt with in the CSA Code have been identified as requiring attention. The first is "Sectoral Codes". The second is "Enforcement".

a. Sectoral Codes

The issue here is whether data protection legislation might permit or encourage particular sectors of industry to develop their own codes, whether customized versions of the CSA Code or entirely home-grown products, and if so, what the legal effect of those codes should be. The issue arises out of a concern that the CSA Code, and data protection legislation based on it, is expressed in terms that may not be totally applicable to all organizations or that it may be too general to give useful guidance to what actually is or is not permissible in specific situations. A sectoral code would allow an industry to develop rules that were sensitive to the particular requirements of its own operations.

The critical issue here is whether the sectoral code should have legal force, and in particular whether it would prevail over the statutory Code if the two were in conflict. If so, it would be necessary for the sectoral code to receive some kind of official approval from a body that had legal authority under the Act. Otherwise, industries would effectively be being given the authority to write themselves out of the legislation. If, on the other hand, the sectoral code could not prevail over the statutory Code, there would be less need, if any, for an official approval process. Whatever the sectoral code said, the statutory Code would still provide the governing principles. The sectoral code, of course, would then be of less value from the industry's point of view, since reliance on the sectoral code could never be a guarantee that the industry was complying with the legislation.

While sectoral codes do have advantages -- as, indeed, do codes and policies internal to particular organizations -- the better approach here seems to be that codes and policies should operate within the framework set out in the legislation, and the legislation must prevail in case of conflict. Admittedly the framework is expressed in general terms, but data protection is far from the only context in which legal rules are stated in general terms, and organizations have to develop policies and practices based on their best understanding of what the rules mean. If specific kinds of organization, or specific activities, require more detailed legal rules than the general principles in the statutory Code, it would be better to establish these by regulations under the Act than by way of industry codes.

Proposition #30

Sectoral codes should not be given the force of law under data protection legislation. Data protection legislation should include regulation-making authority under which, if necessary, more detailed provision can be made in relation to particular kinds of organization or information, or particular activities.

b. Enforcement

Enforcement is an issue that the CSA Code did not need to address, since the CSA Code was a purely voluntary one, and would be entirely self-policed. In a legislative framework, however, the question of what happens when the rules are broken must be dealt with. If the legislation were silent on the subject, it would ultimately be the courts that interpreted the legislation and decided what was implied by way of remedies.

The three basic approaches to the enforcement of legislation are (a) the penal remedy, (b) the civil remedy, and (c) the administrative remedy. The penal remedy involves prohibiting unacceptable conduct and punishing offenders; government lawyers are normally the prosecutors, and fines are paid to the court. The civil remedy is a means by which individuals can go to court in their own right, seeking compensation for, or the prevention of, a wrong done to them. Any compensation is paid to the individual. The administrative remedy involves the establishment of an agency outside the courts to enforce a particular piece of legislation; this agency can be given a variety of remedial powers. The position of the individual and the role of the courts will vary depending on what those powers are.

The penal remedy

The *Public Sector Act* makes it an offence for a public body, or an officer, employee or agent of a public body, to collect, use or disclose personal information in wilful contravention of Principles 3 (Consent), 4 (Limiting Collection), or 5 (Limiting Use, Disclosure and Retention) of the Statutory Code of Practice. A conventional interpretation of a "wilful" violation of an Act is that it involves doing a wrongful act either knowing that it is wrong or acting with reckless disregard as to whether it is wrong or not. Legislation prohibiting the wrongful disclosure of information is more familiar in the public sector than the private sector, but an offence along these lines might be appropriate in private sector legislation, too. Private sector legislation might also establish an offence of wilful refusal to provide information, or to make a correction, to which an individual is entitled under CSA Principle 9. This is a subject that does not arise under the *Public Sector Act*, since enforcement of the individual's right of access takes place under the *Right to Information Act*.

Proposition #31

Data protection legislation could make it an offence to wilfully violate CSA Principle 3 (Consent), 4 (Limiting Collection), 5 (Limiting Use, Disclosure and Retention), and 9 (Individual Access).

The civil remedy

Is there a place for civil remedies in data protection legislation? The basic civil remedies are declarations, injunctions and damages. A declaration simply states what the law is or how it applies to a particular set of facts. Injunctions also involve a ruling on how the law applies to a particular set of facts, but add to this a mandatory element, requiring people either to take or not to take a particular course of action. Awards of damages, finally, require one party to compensate another for the harm arising out of a wrongful act.

What part might civil remedies play in the enforcement of data protection legislation? This paper will first consider these remedies in isolation. It will then revisit the question in the light of its discussion of administrative remedies. If a substantial administrative enforcement mechanism were put in place, the part to be played by civil remedies might be much reduced.

The main function of the civil remedy, as opposed to the penal remedy, is to give an individual who is the victim of a wrongful act a personal right to protect his or her own interests. It also has a more general effect. While dealing with individual cases, the civil remedy allows courts to provide authoritative and binding rulings as to what particular provisions of the legislation mean. There is then a ripple effect as the court decision sets a standard to be followed by all organizations that are subject to the Act. Court proceedings are often considered costly and inconvenient. Nonetheless, people are sometimes prepared to litigate over matters that are important to them, and the litigation can settle important points of principle. A prime example in the 'personal information' field would be *McInerney v Macdonald* (1992) 126 NBR (2d) 271, a New Brunswick case in which the Supreme Court of Canada eventually established the right of a doctor's patient to see a consultant's report.

Generally speaking, unless there is some administrative remedy making recourse to the courts inappropriate, one would think that if a law is enacted, the courts should be able to say what it means. Declarations, therefore, would appear to be a natural part of the scheme. Injunctions would naturally follow. It would be odd to allow the courts to say what an Act means but to give them no authority to require an organization to act as the legislation says it should. The idea that organizations might be ordered to comply with the legislation is something to be borne in mind when considering the detailed wording of legislation; it would be essential that the legislation did not impose obligations that organizations could not reasonably be expected to live up to. Unless unreasonable obligations are imposed, however, injunctions should not be problematic.

Awards of damages require more careful thought. A review of data protection materials from elsewhere suggests that one may legitimately ask both (a) whether damages should be available at all for breach of the data protection principles and (b) if so, in what circumstances. Most existing public sector data protection Acts in Canada do not provide for awards of damages. In Quebec, where legislation covers the private sector as well, the basic data protection provisions are in the Civil Code, and awards of damages are available. In private sector data protection statutes from common law jurisdictions outside Canada (there

are none in Canada at present), awards of damages are approached with care. New Zealand's *Privacy Act 1993* expressly states that it creates no legal rights enforceable through the courts. Compensation can be ordered by the Complaints Review Tribunal, but this is discretionary, not a matter of entitlement. In the U.K., under the *Data Protection Act 1984*, damages can be awarded in some situations, but not where an organization has taken "such care as in all the circumstances was reasonably required" to prevent the violation from occurring. When the amount of the compensation is assessed, the "distress" suffered by the individual can be taken into account, but apparently "distress" by itself is not enough to entitle the individual to compensation. The existence of "damage," it seems, is an essential precondition to the claim. (See sections 22 and 23.)

There is good reason for caution in making awards of damages available for violation of data protection principles. The principles set standards of good practice, but it is not necessarily the case that every act that falls short of these standards, and is therefore less than 'good', is necessarily so 'bad' that it should give rise to a claim for compensation if damage or distress results. If "personal information" is defined as suggested in Proposition #5 -- as any information about an identifiable individual, recorded in any form -- it will cover a wide range of material, some of it sensitive, much of it not. The handling of personal information, and thus the possibility of error, will abound in the everyday operations of most organizations, and the implementation of the legislation will regularly involve decisions being made about what is "appropriate" or not, or what is "reasonable" or not. The legislation could become burdensome if every decision reached were liable to be questioned in the courts, with a potential liability to damages arising out of any error in judgment, even where the organization had made genuine and substantial efforts to comply with the legislation.

For this reason it seems wise, in relation to awards of damages, to build a margin of error into data protection legislation, so that the mere fact that an organization falls short of the standards in the Act, and damage results, would not of itself be sufficient to support a claim for compensation. This margin of error might be defined in different ways. The U.K. legislation, as noted above, uses lack of reasonable care as the test for an award. An alternative might be to look at the consequences of the non-compliance, and say that it was only where these amounted to a true 'invasion of privacy' that compensation could be awarded. Preferable to either of these, perhaps, would be to provide a test of 'manifest inconsistency with the Act' as the threshold that a plaintiff had to establish in an action for damages. Under such a test, reasonable but mistaken actions would not expose organizations to liability for damages.

Proposition #32

Unless data protection legislation adopts administrative remedies that make civil remedies unnecessary, declarations, injunctions and awards of damages should be available for the enforcement of the legislation. However, awards of damages should only be made where an organization's non-compliance with the Act causes loss and satisfies some additional criterion such as being manifestly inconsistent with the Act.

The administrative remedy

In the public sector the issue of administrative remedies was relatively straightforward. A statutory agency already existed -- the provincial Ombudsman -- with a mandate that naturally included information-handling issues of the type that data protection principles involve. This connection was officially recognized when the Province adopted its *Personal Privacy Code* in 1994; the Ombudsman was identified then as the body to oversee compliance with the Code. The Department of Justice's 1996 Discussion Paper suggested that the Ombudsman should have the same role under public sector data protection legislation. The Law Amendments Committee confirmed that role, and this is now the effect of the *Public Sector Act*. Under that *Act*, the administrative remedy through the Ombudsman is in fact the primary remedy, with judicial remedies having a much more limited scope.

In the private sector, however, things are not so simple. There is no existing agency with a mandate that naturally extends to data protection in all, or even many, of the "organizations" that Proposition #4 suggests data protection legislation might cover. There are, however, many fields of activity where there are statutory regulators whose mandates either do or could include data protection issues. Regulated bodies include insurance companies, financial institutions, collection agencies, private investigators and nursing homes, to name just a few. Self-regulating occupations like lawyers and doctors also have statutory complaints mechanisms in place that might deal with data protection matters -- and probably already do so in contexts such as client confidentiality. Non-statutory complaints mechanisms have also been put in place by voluntary standards-setting bodies such as industry associations. The recent federal consultation paper mentions all of these bodies as potentially having a part to play in the non-judicial enforcement of private sector data protection legislation (p.21).

Discussion of administrative remedies for data protection legislation tends to focus on whether a designated data protection agency should be established to oversee compliance. The expression 'Privacy Commissioner' is often used to identify this agency, but the term is misleading. It suggests that the agency might be concerned with 'privacy' in the broad and more natural sense of Part II of this Paper, rather than with the more limited 'data protection' issues that are in fact the agency's role. This Paper will therefore use the expression 'data protection agency' rather than 'Privacy Commissioner'. It must also be noted, of course, that establishing administrative remedies for data protection legislation does not necessarily require the creation of a data protection agency. There are other options.

There are two broad reasons why one might establish administrative remedies for data protection legislation. One would be to reduce the role that the courts might otherwise play in enforcing the Act. This might be done if, for example, the obligations created by the legislation did not readily lend themselves to judicial enforcement, or if there was concern that the legislation might expose organizations to too much litigation over too many issues. The other would be that judicial remedies, though appropriate to data protection legislation, could not cover enough of the ground. They might be thought to be too slow and expensive

to deal with ordinary non-compliance issues, and unable to deal with things such as prevention and education, which some people would argue a data protection scheme must include.

The first of these reasons is essentially an assertion that judicial remedies are not appropriate to data protection legislation. Some people might argue, for example, that the CSA Code must be seen as an ethical statement rather than a legal one, that organizations cannot realistically be expected to maintain the standards that it sets, and that they should not be exposed to law-suits every time they fail to do so. On this basis an administrative remedy based substantially on moral suasion might be seen as more appropriate than the courts.

The strength of such an argument depends on whether the CSA Code, and data protection legislation based on it, does or does not accurately describe realistic standards of good practice. It also depends on the nature of the judicial remedies proposed -- which, on the basis of Propositions #31 and #32, would be (a) prosecutions for "wilful" violations of specific principles, (b) damages where loss is caused by an action that is "manifestly inconsistent with" the legislation, and (c) declarations and injunctions in any case of non-compliance. Whether this balance of obligations and remedies is appropriate and realistic is an important subject for public debate.

One point that is worth making, though, is that the obligations in the CSA Code are of a kind that courts do enforce in other contexts. The Code incorporates flexible ideas like "except where inappropriate" (CSA Principle 3) and the "reasonable expectations of the individual" (para.4.3.5). The courts regularly deal with flexible concepts such as these; examples include "reasonable care" in the law of negligence, and "reasonable expectations of privacy" under s.8 of the *Canadian Charter of Rights and Freedoms*, to mention just two. The courts are, indeed, probably more familiar than most administrative agencies with enforcing generic standards such as these, and particularly so in applying them across a broad sweep of activities. It seems unlikely, therefore, that the obligations in data protection legislation can be said not to lend themselves to interpretation and enforcement by the courts. One might, perhaps, limit the role of the courts on the ground that organizations and individuals would have a greater 'comfort level' in dealing with an administrative body when a dispute under the legislation arose. This, though, is different from saying that the courts are not well suited to interpreting principles such as those in the CSA Code.

