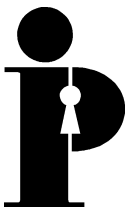
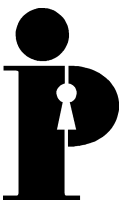
Information
and Privacy
Commissioner/
Ontario

Submission to the Ministry of Consumer and Commercial Relations in Response to *A Consultation Paper: Proposed Ontario Privacy Act*



Ann Cavoukian, Ph.D.
Commissioner
September 2000



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Cette publication est également disponible en français.

This publication is also available on the IPC website.

Introduction

The Office of Information and Privacy Commissioner of Ontario (IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act* to review and comment on the privacy protection implications of proposed legislative schemes. The proposed private sector privacy legislation will have a significant impact on the privacy of every individual in the province of Ontario.

Recent developments have served to highlight the need to have a comprehensive framework for privacy protection for the private sector in Ontario. These developments include:

- the development and implementation of new information and telecommunications technology;
- the evolution of the digitized global economy;
- federal and provincial government strategies that rely on partnerships with private sector organizations and the contracting out of government functions to private enterprises;
- enhanced public awareness of privacy issues and support for privacy legislation;
- the passage of the Directive of the European Union which restricts the transborder data flow of personal information to non-member countries lacking adequate protection; and
- the recent passage of the federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (formerly Bill C-6).

In light of these developments, it is our view that the establishment of a comprehensive legal framework for protection of personal information by private sector organizations is critical to ensure the protection of personal information that is collected, used and disclosed within the province.

We are pleased that the protection of personal privacy is a top priority for the government and that the government has moved forward with the consultation process through the release of the document, *A Consultation Paper: Proposed Ontario Privacy Act*. We offer the following comments and suggestions to enhance the framework that is being proposed in this document.

Our comments are organized under the major headings set out in the consultation paper of the Ministry of Consumer and Commercial Relations (MCCR).

Goals in Developing Ontario's Own Legislation (MCCR page 3)

For some time, the IPC has been promoting the implementation of private sector privacy legislation. We commend the Government of Ontario for recognizing the immediate need for this legislation and for leading the provinces and territories with this important initiative. As noted in the consultation paper, the implementation of this legislation now will ensure that rules for the collection, use and disclosure of personal information within Ontario are consistent with public expectations and this should help to position the province as a trusted marketplace in the new digital economy. In general, we support the four goals in developing made-in-Ontario legislation, as set out in the consultation paper.

Goal 1. Comprehensive and Seamless Privacy Protection

With respect to the first goal, we agree that the legislation should apply to all individuals, organizations and activities within the province, except government organizations already covered by public sector privacy legislation and organizations that are federally regulated. In line with the goal of providing comprehensive and seamless privacy protection, we believe the legislation should, at a minimum, meet the privacy standards set out in the federal *Personal Information Protection and Electronic Documents Act*.

In our view, one of the main limitations of the federal *Personal Information Protection and Electronic Documents Act* is that it only applies to personal information collected, used and disclosed during the course of commercial activity. Personal information that is collected, used and disclosed for non-commercial purposes and, in most cases, for employment-related purposes is not protected under the federal legislation.

Personal information is collected, used and disclosed on a daily basis by organizations which may or may not engage in commercial activities. In addition to organizations clearly engaged in commercial activities, the legislation should apply to a broad range of entities such as universities, hospitals, Crown corporations not covered by public sector privacy legislation, community groups with public objects or functions, non-governmental organizations (NGOs), professional governance bodies, trade and professional associations, trade unions, learned societies, research organizations, employer associations, charitable organizations, churches and religious institutions, health care providers and professionals such as lawyers and accountants, arts and performance organizations, and non-profit corporations.

In general, the privacy protections afforded by the proposed legislation should cover all personal information that is collected, used or disclosed in the course of an organization's operations and activities. In addition, the legislation should apply to any personal information that an organization collects, uses or discloses about its employees or potential employees for human resources purposes. It should also be sufficiently robust and anticipatory to accommodate new and emerging privacy

issues such as the collection, use and disclosure of biometric and genetic information. The use of unique identifiers should be prohibited under the legislation, except where specifically provided for by law. Finally, to provide consistency with other legislation (i.e., the federal *Privacy Act*), and to avoid confusion, the legislation should stipulate that information about the employment and business responsibilities, activities and transactions of an individual is not subject to the privacy protection provisions of the legislation.

Goal 2. Flexibility for Unique Privacy Needs and Circumstances

We agree that the privacy rules set out in the legislation should be sufficiently flexible to accommodate privacy needs in a range of contexts. Fair information practices, such as those set out in the *Canadian Standards Association Model Code for the Protection of Personal Information* (CSA Code) and embodied in the federal *Personal Information Protection and Electronic Documents Act*, are internationally accepted rules for the collection, use and disclosure of personal information. They have been successfully applied to personal information in a broad range of contexts. In general, it is our view that the basic privacy rules do not need to change from one situation to the next. Unique privacy needs that arise in various contexts can be accommodated through narrow and carefully worded exceptions to the privacy rules that may apply under specific circumstances.