This leads to the second of the reasons identified above for establishing administrative remedies under data protection legislation -- that though judicial remedies might be appropriate to data protection legislation, administrative remedies would be preferable. There are two main aspects to this. One relates to complaints and the nature of the dispute resolution process. The other relates to issues such as prevention and education, which, if they were part of the legislative scheme, could obviously not be the function of the courts.

In relation to complaints, the argument for establishing an administrative remedy can be stated quite bluntly. It is that litigation is expensive and intimidating, and most people, in

most situations, will not sue over the kinds of issues involved in data protection legislation. On this argument, unless there is administrative enforcement, there will effectively be no enforcement at all. Administrative enforcement, one might add, could operate largely by mediation and conciliation, whereas judicial remedies tend to be confrontational.

Countering this is the view that administrative remedies are the exception rather than the rule for most legal disputes. Though agencies such as rentalsmen, employment standards officers and human rights commissions exist, normally the parties to legal disputes must sort things out between themselves, or take their lumps, or sue. This is the position that the law takes on 'personal information' matters such as defamation or breach of confidence. The same applies in relation to the fundamental human rights set out in the *Canadian Charter of Rights and Freedoms*, including the right of privacy that the courts have held it implies. It is also largely true of consumer protection statutes (under which consumers will probably use the small claims procedure if the matter eventually comes to litigation). The consumer analogy is a relevant one because much of the discussion of private sector data protection legislation, including the recent federal consultation paper, places data protection in the context of the need to protect consumer rights, especially on the information highway.

The creation of an administrative complaints procedure in data protection legislation should not, therefore, be taken for granted. A choice is involved about costs, about benefits and about priorities. On the one hand, administrative resources devoted to the enforcement of data protection legislation should presumably improve the likelihood that 'fair information practices' will be observed in practice. On the other hand, there are always many claims for administrative resources, and it would not diminish the values promoted by data protection legislation if it were simply left up to individuals to pursue their remedies by legal proceedings if they so chose. Existing regulators would of course continue to be available to receive complaints within their spheres of responsibility.

If an administrative complaint process for data protection legislation appears to be, in the abstract, desirable, one must also ask what the process should involve. One possibility is that it should be a process of mediation and conciliation, with no compulsory powers attached. Arguably this would improve the prospects of reaching amicable solutions; on the other hand, it might be criticised as being weak. If one moves beyond this, however, and adds compulsory powers to the administrative remedy, a range of issues arises as to what those powers should be. If binding orders could be issued, formal powers to hold hearings would presumably be required. Along with them would probably go the power to summon witnesses and compel the production of evidence. Powers to enter premises and inspect books and records might also be called for. Enforcement mechanisms designed to ensure that the binding orders were complied with would also have to be considered.

In short, one step leads to another. The issue for public discussion at this point is just how far it is right to go in establishing an administrative complaint process. Three credible points on the scale are (1) to rely on judicial processes entirely, (2) to have an administrative process with no compulsory powers (the judicial process might still perhaps be available if

mediation failed), or (3) to have an administrative process with compulsory powers that would probably be quite extensive. Which of these approaches is better suited to the goal of ensuring that organizations follow 'fair information practices' in their handling of personal information?

The other issue that was raised earlier in relation to administrative remedies was whether an administrative process could provide things that judicial remedies, being strictly complaints-based, could not. One item mentioned previously was prevention; another was education.

If functions such as these enter the picture, the administrative remedy under data protection legislation begins to take on the shape of a permanent body -- not necessarily a single-purpose data protection agency, but at least a body with a continuing existence and data protection as one of its functions. By contrast, a pure complaints mechanism, as described in previous paragraphs, could be a more temporary entity, established to deal with complaints as they arose.

Nonetheless, some of the issues raised by these additional functions are comparable to those raised in relation to the complaints mechanism. Prevention, on the face of things, seems desirable. But if, in practice, prevention means that an administrative agency has the compulsory power to enter the premises of any organization and inspect its records and practices, even in the absence of a complaint, is it an appropriate power to confer in the interests of the proper handling of personal information?

Prevention in another sense might mean giving advice to organizations so that they can ensure that their practices comply with the legislation. Yet this too can be problematic, because whatever advice the agency might give, it would also have to reserve the right to re-investigate the matter with an open mind if an individual subsequently made a complaint about the action in question. The agency's advice, therefore, could not be authoritative, and unless authoritative it would be of questionable value to the organizations that sought it.

Education, in the pure sense of providing general information to the public about the legislation, and advocacy, in the sense of trying to encourage governments and organizations to pay greater attention to data protection issues in their decisions and practices are perhaps less likely to cause practical or technical difficulties. There is, however, a question of priorities and resources to be addressed. As part of the mandate of a substantially complaints-oriented agency they might well be desirable. As a mandate in themselves, however, in the absence of a substantial volume of complaints, one might wonder whether they were justified.

It may be worth noting here that the volume of complaints received by the Ombudsman under New Brunswick's public sector *Personal Privacy Code* in the first three years after its adoption was small -- less than 25 complaints each year. Few conclusions can be based on these figures, but they may at least indicate that policies under data protection legislation should not be based on the assumption that the volume of complaints will be large.

It will be interesting to see whether the replacement of the non-statutory *Personal Privacy Code* in the public sector by the *Protection of Personal Information Act* makes a difference to these figures.

Proposition #33

Administrative remedies are not essential to data protection legislation, but are a policy option. Key issues for public discussion are

(a) whether judicial remedies alone would be appropriate and sufficient,

(b) whether an administrative complaints mechanism without compulsory powers would serve a purpose,

(c) whether an administrative complaints mechanism with compulsory powers would be over-intrusive or counter-productive,

(d) whether a non-complaints function can be identified that is substantial, viable, and a strong reason in itself for devoting resources to an administrative agency with a specific data protection mandate.

II. Privacy in General

As was pointed out in the Introduction to this Paper, "privacy" is a much broader concept than "data protection". When people speak of their privacy they would normally think of things like the peace and quiet of their homes, their ability to communicate without third parties listening in, and protecting the details of their lives from unwanted publicity. Article 17 of the International Covenant on Civil and Political Rights, which establishes privacy as one of the internationally recognized human rights, and to which Canada is a party, catches the general flavour of this:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honour and reputation. Every one has the right to the protection of the law against such interference or attacks.

In its 1997 report *Privacy: Where Do We Draw the Line?* the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities offered the following as its key statement of "fundamental privacy rights" (p.35):

> Everyone is entitled to expect and enjoy:
>
> - physical privacy;
> - privacy of personal information;
> - freedom from surveillance;
> - privacy of personal communications;
> - privacy of personal space.

Data protection is evidently only one part of this. It falls primarily into the realm of "privacy of personal information", but even there, data protection, with its focus on "recorded information" and "organizations," and its exclusion of personal and household activities, does not cover all of the ground.

The purpose of this Part of this Paper, therefore, is to consider whether New Brunswick should adopt legislative measures to protect 'privacy' in the more general sense. Two specific approaches are identified. One is to expand the existing *judicial* remedies by establishing a 'tort' of invasion of privacy. A 'tort' is a wrongful act for which an aggrieved individual can seek the normal civil remedies of damages, declarations and injunctions. The other is to establish *non-judicial* (or administrative) remedies for infringements of privacy. These two approaches are the natural extensions of the discussion in Part I of possible "civil remedies" and "administrative remedies" under data protection legislation. The House of Commons Standing Committee, though it clearly supported non-judicial remedies for infringements of privacy, paid little attention to judicial remedies. This is surprising. The

Committee's principal recommendation was that Parliament adopt in the federal sphere a "Charter of Privacy Rights" that would have a quasi-constitutional status (p.45). As will be seen, however, the key elements of the Committee's "fundamental privacy rights" (quoted above) are very much the kind of things that some provinces do, and New Brunswick might, assert by way of a 'tort' of invasion of privacy.

A. Judicial Remedies for Invasion of Privacy

The path that the next few pages will take is relatively well-trodden. In countries such as England, Australia and Canada there have been several studies of the similar judicial remedies that are available for the protection of privacy interests. The shared background of these studies is that there is no established remedy for an invasion of privacy as such, but that privacy interests can be protected through a number of other remedies such as actions for trespass or for breach of confidence. The discussion, therefore, is of the scope of the established remedies, of how much more could or should be done to ensure that privacy can be adequately protected, of whether the best way forward, if more should be done, is through legislation or through judge-made law, and of whether, under either of those two approaches, the sounder legal framework is to develop the existing remedies or to create a new tort of "invasion of privacy".

That discussion also refers to experience in the USA for contrast. There the courts have recognized a common law right of privacy for many years. The case-law has been analyzed as recognizing four main categories of actionable invasion of privacy: (1) intrusion upon the plaintiff's seclusion or solitude, or into his or her private affairs; (2) public disclosure of embarrassing facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

In Canada, where the position is described at length by Ian Lawson in his book *Privacy and Free Enterprise* (1993, Public Interest Advocacy Centre), the discussion has some special features. One is that five Provinces have in fact legislated to create a specific tort of invasion of privacy. Four of these -- B.C., Saskatchewan, Manitoba and Newfoundland -- are common law provinces where the remedy was new. The fifth is Quebec, where the remedy originally evolved through interpretation of general provisions of civil responsibility in the former *Civil Code*, but has now been expressly included in the new one. Quebec's *Charter of Human Rights and Freedoms* also contains, as art.5, a provision that "Every person has a right to respect for his private life." Unlike the Canadian *Charter*, this provision is directly enforceable between citizens.

Another special feature of the Canadian debate is that in the common law provinces where there is at present no legislation, the courts have recently become more willing to consider that perhaps a general tort of invasion of privacy may exist at common law. In a few cases in Ontario damages have been awarded on this account. A recent decision of the Court of Appeal of Prince Edward Island commented that "the courts in Canada are not far

from recognizing a common law right of privacy, if they have not already done so" (Carruthers CJPEI, *Dyne Holdings Ltd. et al v Royal Insurance Co. of Canada* (1996) 138 Nfld.& PEI R, 318). These developments complicate the issue of whether it is *legislators*, specifically, who should take action to establish invasion of privacy as a tort, or whether the courts should be left to develop, case by case, this new field of liability. If the case law were clearer that there either is or is not a general tort, it would be easier to assess the contribution that legislative measures might appropriately make.

So far as the judicial remedies are concerned, the key issue is whether New Brunswick should enact legislation that makes an invasion of privacy a tort. As with the data protection section of the Paper, there is a specific legislative model around which the discussion will centre. This is the *Uniform Privacy Act* adopted by the Uniform Law Conference of Canada in 1994. The *Uniform Act* draws upon and attempts to improve the existing provincial statutes, all of which are similar in substance, though different in some of their details. There is no obvious reason for this Paper to attempt to invent something completely different. The Paper will therefore describe the Act, and present three major policy options in relation to judicial remedies for invasions of privacy. One is to adopt legislation substantially similar to the *Uniform Act*. Another is to decide that there should not be a tort of invasion of privacy at all. The third is to say that *if* there is to be a tort of invasion of privacy, it should be left to be developed by the courts rather than established by legislation.

Proposition #34

Discussion of a statutory tort of invasion of privacy should be based on the *Uniform Privacy Act* prepared by the Uniform Law Conference of Canada, set against the background of existing judicial remedies that may protect privacy interests.

A.1 Existing Remedies

The existing legal remedies for invasion of privacy are found under the *Canadian Charter of Rights and Freedoms*, under various federal and provincial Acts and in various existing torts. None of these contains an established and general remedy for 'invasions of privacy' as such. As was mentioned above, there is currently a theoretical debate as to whether, at common law, a general tort of 'invasion of privacy' exists, but if it does, it is certainly not yet "established." By contrast, the other remedies that will be referred to are clearly "established," and can be used to protect *some* privacy interests, but they are not "general."

a. The Canadian Charter of Rights and Freedoms

Privacy under the *Canadian Charter of Rights and Freedoms* can be dealt with fairly briefly. The *Charter* contains no express right of privacy. The courts, however, including the Supreme Court of Canada, have held that a right of privacy is implicit in other express provisions of the *Charter*, notably s.7 and s.8. They appear to talk quite freely of a

"constitutional right of privacy" despite the absence of any express provision on the subject in the *Charter*.

S.7 of the *Charter* says that "Everyone has the right to life, liberty and the security of the person, and the right not to be deprived thereof except in accordance with the principles of fundamental justice." The courts have held that privacy can be an element of "liberty" and of "security of the person." They have held that there is at least a "biographical core of personal information," which may tend to reveal "intimate details of lifestyle and personal choice," that is entitled to protection under this section. Arguably there may be more, but there is at least this much.

S.8 of the *Charter*, says that "Everyone has the right to be free against unreasonable search and seizure." The courts have held the test of whether a search or seizure is "unreasonable" is whether it violates a "reasonable expectation of privacy". "Searches" and "seizures" have been held to include not only physical searches and seizures in the obvious context of criminal law enforcement, but also other forms of mandatory information-gathering. Obtaining information from willing third parties has also been held to be a search or a seizure in some cases -- e.g. *R v Dyment* (1988) 89 N.R. 249, where a doctor voluntarily provided the police with a blood sample from an injured driver which showed that the driver had been impaired at the time of an accident, and *R v Plant* [1993] S.C.R. 281, where a power company voluntarily made electricity consumption records available to the police. (In the latter case, the police "search" by checking the records was held not to be an "unreasonable" one, since in the view of most of the Supreme Court justices, though not all, records of electricity consumption did not disclose "intimate details of lifestyle and personal choice" in which the householder could have a "reasonable expectation of privacy.")

Charter protection, however, is not absolute. Under s.7, for example, a person *can* be deprived of "life, liberty and security of the person" if this is done "in accordance with the principles of fundamental justice." Under s.8, what it protected is a "*reasonable* expectation of privacy." Under s.1, moreover, all *Charter* rights are subject to "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." More important than this, though, in terms of the availability of *general* remedies for invasions of privacy, is that the *Charter* only applies to the actions of governments. It will not normally apply to privacy issues as between citizens. As a remedy in the private sphere, therefore, any *Charter* right of privacy is of limited application.

b. Federal and provincial Acts

Protection of privacy under federal and provincial Acts can be dealt with even more briefly. Unlike the provisions of the *Charter*, which, though general, only apply as between the citizen and the government, federal and provincial Acts are specific. They may provide privacy protection, but only in relation to a particular subject-matter.

At the federal level, legislation such as the *Criminal Code* and the *Privacy Act* obviously come to mind. The procedural provisions of the *Criminal Code* regulate the powers

of the police in investigating offences, and substantive offences under the *Code* cover things such as interception of private communications (s.184) and 'watching and besetting' (s.423). The *Privacy Act* deals with data protection in the institutions of the federal government, and the legislation that the federal government is currently developing for the private sector will apply data protection rules to those elements of the private sector that fall under federal legislative competence.

General legislation on privacy does not exist at the federal level. Normally speaking, privacy would be considered to be a subject that falls within provincial legislative competence under s.92 of the *Constitution Act 1867* as a matter of "property and civil rights" within the province. Even if wide-ranging privacy protection legislation were available under one head or another of federal legislative competence -- perhaps the Criminal Law power -- it might still be legitimate to ask, in a paper such as this one, whether civil remedies should be available to individuals under provincial legislation, in addition to whatever protections might be available under the federal laws.

As for privacy protection under provincial Acts, the position is that some specific New Brunswick Acts deal with subject-matter that is often identified as raising privacy concerns, but that there is no general legislation dealing with invasions of privacy as such, either through civil remedies or through the province's power to create so-called 'quasi-criminal' offences on matters within its legislative competence. Existing provincial legislation covering areas that are often of concern from a privacy point of view includes the *Direct Sellers Act*, the *Collection Agencies Act* and the *Private Investigators and Security Services Act*.

c. Common Law

In his book *Privacy and Free Enterprise*, Ian Lawson describes at length a number established common law remedies that may be available when privacy is invaded, depending in each case on the nature of the conduct complained of. He also discusses the possibly emerging tort of invasion of privacy. Among the many established torts that Lawson mentions, the following appear to be the most important.

(i) Trespass to land. This tort permits an occupier of land to decide who is or is not allowed to enter the property. This is obviously an important instrument for preserving 'spatial privacy'. Less familiar is the tort of 'watching and besetting' a person's house or business in order to compel the occupier to do something, which extends the protection of tort law to some actions done *off* the occupier's property. Extended applications of the tort of *nuisance* have also provided protection against some actions done without entry to an occupier's premises. Examples include *Poole & Poole v Ragen and the Toronto Harbour Commissioners* [1958] O.W.N.77, where the plaintiffs won damages and an injunction against the Toronto Harbour police, who for three months had followed the plaintiffs' boat back and forth through the harbour, and *Motherwell v Motherwell* (1976) 73 D.L.R. (3rd) 62, a dispute among family members in which the plaintiff harrassed the defendants by telephoning them an inordinate number of times with complaints about another family member.

(ii) Assault and *trespass to the person.* Under these torts it is wrongful to touch another person without consent. These torts are the basic protections of 'personal privacy', the privacy of one's body.

(iii) Defamation and *breach of confidence.* The long-established tort of defamation involves the publication of false information that harms the reputation of the plaintiff. Breach of confidence, a tort which is itself in the course of evolving, provides a remedy against the disclosure of confidential information which one person obtains from another, and in which the person providing the information has a reasonable expectation of privacy. Both torts obviously apply in the area of 'information privacy'. Another tort that may apply is *injurious falsehood,* the making of untrue statements with a view to causing pecuniary damage. As with defamation, the information must be false, but unlike defamation, it is not necessary that the statements be harmful to the reputation of the plaintiff.

Traditionally, in countries such as Canada, Australia and the United Kingdom, the question of whether legislative measures are required for the protection of privacy has depended on an assessment of the adequacy of torts such as these. More recently in Canada the question has been complicated by the emergence of a small number of cases suggesting that invasion of privacy may be in the course of becoming established as a tort by virtue of judicial decisions, without the need for *legislative* intervention. Cases include *Saccone v Orr* (1981) 34 OR (2d) 317, where the defendant secretly recorded a telephone conversation with the plaintiff and subsequently played it at a town council meeting, and *Roth v Roth* (1991) 4 OR (3d) 740, where a dispute between neighbours over the use of an access road led to a general campaign of harrassment that was held to include an infringement of the plaintiffs' privacy.

On the question of whether the established tort remedies are sufficient there are two schools of thought. One says that they are. The argument here accepts that there is no specific right of action for invasion of privacy, but points out that there is no express remedy for other important human rights such as "liberty" or "security of the person" either. Rights such as these, it is said, are abstract, and like the right to privacy, they are generally enforced through a variety of specific remedies, with different remedies -- an action for false imprisonment, an application for *habeas corpus*, and so on -- being available in different situations.

The existing remedies, on this argument, are substantially adequate to the task of protecting privacy, and if specific inadequacies in them can be demonstrated, the better approach is to revise the existing remedy rather than to invent a completely new one. Experience in America is referred to as suggesting that an apparently broad 'right of privacy' will in fact resolve itself into a small number of claims which are similar in nature to existing torts. Concern is expressed that a tort of invasion of privacy would be an unknown quantity, and might interfere with other important values such as freedom of expression and the freedom of the press.

The other side of the argument is that privacy is a clear enough concept that it can be satisfactorily defined, and that it is an important enough value that it should be protected expressly. On this view the existing tort remedies would be considered inadequate to the task, because each has its own conceptual framework, and each will fall short in particular situations. A classic example might be a case such as the English case of *Kaye v Robertson* (Appendix I to the *Report of the Committee on Privacy and Related Matters* -- the "Calcutt Committee" -- 1990, HMSO). Here newspaper reporters entered a hospital room where a celebrity was recovering from brain surgery after a serious accident. The reporters ignored notices to keep out. They interviewed the patient and took photographs. They said that the patient did not object, though in the view of the Court of Appeal, it was and should have been obvious to the reporters that the patient was in no condition to consent. The reporters then proposed to publish the photographs and an article based on the interview. In the absence of a cause of action for invasion of privacy, the patient tried to prevent publication on grounds of libel, malicious falsehood, trespass to the person and passing off. All he succeeded in getting, however, was an injunction to the effect that the newspaper could not publish anything implying that he had consented to the interview. Bingham L.J. commented:

> The Defendants' conduct towards the Plaintiff here was a "monstrous invasion of his privacy" (to adopt the language of Griffiths J in *Bernstein v Skyviews Ltd.* [1978] QB 479 at 489G). If ever a person has a right to be let alone by strangers with no public interest to pursue, it must surely be when he lies in hospital recovering from brain surgery and in no more than partial command of his faculties. It is this invasion of his privacy which underlies the Plaintiff's complaint. Yet it alone, however gross, does not entitle him to relief in English law.

Both sides of the argument about a tort of invasion of privacy are credible. Both also depend to a large extent on their proponents' differing views as to the ability of legislators or the courts to find a definition of 'invasion of privacy' that is both clear and manifestly useful. Those who would prefer to work with the established torts fear that establishing a broad concept of invasion of privacy would raise more questions than it answered. Among these was the Calcutt Committee, which, despite cases such as *Kaye v Robertson*, felt that other measures, including the establishment of some focused criminal and civil remedies, was preferable to creating a wide-ranging tort of invasion of privacy. On the other hand, those who prefer an express remedy for invasion of privacy consider that a workable definition can be established, and that without it the law will never be able to focus directly on the real problem.

A.2. A Tort of Invasion of Privacy?

To provide the material on which this discussion can reach a conclusion, this Paper will take much the same approach as it took in relation to data protection and the CSA Code. On the basis of the *Uniform Privacy Act* it will state a number of propositions about how legislation establishing a tort of invasion of privacy might be expressed. There can then be public debate about whether legislation in these or similar terms would be desirable. The

Uniform Act is presented in its entirety in Appendix C. A slightly revised approach derived from the propositions in this Part of this Paper is presented in summary form in Appendix D.

a. "Invasion of privacy"

The key elements of the *Uniform Act* are (a) a broad statement that "Violation of the privacy of an individual by a person is a tort that is actionable without proof of damage" (s.2); (b) a list of specific activities that will "in the absence of evidence to the contrary" be considered to be a violation of privacy (s.3); and (c) a list of defences (s.4). This general framework is common to the other Canadian legislation as well -- though the statutes vary on the question of whether it is only individuals (as opposed to corporations, for example) who can sue for an invasion of privacy.

The activities that the *Uniform Act* identifies as presumed invasions of privacy are (in abbreviated form) (a) auditory or visual surveillance of the individual, (b) listening to or recording another person's conversations, (c) publication of letters, diaries or other personal documents, and (d) wrongful dissemination of information concerning an individual. This list is not exhaustive; other unlisted acts may also be found to amount to an invasion of privacy.

The defences (similarly abbreviated) are (a) that the plaintiff consented to the activity, (b) that the defendant acted in lawful defence of person or property, (c) that the activity was authorized or required by law, (d) that the defendant was lawfully investigating an offence, (e) that the defendant's action was reasonable, having regard to any relationship, domestic or otherwise, between the parties, (f) that the defendant neither knew nor reasonably should have known that his or her act would violate the privacy of any individual, and (g) that the act complained of was a reasonable publication in the public interest.

One thing that this approach does not contain is a general description or definition of what an invasion of privacy is. The defences identify things that are *not* an invasion of privacy, and the examples identify some specific activities that are *likely* to be an invasion of privacy, but beyond that the key statement in the legislation is simply the open-ended statement that a "violation of the privacy of an individual . . . is a tort."

Is this acceptable, or should legislation try to be more explicit? The calculation of the *Uniform Act*, and others like it, is presumably that if legislation tries to explain what an "invasion of privacy" is, it will restrict the ability of the courts to develop this new tort in the context of the specific cases that come before them. The argument on the other side is that without at least some sort of definition, the new tort is unacceptably vague.

In principle, one would think, a general description of what an "invasion of privacy" is would be a useful feature of legislation. The following Proposition therefore suggests one. If the definition is satisfactory, it could be part of an enactment. If it is not, approaches more like that of the *Uniform Act* might be more acceptable.

This definition, one should note, would not have to be complete in the sense of, say, the 'fundamental privacy rights' described by the House of Commons Standing Committee on Human Rights and the Status of Disabled Persons. The definition would be intended as a description of an actionable wrong rather than of a human right, and would proceed on the basis that other torts will continue to exist, so that invasions of privacy by trespass, assault, libel, breach of confidence, and so forth, would continue to be dealt with by other means. The purpose of the definition would be to describe the essence of the new tort that the legislation was to add to the existing catalogue.

Proposition #35

An invasion of privacy might be defined as follows:

An act is an invasion of privacy

(a) if it unduly intrudes into the personal affairs of an individual, or into his or her activities, whether in a public or a private place, or

(b) if it gives undue publicity to personal information concerning an individual.

If a definition along these lines would be too limiting, is an approach like that of the *Uniform Act* acceptable, or is it too uncertain? It should be noted here that some of the existing provincial Acts spell out in more detail the 'unreasonableness' criterion that the *Uniform Act* mentions briefly as a defence under s.4(1)(e). British Columbia's Act, for example, says:

> 1(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
>
> 1(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.

Other existing legislation in the common law provinces (but not Quebec) is also more cautious than the *Uniform Act* in describing the kind of conduct that will amount to an invasion of privacy. In B.C., Saskatchewan and Newfoundland it is only where a person "wilfully and without a claim of right" violates the privacy of another that he or she commits a tort. In Saskatchewan the expression is "substantially, unreasonably and without claim of right".

Whether qualifiers of this sort would be necessary in legislation establishing a tort of invasion of privacy would depend to a considerable extent on whether the legislation

contained a general definition of an invasion of privacy along the lines of Proposition #35. Generally speaking, one would have thought that a 'reasonableness' test would be an appropriate element of the legislation. Establishing a 'wilfulness' threshold, however, might well seem excessive.

Proposition #36

If a definition along the lines of Proposition #35 would be too limiting, invasion of privacy legislation should at least contain an 'unreasonableness' threshold before conduct would be considered to amount to an invasion of privacy.

One of the specific examples of invasion of privacy in s.3 of the *Uniform Act* is this:

(d) dissemination of information concerning the individual that has been gathered for commercial or governmental purposes if

(i) the dissemination is contrary to a statute or regulation, or

(ii) the information was provided by the individual in confidence, and the dissemination is made for a purpose other than the purpose for which the information was provided.