We are pleased that the proposed legislation will include legislated rules setting out privacy requirements for health information. Our comments regarding the privacy requirements for this very sensitive type of personal information will be made in a separate submission in response to the consultation paper being prepared by the Ministry of Health and Long-Term Care.

We are not opposed to the inclusion of provisions for sectoral codes in the legislation as one mechanism for enhancing flexibility. However, it is our position that sectoral codes should be used to enhance or expand upon data protection standards as set out in the legislation, rather than to diminish those standards. Our comments regarding sectoral codes are outlined more fully in response to Question 10.

Goal 3. Efficient, Fair and Effective Enforcement

We understand the government's rationale for proposing that enforcement of the privacy rules should reflect the substance of the CSA Code without imposing an undue regulatory burden. However, we think that it should also be emphasized that enforcement of the privacy rules should not place an undue burden on individuals who are trying to exercise their rights under the proposed legislation. Under the legislation, individuals should be provided with a readily accessible mechanism for independent and impartial review of the actions of organizations with respect to their personal information, and for redress in the event of a violation of privacy rights. Our comments regarding enforcement of the proposed legislation are outlined more fully in response to Questions 12 and 13.

Goal 4. Compatibility with Other Laws

We agree that the proposed legislation should be harmonized with other private sector legislation in Canada. As noted previously, consistent with the goal of providing comprehensive and seamless privacy protection, the legislation should, at a minimum, meet the privacy standard set out in the federal *Personal Information Protection and Electronic Documents Act*. All personal information that is collected, used or disclosed within Ontario should be subject to the same protections regardless of the type of personal information and the organization to which the information has been entrusted.

In response to the statement made in the consultation paper that the proposed legislation would not override the privacy-related provisions of other statutes, we would suggest that this statement may be too general and should be clarified. It is our view that in order to recognize the fundamental nature of the right to privacy, the proposed legislation should prevail over other legislation in the same way that other human rights legislation has primacy. If there is no primacy, the protections in the proposed legislation can be diluted by other legislation where special consideration is not given to privacy protection.

For example, the Quebec private sector statute, *An act respecting the protection of personal information in the private sector*, provides that it has primacy over all other Quebec statutes, unless the other statute specifically provides otherwise. A specific statute must expressly state that one of its provisions shall apply notwithstanding the province's private sector privacy legislation. Similarly, Ontario's public sector privacy (and access) legislation contains a provision which states that the legislation prevails over confidentiality provisions in other legislation, unless either piece of legislation specifically states otherwise.

The proposed legislation will provide for a minimum standard of privacy. If other legislation or sectoral codes provide for a greater measure of privacy, we are of the opinion that the legislation or code providing the greatest standard of protection should prevail, unless expressly stated otherwise. For example, if a code of professional conduct provides for a greater measure of privacy protection for personal information than the proposed legislation, then the professional code should prevail.

Ontario's Proposed Approach Reflects the CSA Standard

(MCCR page 4)

We agree that the proposed legislation should be based on the CSA Code. We also support incorporating the CSA Code into the body of the legislation, rather than appending it as a schedule. In our view, this is an improvement over the approach taken in the federal *Personal Information Protection and Electronic Documents Act*. We believe that this approach will enhance clarity and make the legislation easier to enforce.

However, we do not agree that the legislation should focus "on outcomes, and what is clearly required, rather than processes." The implication of this statement is that key provisions of the CSA Code which are deemed to be process-related would not be included in the legislation.

It is our view that, with respect to privacy protection, it may not be meaningful or useful to make a distinction between outcomes and processes, since in many cases privacy outcomes cannot be achieved unless certain processes are in place. For example, we do not believe the first CSA principle of accountability can be achieved without one or more individuals being designated as accountable for the organization's compliance with the privacy rules.

For legislation to be effective, it should include a combination of results or outcome-focused standards and procedural standards. Where specific processes have been widely established as standard mechanisms for achieving specific privacy objectives, these should be required under the legislation. The inclusion of procedural requirements will help organizations to implement the legislation in an efficient and effective manner. In addition, where processes may help individuals to exercise their rights under the proposed legislation, provisions of the CSA Code relating to these processes should be not be sacrificed in favour of minimizing the administrative burden on organizations that are entrusted with personal information. Our views on the potential exclusion of some of the principles of the CSA Code are expressed more fully in response to Question 9.

What Would Be Your Rights Under the Proposed Ontario Privacy Act? (MCCR page 5)

We agree that the legislation should ensure the individual's rights: to control whether and how personal information is collected, used and disclosed; to access and, if necessary, correct personal information; and to complain about possible violations of the legislation. With respect to the individual's right to control whether personal information is collected, we would also add that, where it is lawful and practicable, it would be desirable if individuals were given the option of not identifying themselves when entering into transactions with an organization. For example, one of the National Privacy Principles, which provide the foundation for Australia's proposed private sector privacy legislation, states that individuals have the right to enter transactions anonymously. The government may wish to consider including a similar provision in Ontario's new legislation.

Also, in addition to the rights set out in the consultation paper, it is our view that individuals should have the right to be informed about an organization's policies and procedures for managing their personal information. With respect to this right, when personal information is collected, individuals should be informed about the following:

- the purposes for collecting personal information;
- anticipated uses and disclosures of personal information;
- that individuals may specify a time after which their consent is no longer valid;
- that individuals may, at any time, revoke their consent in writing;
- the procedures for requesting access to and/or correction of personal information;
- that a copy of the organization's policy and procedures regarding the collection, use and disclosure of personal information will be provided upon request;
- the administrative, technical and physical safeguards relating to the confidentiality and security of the information; and
- who to contact to ask questions about the collection, to request access or correction of personal information, and to complain about the collection, use and disclosure of personal information.

We generally support the specific individual rights set out in the consultation paper. Individuals should be asked to give their consent before personal information is collected, used or disclosed. Consent should usually be "express." "Implied" consent should only be permitted in the limited circumstances set out in the legislation. Individuals should be able to revoke a consent, except in certain circumstances, and individuals should not be denied a good, service or other transaction because they did not consent to the use of their personal information for purposes that are not directly related to the transaction. Individuals should also be entitled to review their personal

information and to be informed about how that information is used or disclosed to other organizations. The limited exceptions to the general right of access should be set out in the legislation. Finally, individuals should be able to correct inaccurate personal information or have the information flagged as being disputed.

We do not entirely agree with the suggestion that privacy legislation is not appropriate or practical for resolving disputes about the accuracy of personal information. Under the proposed legislation, organizations should be required to take reasonable steps to ensure the accuracy of personal information before it is used or disclosed. In addition, the independent oversight body should have the authority to resolve disputes about the accuracy of certain types of personal information. The accuracy of personal information is discussed in greater detail in our responses to Questions 6 and 9.

Who Can Provide Consent?

Question 1: Should the proposed Privacy Act include rules governing when minors can give consent?

It may be useful if the proposed legislation were to include an age at which minors are able to provide consent. As stated in the consultation paper, this will provide certainty and enable youth to effectively engage in employment and commerce.

The selection of 13 as the age of consent is consistent with the work of the Canadian Marketing Association (CMA). The CMA's Code of Ethics uses the term "child" to refer to someone who has not reached his or her 13th birthday and sets out special considerations for marketing to children. While the new federal privacy law does not deal with this issue specifically, in his 1999/2000 Annual Report, the federal Privacy Commissioner expressed support for the CMA's guidelines on marketing to children. The age of 13 is also consistent with recently passed U.S. legislation, the *Children's Online Privacy Protection Act of 1998*.

The IPC does not object to the proposal that minors, age 13 and over, be allowed to consent to the collection, use and disclosure of their personal information for the purposes of commerce and employment. In Ontario, while the age of majority, set by the *Age of Majority and Accountability Act* is 18 years, that act recognizes that specific legislation may determine the age at which an individual may be treated as an adult for the purposes of that particular legislation.

Regulations under the *Occupational Health and Safety Act* set the minimum ages at which young people in Ontario can begin employment. Under the regulation regarding Industrial Establishments, the minimum age of a worker is 14 years of age in a workplace other than a factory. As stated in the consultation paper, if youths, at age 13, could not consent to giving personal information to their prospective employers, it would affect their ability to complete a job application. However, we recognize that although a person may obtain employment, buy goods and do other things, at an age younger than 13, it is our view that parental consent to providing personal information is appropriate in this context.

Our support for the selection of 13 as the age of consent is contingent upon certain safeguards being put in place. For example, as suggested, such consent should be limited to the particular interaction and parental consent should be required for any unrelated use of the information, including subsequent disclosures.

There appears to be a rationale for using the age of 13 as a general default age at which minors are able to provide consent, particularly in the spheres of employment and commerce. However, in other areas, such as when especially sensitive information is involved or when children are speaking to distress line personnel, different ages for consent may be appropriate. The legislation may need to incorporate a mechanism for defining other ages of consent for specific contexts. If a particular age or ages are to be specified for consent, then this should be done through an open and transparent process, such as directly in the legislation, in regulations or in sectoral codes.