The general defences in the Act would apply, of course, including 'consent' and 'reasonableness' (see below).

There is an obvious link here to data protection issues. S.3(d) can be seen as a demonstration of how a tort statute might attempt to get to the essence of data protection legislation in a few short words that might perhaps make more extensive legislation unnecessary. S.3(d) does not have a counterpart in the Privacy Acts of B.C., Alberta, Saskatchewan or Newfoundland. In Quebec, however, basic data protection principles are found in arts.37 to 41 of the *Civil Code*; the more extensive public sector and private sector data protection statutes are an extension of the *Civil Code* provisions.

One would obviously have to think carefully about a provision like s.3(d) before deciding that it should be included in an invasion of privacy statute. If New Brunswick adopts data protection legislation along the lines described in Part I of this Paper, the data protection Act would presumably be the place where the legislative policy on civil remedies was set out -- whether, ultimately, that policy included them or deliberately excluded them. If, however, data protection legislation is not eventually adopted, s.3(d) might deserve further study. It appears to be narrower in scope than a data protection Act, which might make it more acceptable. On the other hand, if the present consultation indicates that private sector data protection legislation is not desirable, the reasons may be such that s.3(d) would be equally undesirable.

Proposition #37

A decision on whether 'wrongful dissemination of information about an individual' might amount to a tort of invasion of privacy should await the outcome of the consultation on private sector data protection legislation.

b. Defences

Next comes the question of whether the specific defences in s.4 of the *Uniform Act* are appropriate and need to be stated. Here again there is substantial consistency between the provincial Acts. It is common ground that there should be a defence against actions for invasion of privacy if the defendant acted with consent, or in lawful defence of person or property, or was authorized by law, or acted for law enforcement purposes, or published information in the public interest. Two features of the *Uniform Act* that are less standard, though, are s.4(1)(d) -- that the conduct is "reasonable, having regard to any relationship, domestic or otherwise, between the parties" -- and s.4(1)(e) -- that the defendant "neither knew nor reasonably should have known that the act, conduct or publication would violate the privacy of an individual." Both of these seem acceptable in substance, though exactly where they belong in legislation would depend on whether a general definition of 'invasion of privacy' or a 'reasonableness threshold' were a part of the legislation.

One other small point is that the *Uniform Act* deliberately omitted one specific defence that appears in the Saskatchewan Act alone. This is that the act complained of "was that of a person engaged in news gathering . . . for any newspaper . . . or . . . broadcaster . . . and such act was reasonable in the circumstances and was necessary for or incidental to ordinary news gathering activities." The report prepared for the Uniform Law Conference argued that a special provision for news-gatherers was not appropriate: that if such a provision gave news-gatherers any real protection it was, in effect, giving them a special privilege that allows them to violate the privacy of individuals.

Proposition #38

In substance, the defences listed in s.4 of the *Uniform Act* are appropriate.

c. Remedies

S.5 of the *Uniform Act* deals with remedies. It spells out that a court can award damages and grant injunctions, can order the defendant to account for any profits arising out of the invasion of privacy or to return any items obtained from it, and can grant any other relief to the plaintiff that the court considers necessary in the circumstances.

These remedies are substantially common to the Saskatchewan, Manitoba and Newfoundland Privacy Acts. By contrast, B.C's Act and the privacy provisions of Quebec's *Civil Code* say nothing about remedies, relying on the general law on the subject. Which approach is preferable is largely a matter of technical judgment, based on one's best assessment of what the courts will do either with or without statutory guidance on the subject.

In substance, however, s.5 seems to contain a reasonable statement of what the available remedies should be.

Proposition #39

The remedies described in s.5 of the *Uniform Act* should be available for an invasion of privacy, though they may not need to be expressly stated in legislation.

S. 6 of the *Uniform Act* goes on to mention a variety of things that a court can consider in assessing damages for an invasion of privacy. These include things like "the nature of the act . . . and the context in which it occurs" and "the conduct of the plaintiff and of the defendant before and after the act . . . including any apology or offer of amends made by the defendant." The section also makes clear that the court may award punitive damages in appropriate cases.

Though the section does not seem objectionable, this is probably one of those cases in which the less the legislation says, the better. The main effect of s.6 is to make it clear that the conduct of the defendant can be relevant to the calculation of damages for an invasion of privacy, but it is doubtful that this really needs to be said -- or more importantly, perhaps, it is doubtful that it should be highlighted as compared to other factors that might be equally important. The courts in Quebec have several years' experience of developing damage awards for invasions of privacy, and in the few recent cases from Ontario, figures have been developed in which the harm done was not measured simply in terms of financial loss. The actual level at which damage awards would be set would probably take some time to become settled, whether under a provision like s.6 or without such a provision, but even without such a provision the courts could be relied on to develop appropriate measures.

Proposition #40

The rules on calculation of damages for a tort of invasion of privacy could satisfactorily be left to be developed by the courts.

d. Technical matters

The *Uniform Act* closes with some provisions on technical legal matters -- the relation of this tort to other torts, and whether the Act binds the Crown. Other existing provincial Acts deal with things like limitation periods, precedence as between this Act and other Acts, the inadmissiblity in civil proceedings of evidence obtained in violation of the Act and the question of whether it is possible to 'invade the privacy' of a person who is deceased.

Technical issues of this sort do not need to be discussed in any detail here. The best approach to dealing with them seems to be to adopt the general policy that the tort of invasion of privacy, if established by legislation, should be a tort like any other. From this general principle answers to most of these technical issues would follow. The one item that has more

substance, though, is the question of whether one can 'invade the privacy' of a person who is deceased. The most natural answer seems to be "no," especially following the idea set out in relation to s.2 of the *Act* that only individuals can sue for an invasion of privacy. B.C., Saskatchewan and Newfoundland appear to take this one step further, and say that if an invasion of privacy occurs before a person dies, the right of action is extinguished by his or her death. Whether this is the right approach would require further consideration.

Proposition #41

Technical questions on matters such as limitation periods, binding the Crown, precedence of Acts and admissibility of evidence should be decided on the basis that the tort of invasion of privacy, if established by statute, would be established as a tort like any other. There should be no right of action for an invasion of the privacy of a person who is deceased.

A.3 To Legislate or Not?

With the assistance of the discussion of the *Uniform Act* one can now return to the main question that this Section considers. Should there be legislation to establish a tort of invasion of privacy or not? Two possible legislative models are presented in the appendices. Appendix C is the *Uniform Act*. Appendix D states in summary form a slightly different approach based on the propositions in this paper. The two would be similar in effect. The main differences are (1) that Appendix D includes a generic definition of 'invasion of privacy', while Appendix C does not, and (2) that Appendix D excludes the material on remedies that Appendix C contains. In their outlines, however, the two are comparable. A decision to enact invasion of privacy legislation requires a decision that legislation substantially along these lines is desirable.

As was stated earlier, there are three main conclusions that the present consultation could reach. One is that legislation substantially similar to the *Uniform Act* should be adopted. Another is to decide that there should not be a tort of invasion of privacy at all. The third is to say that *if* there is to be a tort of invasion of privacy, it should be left to be developed by the courts rather than established by legislation. The arguments for these last two positions have not been mentioned for some time. They therefore deserve a brief review before the discussion closes.

"There should not be a tort of invasion of privacy."

The general argument against a tort of invasion of privacy is, in short, that the tort is unnecessary, undefinable, inappropriate and misconceived. It is unnecessary because other established tort remedies are substantially adequate to protect privacy interests. It is undefinable because privacy is too subjective a concept to support a workable legal definition. It is inappropriate because it presents too great a threat to desirable activities (e.g. legitimate reporting) to counter too small a problem. It is misconceived because it ignores the necessary

give and take of everyday life, assuming too readily that any insult to one's dignity must necessarily give rise to a legal remedy.

These are issues on which the legislative models discussed in this Paper can cast some light. One can start with the question of definability: discussion of the legislative models will determine whether the tort is satisfactorily described. One can then move to the question of appropriateness: does legislation along these lines actually pose a threat to desirable activities, or does it not? Whether the tort is misconceived also depends heavily on the way in which the legislation is expressed: does it accurately capture those kinds of insults to dignity that *should* be the subject of a legal remedy, or does it go too far. Whether the tort is necessary, however, cannot be assessed by considering the terms of the tort alone. There are certainly some gaps in the established tort remedies that a tort of invasion of privacy might fill. For the opponents of the tort, however, those gaps are small and tolerable.

One should probably add that if the present consultation leads to the conclusion that there should *not* be a tort of invasion of privacy, it would presumably be appropriate to look again at the common law on the subject, and to consider whether its further development in New Brunswick should be nipped in the bud. That, however, is a decision for another day.

"If there is to be a tort of invasion of privacy, it should be developed by the courts, not by legislation."

The argument here is primarily one of method, but issues of substance are also involved.

When torts are developed by the courts, the process evolves step by step, one case at a time. As more cases are decided, similarities and connecting principles emerge. Sometimes new principles evolve as courts look at old decisions in a new light. The advantage of this is that the law develops gradually, and each decision comes with a particular set of facts that illustrate what, in practical terms, the tort really amounts to. The disadvantage is that development by this method can be slow and unpredictable. It depends on the facts that litigants present to the courts and on the decisions that judges reach on those facts.

In Canada there appears to be enough case-law now that the courts in New Brunswick could develop a tort of invasion of privacy if suitable cases were presented to them. On the other hand, it is also possible that they might decide not to. They might, for example, accept the argument that a general tort of 'invasion of privacy' is just too vague to be acceptable. They might decide that other existing torts provided more appropriate legal frameworks for deciding the disputes that were litigated. Each case would contain a reasoned explanation of why the court decided as it did. If a tort of invasion of privacy failed to become established through the case-law, it would presumably be because experience suggested that the potential tort contained inherent difficulties that were too great to be resolved.

A decision that a tort of invasion of privacy should be developed by the courts (if at all) reflects a preference for a gradual approach to the development of the law in this area, a preparedness to 'wait and see', and to accept that perhaps the results of the process may be different from what, at the outset, one might think to be desirable. This would apply not only to the question of whether the tort should be recognized at all, but also to its details if it were. On matters such as whether a corporation could have 'privacy' that could be 'invaded', for example, a court might reach a different conclusion from the one suggested in this Paper.

If there is substantial ambivalence about whether a tort of invasion of privacy should exist, and if so, how it might be described, taking a 'wait and see' approach might be sensible. As things stand, it seems more likely than not that a tort of invasion of privacy will become established through case law -- some would argue that the tort is already established, though not yet developed -- but one cannot predict the future. The only way of making it certain, now, that the tort exists is to enact legislation. The risk, though, is that if legislation is poorly expressed, it may restrict developments that would otherwise occur more satisfactorily through the case-law. This is a criticism that has been made of, for example, the expression "wilfully and without claim of right" that determines which "violations of privacy" are actionable under some of the existing Canadian Privacy Acts.

Proposition #42

Key issues for public discussion are

(a) whether an invasion of privacy should be a tort at all,

(b) whether legislation based on the *Uniform Act* would adequately describe an 'invasion of privacy' and pose no threat to desirable activities,

(c) whether caution dictates that the development of the tort should be left to the courts rather than undertaken by legislation.

B. Non-Judicial Remedies for Infringements of Privacy

The question in this Section is whether non-judicial remedies -- remedies available from an administrative agency or official rather than from the courts -- should be established for infringements of privacy. The word "privacy" is still being used here in the broad sense adopted by the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, as a broad human right encompassing physical privacy, privacy of personal information, freedom from surveillance, privacy of personal communications and privacy of personal space. The word "infringement" is used to create a distinction with the discussion of "invasion" of privacy in the previous Section. An "invasion" of privacy was presented there as being conduct that was sufficiently unacceptable to entitle the aggrieved party to the legal remedies of damages, declarations and injunctions. An "infringement" of

privacy, by contrast, might be a broader term. Any action that is insufficiently respectful of the privacy of another could perhaps be considered an "infringement" of his or her privacy. But not all "infringements" of privacy would necessarily amount to an "invasion" of privacy, a tort.

The use of this terminology makes it possible to differentiate two separate reasons why one might consider establishing non-judicial remedies for infringements of privacy. One is that even in cases where a legal remedy might be available, a non-judicial remedy might be more desirable -- for reasons of cost, convenience, or whatever. The other is that in some cases the conduct complained of might not constitute a tort, but it might still be thought that it was less than satisfactory, and that there should be some official means of making that point (whether or not with a sanction attached) and of attempting to set standards for the future.

The other reason, of course, for considering non-judicial remedies for infringements of privacy in this Paper is that the same issue has already been examined in the narrower context of data protection. It would be wrong to assume, without further discussion, that data protection was the only context in which non-judicial remedies might be appropriate. Indeed, some people may argue that the case for non-judicial remedies is stronger at the general level than in relation to data protection in particular. They might also suggest that non-judicial remedies for data protection could easily be included within a broader privacy mandate.

The discussion in this Section will be similar in part to the discussion in Part I. Comparable questions arise as to what an administrative agency might do and what its powers might be. In part, however, the issues here are different. When administrative remedies were considered earlier, it was on the basis that there was a fixed set of rules to be enforced -- the fair information practices of the CSA Code -- and the question was whether the courts, or an administrative body, or both, should do the job. In relation to infringements of privacy, however, there is no fixed set of rules at the centre of the discussion.

B.1 "Infringements of Privacy"

An obvious question to ask here is what the "infringements of privacy" are that a non-judicial remedy might deal with. Infringements of privacy come in different shapes and sizes, and in different forms at different times. A traditional source of complaint has been the allegedly intrusive activities of reporters and photographers. More recently there have been concerns about a number of workplace-related matters. Employers have required employees to be tested for drug use, for example, or to take lie-detector tests. There have been questions about whether employers should or should not have access to employees' e-mails, which may be personal, and about what kinds of performance monitoring are acceptable. The increasing use of surveillance devices, whether overt or covert, and in both public and private places is another source of expressed concern about what some people feel to be a progressive loss of privacy in modern society.

There are also, of course, things that some people consider to be significant privacy issues but others do not. Caller identification on telephone recievers might be an example. Some people object to the fact that their name or the number they are calling from may be automatically displayed to the receiver of the call. Others would feel differently. Another example might be telephone solicitations. Some people may feel these are an infringement of their privacy. Others may find them inoffensive -- though perhaps there might be a point at which the solicitations became so frequent that they would change their minds.

Behind these specific examples is the more general proposition that privacy itself is always a matter of concern, and that though one may never be able to predict exactly what kinds of conduct may be current as privacy issues at any particular point in time, there will always be something. A non-judicial remedy for infringements of privacy, therefore, would be permanently available to deal with whatever the issues of the day might be.

Proposition #43

There are many actual and potential privacy issues that would fall outside the scope of either a judicial remedy for invasion of privacy or a non-judicial remedy under data protection legislation.

B.2 Beyond a Social Sanction?

It is entirely possible to agree with everything that has been said so far in this Section, but still not not reach the conclusion that a non-judicial remedy for infringements of privacy should be established. One can accept that there are now, always have been, and always will be issues of concern in relation to privacy without necessarily believing that we need either laws or bureaucracies to deal with them. The true sanction for an infringement of privacy, on this view, is the social sanction -- questionable practices will be abandoned if enough people find them objectionable -- and the true yardstick of an infringement of privacy is the vigour, or lack of it, of the social response -- unless enough people object, the action in question is not an infringement of privacy at all, when assessed by the acid test of actual social standards.

The very breadth of the notion of an 'infringement of privacy' might be viewed by some as a reason for caution. So many of the things that we say or do in relation to other people could potentially be viewed by them (though presumably not by us) as infringements of their privacy. Establishing a non-judicial remedy might be seen as opening the doors to large volumes of complaints, many of them about things that people should simply have to deal with as best they can as part of the give and take of living in society.

In a 1973 *Report on the Law of Privacy*, prepared for the Parliament of New South Wales, Australia, W.L. Morrison captures some of the ambivalence that surrounds the issue:

> The continuing dilemma of bodies called upon to make recommendations on this subject and of legislatures called upon to resolve on bills brought before them has been that generally such proposals as have been put before them have provided for an extraordinary degree of discretion in the bodies who would be entrusted with the implementation or application of the legislation. Since these bodies are always inevitably themselves governmental bodies such legislation always itself raises the prospect of a new arbitrary governmental interference with the freedom of the individual to offset the advantages offered in the direction of the protection of privacy.
>
> . . . The wide discretions reposed in those called on to implement proposed legislation are a result of the inability of those framing it to delineate with any precision the problems which will arise in the future over so wide a range and what precisely is to be done about them. Hence the buck is passed to the subordinate body provided for in the legislation (p.15).

Morrison's report did, however, recommend the establishment of a non-judicial remedy for infringements of privacy, in the form of a non-intrusive Ombudsman-type agency, with powers to advise, inform, investigate and conciliate, but with no compulsory powers. The recommendation led to the creation of the New South Wales Privacy Committee, more information about which will be given below.

The key issue, though, is whether privacy, in the broad sense, has now gone beyond the stage at which it can safely be left as a matter of social relations, which people should sort out among themselves, and has reached the point at which some form of official agency has to be drawn in to influence the practices either of individuals or organizations or of society at large. If society in general, or particular groups in society, need guidance on appropriate standards of respect for privacy, or if individuals need help in resolving privacy-related disagreements, non-judicial remedies might well be appropriate. If, on the other hand, infringements of privacy are a matter best left predominantly in the social sphere, creating non-judicial remedies would be inappropriate.

Proposition #44

The key issue for public discussion is whether infringements of privacy should be left as issues within the social sphere, or whether the involvement of an administrative agency would be beneficial in ensuring proper respect for individual privacy.

B.3. Possible Models

There are many ways in which a non-judicial privacy agency could be constituted. In Australia, the New South Wales Privacy Committee offers one example. The Committee's website (http://www.agd.nsw.gov.au/privacy.html) states:

> The Privacy Committee is a New South Wales statutory body created in 1975 under the Privacy Committee Act to investigate and report on privacy issues affecting the people of New South Wales. The Committee performs an Ombudsman type role and does not enforce specific privacy legislation.
>
> The Privacy Committee promotes and protects the right to privacy by
>
> Advising individuals, government agencies and business organisations on what action they can take to protect the right to privacy
>
> Researching significant developments in policy, law and technology which have an impact on privacy, and making reports and recommendations to relevant authorities
>
> Investigating and where possible conciliating complaints about breaches of privacy and
>
> Answering inquiries and educating the community about privacy issues.

In Quebec the legal structure is very different, but the practical results are perhaps somewhat similar -- at least until one considers data protection. In Quebec the Human Rights Commission has a responsibility to promote the Quebec *Charter of Human Rights and Freedoms*. This *Charter* includes the provision in art.5 that "Every person has a right to respect for his private life." The Commission's promotion of art.5 (along with other provisions of the *Charter*) includes public education activities and analyzing and commenting upon laws and policies. The Commission also issues opinions on matters that come to its attention, forwarding its advice to appropriate parties, and it has the power to intervene in litigation between third parties that involves the interpretation of the *Charter*. However, it has no formal investigatory powers in relation to infringements of privacy as such. On an informal basis it can attempt to assist and conciliate in matters that are brought to its attention, but its formal complaints procedures only apply in cases of discrimination. Privacy issues can sometimes be implicated in complaints of discrimination -- for example, complaints about medical screening for inherited disease might have both privacy and discrimination aspects -- but when the privacy issues stand alone, the Commission has no formal investigatory powers.

This can be contrasted with Quebec's (separate) Access to Information Commission. This Commission only has data protection functions, but it has a wide-ranging power to recommend or order remedial measures, and any order it gives is enforceable as though it were an order of a court.

If non-judicial remedies for invasions of privacy were felt to be desirable in New Brunswick, the alternatives would be either to create a new remedy or to expand the functions of an existing agency. Among existing agencies, the New Brunswick Human Rights Commission seems the most likely candidate, given the established status of privacy among

the internationally recognized human rights. This, though, would involve a substantial change of mandate for the Commission. The Commission currently only deals with complaints of "discrimination" on various enumerated grounds and in specified settings. Nonetheless, if any existing agency is to be chosen, its existing role as a human rights agency seems naturally to attract the human right of privacy.

If a privacy mandate were conferred on the Commission, this would also be likely to attract the Commission's existing implementation powers. These include the power to educate and inform, as well as the power to investigate and mediate complaints. If mediation is unsuccesful, the Commission also has the power to ask the responsible Minister to call a formal inquiry, out of which binding orders may be issued. Prosecutions can also be brought, with the approval of the Minister. However, if it were decided that these powers were not as suitable for infringements of privacy as they are for the existing mandate in relation to discrimination, appropriate legislative amendments could be made.

If, by contrast, a new remedy were created, all options would be on the table. A specific privacy agency with mandatory powers might be one option. An Ombudsman-type agency like the New South Wales Privacy Committee might be another. A further possibility might be not to create a standing agency, but to create, instead, a mechanism under which somebody could be appointed to deal with specific complaints of infringement of privacy as they were received.

The alternatives here are comparable to the ones that were discussed in Part I in relation to administrative remedies for data protection legislation. Comparable also is the importance of determining whether resolving complaints should be the full extent of the mandate and what part, if any, compulsory powers should play in the scheme. Some people might question the value of a something like the New South Wales Privacy Committee on the ground that, when the going gets tough, it has no real powers. On the other hand, W.L. Morrison's explanation of the difficulty of assigning compulsory powers to an agency with a wide and indistinct privacy mandate has some force.

The provisions of New Brunswick's *Human Rights Act* provide an interesting half-way house here. The Commission's basic responsibity is that it "shall inquire into any complaint made pursuant to section 17 and shall endeavour to effect a settlement of the matter complained of" (s.18(1)). The Commission has no independent power to enter premises, inspect records or compel the production of evidence, but a judge of the Provincial Court can authorize the Commission to designate a person to exercise those powers for the purpose of effecting a settlement (ss.18, 19 and 19.1). The Commission cannot itself hold hearings or issue orders. Instead it applies to the responsible Minister for a decision that an inquiry should be held (s.20). It is the board of inquiry, not the Commission, that will issue any orders, and the board's order can be filed with the Court of Queen's Bench and enforced as though it were an order of the court (s.21).

Some people may feel that this approach provides a nice balance between a substantially conciliatory role and the *possibility* that compulsory measures may sometimes be needed. (They might also suggest that a similar pattern could be appropriate for a pure data protection agency if, ultimately, administrative remedies were only extended that far.) On the other hand, it might be argued that there is no middle ground between between having compulsory powers and not having them, and that if provisions such as those in the *Human Rights Act* appear to soften the element of compulsion, the appearance is deceptive.

Proposition #45

Models exist on which non-judicial remedies for infringements of privacy could be based. Key issues for public discussion, here as they were in relation to data protection remedies, are

(a) whether non-judicial remedies should include compulsory powers;

(b) whether dealing with complaints should be the full extent of the role.

Conclusion

The various legislative possibilites described in this Paper are, at one and the same time, both independent and potentially interdependent. Each can be considered in its own right, and all of them, any of them, or any combination of them, could be enacted. Alternatively, none of the measures described in this Paper might be adopted, and it still might be argued that privacy enjoys as much legal protection in New Brunswick as it needs. The various alternatives will be explained briefly, starting with the last.

Adopting no new legislative measures for privacy protection would mean that private sector data protection legislation was not needed, that the existing common law protections for privacy interests (including the probably-evolving tort of invasion of privacy) were adequate, and that non-judicial remedies for infringements of privacy in the broad sense were not required. The first element would presumably reflect the idea that self-regulation and social forces will be sufficient in the data protection field, or at least that they will be as effective as legislation is likely to be. The second element would presumably be based both on the coverage provided by the existing torts and on concerns about the possible open-endedness of any new tort of invasion of privacy. The third element would presumably accept the argument that infringements of privacy should remain largely in the social sphere, and that a privacy agency with a wide-ranging mandate might be a 'cure' that was worse than the 'disease'.

Alternatively, any one of the legislative options discussed in this Paper might be selected in preference to the others. Enacting data protection legislation alone would reflect the idea that this was the only one of the issues discussed that had now gone beyond the stage where social forces were an adequate protection. Enacting tort legislation alone might be presented as creating the one real protection that should have *legal* recognition; it could be said that this went to the heart of both the data protection and infringement of privacy issues, establishing the one point at which it was appropriate that the law, specifically, should become involved. Finally, creating a wide-ranging non-judicial remedy for infringements of privacy could be seen as a complete answer in itself; since the agency could cover *all* privacy issues, there would be no logical need for anything more.

Combining any two of the options can also be justified, as can combining all three. All three are in fact combined in Quebec's current legislation, where there is an Access to Information Commission that deals with data protection in both the public and the private sector, a tort under the Civil Code for invasions of privacy in general, as well as specific torts based on the key elements of data protection principles, and a Human Rights Commission with a mandate in relation to privacy under the Quebec *Charter of Human Rights and Freedoms.*

Which path should New Brunswick choose? That question is now open for discussion.

APPENDIX A

SUMMARY OF PROPOSITIONS

I. Data Protection in the Private Sector

A. Is there a need for private sector legislation?

Proposition #1

The general objectives of data protection initiatives are laudable. Key questions for public discussion are

(a) whether legislation is the right way of advancing those objectives,

(b) whether legislation would achieve its objectives, and

(c) whether its benefits would justify the costs and restrictions it imposed.

B What might data protection legislation say?

Proposition #2

Possible data protection legislation for the private sector should take the Canadian Standards Association's *Model Code for the Protection of Personal Information* as its starting point.

Proposition #3

Data protection legislation should adopt the ten "Principles" of the CSA Code verbatim, as far as possible. The "Definitions," "Notes" and "Commentary" in the CSA Code should serve as source material for data protection legislation, with key elements being adopted as appropriate.

B.1 The scope of data protection legislation

a. To whom will the Act apply?

Proposition #4

Data protection legislation could apply to all incorporated and unincorporated organizations, and to individuals when they collect and use personal information for purposes other than personal and household ones.

b. What is meant by "personal information"?

Proposition #5

Data protection legislation could adopt the CSA Code's definition of personal information: "information about an identifiable individual that is recorded in any form."

B.2 The CSA Principles

CSA Principle 1 - Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Proposition #6

Unless and until a designation is made under CSA Principle 1, the person accountable for an organization's compliance with the data protection principles should be

(a) the organization's Chief Executive Officer, if it has one; or

(b) in an organization without a Chief Executive Officer, the person or persons who control the affairs of the organization.

CSA Principle 2 -- Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Proposition #7

The purposes for which an organization collects personal information must be legitimate and must directly relate to an existing or proposed activity of the organization.

Proposition #8

CSA Principle 2 could be supplemented by a requirement that organizations document the purposes for which they maintain personal records systems, but if it is, such a requirement should not apply where documentation would be superfluous to proper administrative controls.

Proposition #9

Where an organization's documented purposes do not match the explanation given to the individual, the latter should prevail, in accordance with CSA Principle 3 -- Consent.

CSA Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

a. Wording

Proposition #10

The essence of CSA Principle 3 is "consent." Data protection legislation should not include "knowledge" as a separate and independent criterion which must be satisfied.

b. Express and implied consent

Proposition #11

Data protection legislation must include the concept of implied consent, based on the reasonable expectations of the individual.

Proposition #12

The actions for which consent can be implied should be those that the individual should reasonably expect the organization to take, and would be unlikely to disapprove of, having regard to

(a) the nature of the personal information in question, including whether it is or is not sensitive or confidential,

(b) any benefit or detriment to the individual,

(c) any explanation that the organization has given of its intended actions,

(d) any indication that the individual has given of his or her actual wishes, and

(e) the ease or difficulty with which the actual wishes of the individual might be discovered.

c. "Except where inappropriate"

Proposition #13

Consent should not be required when an organization collects, uses or discloses personal information

(a) to protect the health, safety or security of the public or of an individual,

(b) for purposes of an investigation related to the enforcement of an enactment,

(c) to protect or assert its own lawful rights, including lawful rights against the individual,

(d) to verify to a government body the individual's eligibility for a program or benefit for which the individual has applied to that body,

(e) for purposes of legitimate research in the interest of science, of learning or of public policy, or for archival purposes,

(f) as required or expressly authorized by law, or

(g) for some other substantial reason in the public interest, whether or not it is similar in nature to paragraphs (a) to (f).

Before collecting, using or disclosing personal information without consent an organization should consider the nature of the information in question and the purpose for which it is acting, and must satisfy itself that in the circumstances that purpose justifies the action proposed.

Any collection, use or disclosure of personal information without consent should be limited to the reasonable requirements of the situation.

CSA Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Proposition #14

Data protection legislation should state the sources from which personal information may be collected, and should state that an individual shall not be refused any service or benefit because he or she declines to provide personal

information which is not necessary for the identified purpose of the organization.

The requirement that personal information be collected by fair and lawful means does not need further explanation in data protection legislation.

CSA Principle 5 -- Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

a. Wording

Proposition #15

CSA Principle 5 should permit uses and disclosures that are "expressly authorized by law" as well as those that are "required by law."

b. Inter-relation of "purpose", "consent" and "the law"

Proposition #16

Data protection legislation need not elaborate upon the relationship between "purposes," "consent" and "the law" as alternative bases for the use or disclosure of personal information.

c. Retention

Proposition #17

Data protection legislation should make it clear that an organization's duty not to retain personal information can be satisfied by converting the information into a form in which the individuals to whom it relates cease to be identifiable.

Proposition #18

Organizations should not be required to purge all personal information from 'non-personal' files in which the personal information appears incidentally.

CSA Principle 6 -- Accuracy

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

Proposition #19

CSA Principle 6 is self-explanatory. Data protection legislation would not need to provide additional guidance on its application and interpretation.

CSA Principle 7 -- Safeguards

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

a. Wording

Proposition #20

The word "security" should be removed from CSA Principle 7 so as not to narrow its scope.

b. What kinds of safeguards?

Proposition #21

Data protection legislation should specify that the safeguards to be implemented include training and physical, technical, administrative and other measures, as appropriate in the circumstances. It should not attempt to define what will make a safeguard "appropriate to the sensitivity of the information."

c. Transfers to third parties

Proposition #22

Data protection legislation should make it clear that "appropriate safeguards" may be required when an organization transfers personal information to another organization, but it should not require specific forms of safeguards.

CSA Principle 8 -- Openness

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

Proposition #23

CSA Principle 8 is self-explanatory. Data protection legislation need not attempt to clarify its meaning.

CSA Principle 9 – Individual Access

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

a. Wording

Proposition #24

The words "except where inappropriate" should be added to the right to information in CSA Principle 9.

b. The nature of the right

Proposition #25

Data protection legislation should make it clear that, under CSA Principle 9, providing *information* is sufficient unless access to documents is specifically requested.

c. Exceptions to access

Proposition #26

An organization should not be required to disclose personal information to the individual

(a) where disclosure would be harmful to the health, safety or security of the public or an individual, including the applicant;

(b) where disclosure would be prejudicial to an investigation related to the enforcement of an enactment

(c) where non-disclosure is required or expressly authorized by law, or where the individual would have no right to obtain the information in legal proceedings;

(d) where the information was provided by another person in confidence, or is confidential in nature;

(f) where the information requested is inextricably linked to the personal information of another individual;

(f) where the information requested would be unduly expensive or onerous to provide.

Consideration should also be given to authorizing non-disclosure when there is some other legitimate and substantial reason for not providing the information requested.

Non-disclosure should be limited to the reasonable requirements of the situation. If it is practicable to explain the substance of the information withheld without prejudicing the reason for withholding it, the organization should do so.

d. Procedure

Proposition #27

Data protection legislation could be silent on the question of access procedures under CSA Principle 9.

e. Corrections

Proposition #28

When the individual has challenged the accuracy or completeness of personal information, but fails to convince the organization, the organization should nake a note that the individual disputes the information in question.

CSA Principle 10 -- Challenging Compliance

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

Proposition #29

An organization should be required to investigate in good faith the complaints it receives and to take appropriate measures when a complaint is found to be justified.

B.3 Other Issues Arising

a. Sectoral Codes

Proposition #30

Sectoral codes should not be given the force of law under data protection legislation. Data protection legislation should include regulation-making authority under which, if necessary, more detailed provision can be made

in relation to particular kinds of organization or information, or particular activities.

b. Enforcement

The penal remedy

Proposition #31

Data protection legislation could make it an offence to wilfully violate CSA Principle 3 (Consent), 4 (Limiting Collection), 5 (Limiting Use, Disclosure and Retention), and 9 (Individual Access).

The civil remedy

Proposition #32

Unless data protection legislation adopts administrative remedies that make civil remedies unnecessary, declarations, injunctions and awards of damages should be available for the enforcement of the legislation. However, awards of damages should only be made where an organization's non-compliance with the Act causes loss and satisfies some additional criterion such as being manifestly inconsistent with the Act.

The administrative remedy

Proposition #33

Administrative remedies are not essential to data protection legislation, but are a policy option. Key issues for public discussion are

(a) whether judicial remedies alone would be appropriate and sufficient,

(b) whether an administrative complaints mechanism without compulsory powers would serve a purpose,

(c) whether an administrative complaints mechanism with compulsory powers would be over-intrusive or counter-productive,

(d) whether a non-complaints function can be identified that is substantial, viable, and a strong reason in itself for devoting resources to an administrative agency with a specific data protection mandate.

II. Privacy in General

A. Judicial Remedies for Invasion of Privacy

Proposition #34

Discussion of a statutory tort of invasion of privacy should be based on the *Uniform Privacy Act* prepared by the Uniform Law Conference of Canada, set against the background of existing judicial remedies that may protect privacy interests.

A.1 Existing Remedies

[No Proposition is presented on this subject.]

A.2 A Tort of Invasion of Privacy?

a. "Invasion of privacy"

Proposition #35

An invasion of privacy might be defined as follows:

An act is an invasion of privacy

(a) if it unduly intrudes into the personal affairs of an individual, or into his or her activities, whether in a public or a private place, or

(b) if it gives undue publicity to personal information concerning an individual.

Proposition #36

If a definition along the lines of Proposition #35 would be too limiting, invasion of privacy legislation should at least contain an 'unreasonableness' threshold before conduct would be considered to amount to an invasion of privacy.

Proposition #37

A decision on whether 'wrongful dissemination of information about an individual' might amount to a tort of invasion of privacy should await the outcome of the consultation on private sector data protection legislation.

b. Defences

Proposition #38

In substance, the defences listed in s.4 of the *Uniform Act* are appropriate.

c. Remedies

Proposition #39

The remedies described in s.5 of the *Uniform Act* should be available for an invasion of privacy, though they may not need to be expressly stated in legislation.

Proposition #40

The rules on calculation of damages for a tort of invasion of privacy could satisfactorily be left to be developed by the courts.

d. Technical matters

Proposition #41

Technical questions on matters such as limitation periods, binding the Crown, precedence of Acts and admissibility of evidence should be decided on the basis that the tort of invasion of privacy, if established by statute, would be established as a tort like any other. There should be no right of action for an invasion of the privacy of a person who is deceased.

A.3 To Legislate or Not?

Proposition #42

Key issues for public discussion are

(a) whether an invasion of privacy should be a tort at all,

(b) whether legislation based on the *Uniform Act* would adequately describe an 'invasion of privacy' and pose no threat to desirable activities,

(c) whether caution dictates that the development of the tort should be left to the courts rather undertaken by legislation.

B. Non-Judicial Remedies for Infringements of Privacy

B.1 "Infringements of Privacy"

Proposition #43

There are many actual and potential privacy issues that would fall outside the scope of either a judicial remedy for invasion of privacy or a non-judicial remedy under data protection legislation.

B.2 Beyond a Social Sanction?

Proposition #44

The key issue for public discussion is whether infringements of privacy should be left as issues within the social sphere, or whether the involvement of an administrative agency would be beneficial in ensuring proper respect for individual privacy.

B.3. Possible Models

Proposition #45

Models exist on which non-judicial remedies for infringements of privacy could be based. Key issues for public discussion, here as they were in relation to data protection remedies, are

(a) whether non-judicial remedies should include compulsory powers;

(b) whether dealing with complaints should be the full extent of the role.

APPENDIX B

THE PUBLIC SECTOR ACT

CHAPTER P-19.1

Protection of Personal Information Act

Assented to February 26, 1998

Chapter Outline

CHAPITRE P-19.1

Loi sur la protection des renseignements personnels

Sanctionnée le 26 février 1998

Sommaire

Her Majesty, by and with the advice and consent of the Legislative Assembly of New Brunswick, enacts as follows:

1(1) In this Act

"agent" means

(a) a person who collects personal information for a public body, and

(b) a person to whom a public body discloses personal information so that the person may provide a service on behalf of the public body;

"personal information" means information about an identifiable individual, recorded in any form;

"public body" means

(a) a body to which the *Right to Information Act* applies, and

(b) any other body, designated by regulation, that is established by a body referred to in paragraph (a) or by a public Act of New Brunswick;

"Statutory Code of Practice" means the code of practice set out in Schedule A.

1(2) Information that relates to an identifiable individual but is collected, used or disclosed in a form in which the individual is not identifiable is not personal information when so collected, used or disclosed.

1(3) An individual is identifiable for the purposes of this Act if

(a) information includes his or her name,

(b) information makes his or her identity obvious, or

Sa Majesté, sur l'avis et du consentement de l'Assemblée législative du Nouveau-Brunswick, décrète:

1(1) Dans la présente loi

«agent» désigne

a) une personne qui recueille des renseignements personnels pour un organisme public, et

b) une personne à qui un organisme public divulgue des renseignements personnels pour qu'elle puisse rendre un service au nom de l'organisme public;

«Code de pratique statutaire» désigne le code de pratique établi à l'Annexe A;

«organisme public» désigne

a) un organisme auquel la *Loi sur le droit à l'information* s'applique, et

b) tout autre organisme, désigné par règlement, qui est établi par un organisme visé à l'alinéa a) ou par une loi d'intérêt public du Nouveau-Brunswick;

«renseignement personnel» désigne un renseignement sur un particulier identifiable, enregistré sous quelque forme que se soit.

1(2) Les renseignements qui concernent un particulier identifiable mais qui sont recueillis, utilisés ou divulgués sous une forme dans laquelle le particulier n'est pas identifiable ne constituent pas des renseignements personnels lorsqu'ils sont recueillis, utilisés ou divulgués de cette façon.

1(3) Un particulier est identifiable aux fins de la présente loi si des renseignements

a) comprennent son nom,

b) rendent évidente son identité, ou

(c) information does not itself include the name of the individual or make his or her identity obvious but is likely in the circumstances to be combined with other information that does.

c) ne comprennent pas son nom ou ne rendent pas évidente son identité mais sont susceptibles dans les circonstances d'être adjoints à d'autres renseignements qui comprennent son nom ou rendent son identité évidente.

2(1) Every public body is subject to the Statutory Code of Practice.

2(1) Tout organisme public est soumis au Code de pratique statutaire.

2(2) The Statutory Code of Practice shall be interpreted and applied in accordance with Schedule B and with any regulations made under paragraph 7(b).

2(2) Le Code de pratique statutaire doit être interprété et appliqué conformément à l'Annexe B et à tous règlements établis en vertu de l'alinéa 7b).

3(1) The *Ombudsman Act* applies to this Act and to the activities of any public body under it, whether or not that public body is otherwise subject to the *Ombudsman Act.*

3(1) La *Loi sur l'Ombudsman* s'applique à la présente loi et aux activités de tout organisme public établi sous son régime, que cet organisme soit ou non assujetti de toute autre manière à la *Loi sur l'Ombudsman.*

3(2) Subject to sections 4 and 6, any complaint of a violation of this Act shall be made to the Ombudsman.

3(2) Sous réserve des articles 4 et 6, toute plainte contre une infraction à la présente loi doit être portée devant l'Ombudsman.

4(1) In relation to a public body to which the *Right to Information Act* applies, an individual may enforce under that Act any right to information that this Act confers.

4(1) Un particulier peut, relativement à un organisme public auquel la *Loi sur le droit à l'information* s'applique, exercer en vertu de cette loi tout droit à l'information que confère la présente loi.

4(2) Subsection (1) does not confer any right to obtain under the *Right to Information Act* information to which there would not otherwise be a right under that Act.

4(2) Le paragraphe (1) ne confère aucun droit d'obtenir des renseignements en vertu de la *Loi sur le droit à l'information* qui ne pourraient de toute autre façon être obtenus en vertu de cette loi.

5(1) Nothing in this Act displaces any duty of confidentiality that exists in relation to personal information under any other Act or law.

5(1) Aucune disposition de la présente loi ne supprime l'obligation de confidentialité à l'égard des renseignements personnels imposée par toute autre loi ou droit.

5(2) Where another Act confers on a public body, or an officer or employee of a public body, a discretion that may be exercised in relation to personal information, that body or person shall have regard to this Act in the exercise of that discretion, to the extent that the other Act allows.

5(2) Lorsqu'une autre loi accorde à un organisme public, ou à un dirigeant ou à un employé d'un organisme public, un pouvoir discrétionnaire qui peut être exercé relativement à des renseignements personnels, cet organisme ou cette personne doit prendre en considération la présente loi dans l'exercice de ce pouvoir discrétionnaire, dans la mesure où l'autre loi le permet.

6(1) A public body, or an officer, employee or agent of a public body, who collects, uses or discloses personal information in wilful contravention of Principles 3, 4 or 5 of the Statutory Code of Practice commits an offence punishable under Part II of the *Provincial Offences Procedure Act* as a category F offence.

6(2) A person to whom a public body discloses personal information on terms that limit the further use or disclosure of the information, and who wilfully contravenes those terms, commits an offence punishable under Part II of the *Provincial Offences Procedure Act* as a category F offence.

7 The Lieutenant-Governor in Council may make regulations

(a) designating bodies as public bodies;

(b) making special provision respecting the interpretation and application of the Statutory Code of Practice in relation to

(i) particular public bodies,

(ii) particular kinds of personal information, or

(iii) particular activities involving the handling of personal information;

(c) respecting forms to be used under this Act;

(d) respecting procedures to be followed under this Act;

(e) respecting fees payable under this Act;

(f) respecting exemptions from this Act for personal information, or for any arrangement

6(1) Commet une infraction punissable en vertu de la Partie II de la *Loi sur la procédure relative aux infractions provinciales* à titre d'infraction de la classe F, tout organisme public, ou tout dirigeant, tout employé ou tout agent d'un organisme public qui recueille, utilise ou divulgue des renseignements personnels en contravention délibérée du Principe 3, 4 ou 5 du Code de pratique statutaire.

6(2) Commet une infraction punissable en vertu de la Partie II de la *Loi sur la procédure relative aux infractions provinciales* à titre d'infraction de la classe F, toute personne à qui un organisme public divulgue des renseignements personnels à des conditions qui limitent l'usage ou la divulgation ultérieurs des renseignements et qui délibérément contrevient à ces conditions.

7 Le lieutenant-gouverneur en conseil peut établir des règlements

a) désignant des organismes à titre d'organismes publics;

b) prenant des dispositions spéciales relativement à l'interprétation et à l'application du Code de pratique statutaire relativement

(i) à des organismes publics particuliers,

(ii) à des genres particuliers de renseignements personnels, ou

(iii) à des activités particulières comportant le traitement des renseignements personnels;

c) concernant les formules à utiliser en vertu de la présente loi;

d) concernant les procédures à suivre en vertu de la présente loi;

e) concernant les droits à payer en vertu de la présente loi;

f) concernant les exemptions à la présente loi en matière de renseignements personnels ou de

for the management of personal information, that exists on the commencement of this Act.

8(1) ***Section 1 of the Archives Act, chapter A-11.1 of the Acts of New Brunswick, 1977, is amended:***

(a) by adding after the definition "hospital corporation" the following:

"identifiable individual" means an individual who can be identified by the contents of information because the information

(a) includes the individual's name,

(b) makes the individual's identity obvious, or

(c) is likely in the circumstances to be combined with other information that includes the individual's name or makes the individual's identity obvious;

(b) by repealing the definition "personal information" and substituting the following:

"personal information" means information about an identifiable individual;

8(2) ***Subsection 10(3) of the Act is amended by adding after paragraph (b) the following:***

(b.1) would reveal personal information concerning the applicant that

(i) was provided by another person in confidence, or is confidential in nature, or

(ii) could reasonably be expected to threaten the safety or mental or physical health of the applicant or another person;

mesures relatives à la gestion des renseignements personnels, qui existent lors de l'entrée en vigueur de la présente loi.

8(1) ***L'article 1 de la Loi sur les Archives, chapitre A-11.1 des Lois du Nouveau-Brunswick de 1977, est modifié***

a) par l'adjonction après la définition «Ministre» de ce qui suit:

«particulier identifiable» désigne un particulier qui peut être identifié par le contenu de renseignements qui

a) comprennent son nom,

b) rendent son identité évidente, ou

c) sont susceptibles dans les circonstances d'être adjoints à d'autres renseignements qui comprennent son nom ou rendent son identité évidente;

b) par l'abrogation de la définition «renseignement personnel» et son remplacement par ce qui suit:

«renseignement personnel» désigne un renseignement sur un particulier identifiable;

8(2) ***Le paragraphe 10(3) de la Loi est modifié par l'adjonction après l'alinéa b) de ce qui suit:***

b.1) pourrait dévoiler des renseignements personnels sur le demandeur qui

(i) ont été fournis par une autre personne à titre confidentiel, ou qui sont de nature confidentielle, ou

(ii) pourraient raisonnablement menacer la sécurité ou la santé mentale ou physique du demandeur ou d'une autre personne;

9(1) ***Section 1 of the Right to Information Act, chapter R-10.3 of the Acts of New Brunswick, 1978, is amended***

(a) by adding after the definition "hospital corporation" the following:

"identifiable individual" means an individual who can be identified by the contents of information because the information

(a) includes the individual's name,

(b) makes the individual's identity obvious, or

(c) is likely in the circumstances to be combined with other information that includes the individual's name or makes the individual's identity obvious;

(b) by repealing the definition "personal information" and substituting the following:

"personal information" means information about an identifiable individual;

9(2) ***The Act is amended by adding after section 2 the following:***

2.1 Without limiting section 2, subject to this Act, every individual is entitled to request and receive information about himself or herself.

9(3) ***Section 6 of the Act is amended by adding after paragraph (b) the following:***

(b.1) would reveal personal information concerning the applicant that

(i) was provided by another person in confidence, or is confidential in nature, or

(ii) could reasonably be expected to threaten the safety or mental or physical health of the applicant or another person;

9(1) ***L'article 1 de la Loi sur le droit à l'information, chapitre R-10.3 des Lois du Nouveau-Brunswick de 1978, est modifié***

a) par l'adjonction après la définition «ministre compétent» de ce qui suit:

«particulier identifiable» désigne un particulier qui peut être identifié par le contenu de renseignements qui

a) comprennent son nom,

b) rendent son identité évidente, ou

c) sont susceptibles dans les circonstances d'être adjoints à d'autres renseignements qui comprennent sont nom ou rendent son identité évidente;

b) par l'abrogation de la définition «renseignement personnel» et son remplacement par ce qui suit:

«renseignement personnel» désigne un renseignement sur un particulier identifiable.

9(2) ***La Loi est modifiée par l'adjonction après l'article 2 de ce qui suit:***

2.1 Sans restreindre la portée de l'article 2 et sous réserve de la présente loi, tout particulier a le droit de demander et de recevoir toute information sur lui-même.

9(3) ***L'article 6 de la Loi est modifié par l'adjonction après l'alinéa b) de ce qui suit:***

b.1) pourrait dévoiler des renseignements personnels concernant le demandeur qui

(i) ont été fournis par une autre personne à titre confidentiel, ou qui sont de nature confidentielle, ou

(ii) pourraient raisonnablement menacer la sécurité ou la santé mentale ou physique du demandeur ou d'une autre personne;

10 ***This Act or any provision of it comes into force on a day or days to be fixed by proclamation.***

10 ***La présente loi ou l'une quelconque de ses dispositions entre en vigueur à la date ou aux dates fixées par proclamation.***

Schedule A

The Statutory Code of Practice

Principle 1: Accountability

A public body is responsible for personal information under its control. The chief executive officer of a public body, and his or her designates, are accountable for the public body's compliance with the following principles.

Principle 2: Identifying Purposes

The purposes for which personal information is collected shall be identified by the public body at or before the time the information is collected.

Principle 3: Consent

The consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the public body. Information shall be collected by fair and lawful means.

Principle 5: Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required or expressly authorized by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Principle 6: Accuracy

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

Annexe A

Code de pratique statutaire

Principe 1: Responsabilité

Un organisme public est responsable des renseignements personnels dont il a la gestion. Le directeur exécutif d'un organisme public et ses représentants doivent s'assurer du respect par l'organisme public des principes suivants.

Principe 2: Détermination des fins de la collecte

Les fins pour lesquelles les renseignements personnels sont recueillis doivent être déterminées par l'organisme public avant ou au moment de la collecte.

Principe 3: Consentement

Tout particulier doit consentir à toute collecte, utilisation ou divulgation de renseignements personnels, à moins qu'il ne soit pas approprié de le faire.

Principe 4: Limitation de la collecte

L'organisme public ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

Principe 5: Limitation de l'utilisation, de la divulgation et de la conservation

Les renseignements personnels ne doivent pas être utilisés ou divulgués à des fins autres que celles auxquelles ils ont été recueillis, à moins que le particulier n'y consente ou que la loi ne l'exige ou ne l'autorise expressément. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

Principe 6: Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils doivent être utilisés.

Principle 7: Safeguards

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

Principle 8: Openness

A public body shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9: Individual Access

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

Principle 10: Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the individual or individuals accountable for the public body's compliance.

Principe 7: Dispositifs de protection

Les renseignements personnels doivent être protégés par des dispositifs de protection correspondant à leur degré de sensibilité.

Principe 8: Transparence

Un organisme public doit mettre à la disposition des particuliers des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Principe 9: Accès individuel

Un organisme public doit informer tout particulier qui en fait la demande de l'existence de renseignements personnels qui le concernent, de l'usage qui en est fait et du fait qu'ils ont été divulgués à des tiers et lui permettre de les consulter, à moins qu'il ne soit pas approprié de le faire. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections appropriées.

Principe 10: Possibilité de porter plainte contre le non-respect des principes

Tout particulier doit être en mesure de se plaindre du non-respect des principes indiqués plus haut en communiquant avec le ou les particuliers responsables de les faire respecter au sein de l'organisme public.

Schedule B

Interpretation and Application of the Statutory Code of Practice

The provisions of the Statutory Code of Practice that are referred to in this Schedule shall be interpreted and applied in accordance with this Schedule.

Principle 2: Identifying Purposes

2.1 The purposes identified by the public body must directly relate to an existing or proposed activity of the public body.

2.2 The public body must document, in relation to any personal records system, the purpose or purposes for which the personal information in the system is held.

2.3 A "personal records system" is a computerized or manual records system which contains information about individuals and which is structured in such a way that information about specified individuals can be easily recovered.

Principle 3: Consent

3.1 Consent may be express or implied.

3.2 The actions for which consent can be implied are those that an individual should reasonably expect the public body to take, and would be unlikely to disapprove of, having regard to

(a) the nature of the personal information in question, including whether it is or is not sensitive or confidential,

(b) any benefit or detriment to the individual,

Annexe B

Interprétation et application du Code de pratique statutaire

Les dispositions du Code de pratique statutaire qui sont visées dans la présente annexe doivent être interprétées et appliquées conformément à la présente annexe.

Principe 2: Détermination des fins de la collecte

2.1 Les fins déterminées par l'organisme public doivent se rattacher directement à une de ses activités existantes ou proposées.

2.2 L'organisme public doit documenter, relativement à tout système d'enregistrement des renseignements personnels, la ou les fins pour lesquelles les renseignements personnels sont conservés dans le système.

2.3 Un «système d'enregistrement des renseignements personnels» est un système d'enregistrement informatisé ou manuel qui contient des renseignements sur des particuliers et qui est organisé de manière à donner facilement accès à des renseignements sur des particuliers spécifiques.

Principe 3: Consentement

3.1 Un consentement peut être expresse ou tacite.

3.2. Les mesures pour lesquelles un consentement peut être tacite sont celles que le particulier devrait raisonnablement s'attendre à voir prendre par l'organisme public, et qu'il n'est pas susceptible de désapprouver, eu égard à

a) la nature des renseignements personnels en question, y compris la question de savoir si les renseignements ont ou non une nature sensible ou confidentielle,

b) tout avantage ou inconvénient pour le particulier,

(c) any explanation that the public body has given of its intended actions,

(d) any indication that the individual has given of his or her actual wishes, and

(e) the ease or difficulty with which the actual wishes of the individual might be discovered.

3.3 Consent can be given by a parent, guardian or other representative of the individual in appropriate circumstances.

3.4 Consent is not required when a public body collects, uses or discloses personal information

(a) to protect the health, safety or security of the public or of an individual,

(b) for purposes of an investigation related to the enforcement of an enactment,

(c) to protect or assert its own lawful rights or those of another public body, including lawful rights against the individual,

(d) to verify the individual's eligibility for a government program or benefit for which the individual has applied,

(e) for purposes of legitimate research in the interest of science, of learning or of public policy, or for archival purposes,

(f) as required or expressly authorized by law, or

(g) for some other substantial reason in the public interest, whether or not it is similar in nature to paragraphs (a) to (f).

c) toute explication que l'organisme public a donné des mesures qu'il entend prendre,

d) toute indication que le particulier a donné de ses désirs réels, et

e) la facilité ou la difficulté avec laquelle les désirs réels du particulier peuvent être identifiés.

3.3 Un consentement peut être donné par un parent, un tuteur ou un autre représentant du particulier selon les circonstances.

3.4 Un consentement n'est pas requis lorsqu'un organisme public recueille, utilise ou divulgue des renseignements personnels

a) pour protéger la santé ou la sécurité du public ou d'un particulier,

b) aux fins d'une enquête liée à l'exécution d'une mesure législative,

c) pour protéger ou affirmer ses propres droits légaux ou ceux d'un autre organisme public, y compris des droits légaux contre le particulier,

d) pour vérifier l'admissibilité du particulier à un programme ou à une prestation gouvernementale pour lequel le particulier a fait une demande,

e) pour les fins de toute recherche légitime faite dans l'intérêt de la science, de l'enseignement ou de l'ordre public ou pour des travaux d'archives,

f) tel que requis ou expressément autorisé par la loi, ou

g) pour toute autre raison importante dans l'intérêt du public, qu'elle soit ou non semblable à celle des alinéas a) à f).

3.5 A public body may disclose personal information under paragraph 3.4(g) in furtherance of the public interest in open government.

3.6 Before collecting, using or disclosing personal information without consent under paragraph 3.4 or 3.5, a public body shall consider the nature of the information in question and the purpose for which it is acting, and shall satisfy itself that in the circumstances that purpose justifies the action proposed.

3.7 Any collection, use or disclosure of personal information without consent shall be limited to the reasonable requirements of the situation.

Principle 4: Limiting Collection

4.1 A public body may collect personal information

(a) from the individual,

(b) from another person with the individual's consent,

(c) from a source and by means available to the public at large,

(d) from any source if the public body is acting under paragraphs 3.4 to 3.7.

4.2 An individual shall not be refused a service or benefit because he or she declines to provide personal information which is not necessary for a legitimate purpose of the public body.

Principle 5: Limiting Use, Disclosure and Retention

5.1 A public body may discharge its obligation not to retain personal information by converting that information into non-identifying form.

3.5 Un organisme public peut divulguer des renseignements personnels en vertu de l'alinéa 3.4g) dans l'intérêt du public de rendre le gouvernement plus transparent.

3.6 Avant de recueillir, d'utiliser ou de divulguer des renseignements personnels sans consentement en vertu du paragraphe 3.4 ou 3.5, un organisme public doit prendre en considération la nature des renseignements en question et la fin des mesures qu'il prend, et doit se convaincre que dans les circonstances cette fin justifie les mesures projetées.

3.7 Toute collecte, toute utilisation ou toute divulgation de renseignements personnels sans consentement doit se limiter aux exigences raisonnables de la situation.

Principe 4: Limitation de la collecte

4.1 Un organisme public peut recueillir des renseignements personnels auprès

a) du particulier,

b) d'une autre personne avec le consentement du particulier,

c) d'une source et par des moyens qui sont à la disposition du grand public,

d) de toute source si l'organisme public agit en vertu des alinéas 3.4 à 3.7.

4.2 Il est interdit de refuser tout service ou toute prestation à un particulier qui refuse de fournir des renseignements personnels qui ne sont pas nécessaires pour une fin légitime de l'organisme public.

Principe 5: Limitation de l'utilisation, de la divulgation et de la conservation

5.1 Un organisme public peut satisfaire à l'obligation de ne pas conserver des renseignements personnels en convertissant ces renseignements sous une forme non identifiable.

5.2 Personal information that is maintained outside a personal records system and is not readily accessible to a person who has no prior knowledge of the information shall be deemed to be converted into non-identifying form when the use of the information ceases.

Principle 7: Safeguards

7.1 The safeguards to be adopted include training and administrative, technical, physical and other measures, as appropriate in the circumstances, and include safeguards that are to be adopted when a public body discloses personal information to a third party or makes arrangements for a third party to collect personal information on its behalf.

Principle 9: Individual Access

9.1 A public body to which the *Right to Information Act* applies may only refuse to provide an individual with personal information relating to himself or herself if the individual would have no right to that information under the *Right to Information Act.*

9.2 A public body to which the *Right to Information Act* does not apply shall establish a procedure comparable to the procedure in that Act for the purpose of ensuring that the individual can obtain access to information about himself or herself.

9.3 The procedure established under paragraph 9.2 may include exceptions to access comparable to those in the *Right to Information Act.*

9.4 When an individual has made a challenge to the accuracy or completeness of personal information relating to himself or herself but has not satisfied the public body that an amendment is appropriate, the public body shall note that the individual disputes the information in its possession.

5.2 Les renseignements personnels qui sont conservés en dehors d'un système d'enregistrement des renseignements personnels et qui ne sont pas facilement accessibles à une personne qui n'a pas de connaissance préalable de ces renseignements sont réputés être convertis sous une forme non identifiable lorsque l'usage des renseignements cesse.

Principe 7: Dispositifs de protection

7.1 Les dispositifs de protection qui doivent être adoptés comprennent des mesures de formation et des mesures administratives, techniques, physiques et autres, comme il convient dans les circonstances, et comprennent les dispositifs de protection qui doivent être adoptés quand un organisme public divulgue des renseignements personnels à un tiers ou prend des mesures pour qu'un tiers recueille des renseignements personnels en son nom.

Principe 9: Accès individuel

9.1 Un organisme public auquel la *Loi sur le droit à l'information* s'applique ne peut refuser de fournir à un particulier des renseignements personnels qui le concernent que si le particulier n'a aucun droit de les avoir en vertu de la *Loi sur le droit à l'information.*

9.2 Un organisme public auquel la *Loi sur le droit à l'information* ne s'applique pas doit établir une procédure comparable à celle de cette loi pour s'assurer que les particuliers peuvent avoir accès aux renseignements qui les concernent.

9.3 La procédure établie au paragraphe 9.2 peut comprendre des exceptions à l'accès aux renseignements personnels comparables à celles de la *Loi sur le droit à l'information.*

9.4 Lorsqu'un particulier a contesté l'exactitude ou l'état complet de renseignements personnels qui le concernent mais qu'il n'a pas convaincu l'organisme public qu'une modification s'imposait, l'organisme public doit noter que le particulier conteste les renseignements en sa possession.

Principle 10: Challenging Compliance

10.1 A public body shall investigate in good faith the complaints it receives about its management of personal information and shall take appropriate measures if a complaint is found to be justified.

Principe 10: Possibilité de porter plainte contre le non-respect des principes

10.1 Un organisme public doit faire une enquête de bonne foi sur les plaintes qu'il reçoit sur sa gestion des renseignements personnels et doit prendre les mesures appropriées s'il s'avère qu'une plainte est justifiée.

APPENDIX C

UNIFORM PRIVACY ACT

Definition

1. In this Act, "court" means [The Court of Queen's Bench of New Brunswick].

Tort

2. Violation of the privacy of an individual by a person is a tort that is actionable without proof of damage.

Proof in absence of contrary evidence

3. Without limiting the generality of section 2, proof of any of the following, in the absence of evidence to the contrary, is proof of a violation of the privacy of an individual:

(a) auditory or visual surveillance of the individual or the individual's residence or vehicle by any means, including eavesdropping, watching, spying, besetting and following, whether the surveillance is accomplished by trespass or not;

(b) listening to or recording a conversation in which the individual participates, or listening to or recording a message to or from the individual that passes by means of telecommunications, by a person who is not a lawful party to the conversation or message;

(c) publication of letters, diaries or other personal documents of the individual;

(d) dissemination of information concerning the individual that has been gathered for commercial or governmental purposes if

(i) the dissemination is contrary to a statute or regulation, or

(ii) the information was provided by the individual in confidence, and the dissemination is made for a purpose other than the purpose for which the information was provided.

Defences

4.(1) An Act, conduct or publication does not constitute a violation of the privacy of an individual if

(a) it is specifically consented to, expressly or impliedly, by the individual, the

individual is entitled to consent to it, and the court is satisfied that the consent is freely given;

(b) it is reasonably incidental to the exercise of a lawful right of defence of person or property;

(c) subject to subsection (2), it is authorized or required

(i) under a statute or regulation,

(ii) by a court or by a person, tribunal or agency, other than a commissioner for oaths or a notary public, that is authorized by law to administer an oath for the purposes for which the person, tribunal or agency is authorized to take evidence, or

(iii) by any process of a court, person, tribunal or agency mentioned in subclause (ii);

(d) it is an act, conduct or publication of a peace officer or a public officer engaged in an investigation who is acting in the course and within the scope of his or her duty, it is not disproportionate to the gravity of the matter that is the subject of the investigation and it is not committed in the course of trespass or other unlawful act;

(e) it is reasonable, having regard to any relationship, domestic or otherwise, between the parties to the action; or

(f) the defendant neither knew nor reasonably should have known that the act, conduct or publication would violate the privacy of any individual.

(2) No authorization or requirement under a statute or regulation provides a defence to an action for violation of privacy unless the statute or regulation specifically authorizes or requires the act, conduct or publication for the purpose for which it is undertaken.

(3) A publication of a matter is not a violation of the privacy of an individual if

(a) there are reasonable grounds for belief that the publication is in the public interest; or

(b) the publication is privileged under the law relating to defamation.

(4) Subsection (3) does not apply to any act or conduct by which the matter published is obtained if that act or conduct constitutes a violation of privacy.

Remedies

5. In an action for violation of privacy, the court may do one or more of the following:

(a) award damages;

(b) grant an injunction;

(c) order the defendant to account to the plaintiff for any profits that have accrued or may accrue to the defendant as a result of the violation of privacy;

(d) order the defendant to deliver up to the plaintiff all articles or documents that have come into the defendant's possession as a result of the violation of privacy;

(e) grant any other relief to the plaintiff that the court considers necessary in the circumstances.

Damages

6.(1) In awarding damages in an action for violation of privacy, the court shall consider all the circumstances of the case, including

(a) the nature of the act, conduct or publication and the context in which it occurs;

(b) the effect of the act, conduct or publication on the health and welfare or on the social, business or financial position of the plaintiff or relatives of the plaintiff; and

(c) the conduct of the plaintiff and of the defendant before and after the act, conduct or publication, including any apology or offer of amends made by the defendant.

(2) In an action for violation of privacy, the court may award punitive damages, taking into account the flagrancy of the violation of privacy and the conduct of the defendant.

Right of action in addition to other rights

7.(1) The right of action for violation of privacy conferred by this Act and the remedies available under this Act are in addition to, and not in derogation of, any other right or remedy available under any other law.

(2) Subsection (1) does not require damages awarded in an action for violation of privacy to be disregarded in assessing damages in any other proceedings arising out of the same act, conduct or publication that constitutes the violation of privacy.

Crown bound

8. The Crown is bound by this Act.

APPENDIX D

ALTERNATIVE APPROACH (SUMMARY)

1 An invasion of the privacy of an individual is a tort that is actionable without proof of damage.

2 An act is an invasion of privacy

(a) if it unduly intrudes into the personal affairs of an individual, or into his or her activities, whether in a public or a private place, or

(b) if it gives undue publicity to personal information concerning an individual.

3 Without limiting sections 1 and 2, an invasion of privacy may arise from

(a) surveillance of the individual,

(b) eavesdropping or intercepting an individual's communications, or

(c) publication of the personal documents of an individual.

4 The defences to an action for invasion of privacy are

(a) that the individual consented to the action complained of,

(b) that the action complained of was done in the exercise of a lawful right of defence of person or property,

(c) that the action complained of was authorized or required by law,

(d) that the action complained of was done by a peace officer when acting in good faith and in the course of his or her duty,

(e) that the action complained of was reasonable in all of the circumstances, and having regard to any relationship, domestic or otherwise, between the parties to the action,

(f) that the defendant neither knew nor reasonably should have known that the act, conduct or publication would violate the privacy of any individual, and

(g) that the action complained of was a publication that

(a) the defendant reasonably believed to be in the public interest; or

(b) was privileged under the law of defamation.

[No provisions on remedies are included.]