A corollary to the above, and of increasing importance in a world where more and more transactions are conducted online, is the issue of verification of the age of individuals with whom organizations are dealing. This has been an issue in the offline world for years, for example, where there has been an age restriction on buying certain products, however, the problem is exacerbated in the online world. Where parties do not see one another or even have access to other clues as to age, such as a person's handwriting, there must be other ways to verify the age of an individual. The onus to adhere to consent requirements should be placed on the organizations that are collecting the information. In particular, operators of Web sites or online services directed to minors and operators of Web sites or online services who have actual knowledge that they are dealing with such individuals should be aware that it will be their responsibility to ensure that they are not obtaining personal information from those unable to provide a valid consent.

Concomitantly, where parental consent is required, such parental consent must also be subject to verification requirements. The onus must be on the organization to verify that the actual parent is giving consent, where that is required. Other parental rights are discussed in response to Question 6.

Indirect Collection

Question 2: Should the proposed legislation include rules for the indirect collection of personal information without consent?

Direct collection of personal information provides individuals with the ability to control the collection and use of their own information. This is a basic component of privacy protection. If information is collected directly from the individual, the individual is provided with knowledge of the collection as well as the opportunity to consent to it and the purpose for which it may be used. It has been recognized that an individual's privacy "might be threatened less by the actual information provided than by the methods of collection and verifying information."[1]

[1] *Public Government for Private People: The Report of the Commission on Freedom of Information and Individual Privacy 1980, Vol.3* (Toronto: Queen's Printer, 1980) (Chair: D.C. Williams), p. 687.

We agree that people are concerned about excessive use of indirect collection without consent. Indiscriminate indirect collection increases the likelihood of an unjustified invasion of privacy, the loss of control by the individual over his or her personal information, and intrusive action on the part of an organization. Derogations from the fundamental principle of direct (and limited) collection of personal information should be limited and specific. Accordingly, we support the suggestion that the legislation should explicitly state that, with clear, limited and specific exceptions, personal information should be collected directly from the individual to whom the information relates, after first obtaining consent. Further, we concur with the consultation paper that indirect collection should not be allowed where the individual might reasonably disapprove or view this collection or use as undesirable.

Placing the specific exceptions to the direct collection principle in the proposed legislation, as has been done in other legislation, will provide greater certainty. This will be of value to organizations in establishing policies to comply with the legislation and to individuals who are exercising their rights under the legislation. For example, under section 39 of the *Freedom of Information and Protection of Privacy Act*, some of the exceptions to the direct collection principle are as follows:

- the individual authorizes another manner of collection;
- the oversight body has authorized another manner of collection;
- the information is in a report from a reporting agency in accordance with the *Consumer Reporting Act*;
- the information is collected for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service;
- the information is collected for the purpose of the conduct of a proceeding or possible proceeding before a court or tribunal;
- the information is collected for the purposes of law enforcement (defined elsewhere in the statute); and
- another manner of collection is authorized by or under a statute.

Other exceptions to the direct collection principle should also be considered, such as the following:

- for compassionate reasons;
- for a purpose related to an investigation of a breach of an agreement; and
- for public inquiries or commissions.

Since it is not possible to anticipate every circumstance in which indirect collection of personal information may be appropriate, the proposed legislation should give the oversight body the power to approve applications for indirect collection, in appropriate circumstances. This power is currently provided in the context of the public sector privacy legislation, referred to above.

We note that, in certain situations, organizations may inadvertently indirectly collect personal information. One example would be where a child using the Internet voluntarily provides unsolicited information about another person, such as a family member. In such cases, there should be an obligation on the organization, which incidentally indirectly collected personal information, not to use or disclose such information and to destroy it as soon as possible.

In some circumstances where personal information is collected other than directly from the individual to whom the information relates, it may be appropriate to require the organization to inform the individual about the collection, the reasons for the collection, the purpose for which the information will be used, and who to contact to ask questions about the collection. In addition, subject to some exceptions, organizations should be obliged to disclose the source of any indirectly collected information.

Your Organization Uses Personal Information – What Would be Your Organization's Obligations under the Proposed Act? (MCCR page 8)

We generally support what are envisioned as the organization's obligations under the proposed legislation. When seemingly anonymous information is transformed into personally identifiable information, this should be considered to be a collection of personal information and subject to all of the safeguards provided by the proposed legislation. The legislation should apply to a broad range of organizations, not just those involved in commercial activities. However, personal, family and household uses of personal information should not be affected by the proposed legislation.

In addition, as noted in the consultation paper, organizations should be required to: inform an individual what information it wants to collect and why; obtain consent for the collection, use and disclosure of personal information; collect, use and disclose personal information according to the rules set out in the legislation; provide access and correction of errors; and keep personal information safe and dispose of it appropriately. However, these five duties do not cover the full range of obligations for organizations which collect, use and disclose personal information as set out under the CSA Code. It is our view that these duties need to be expanded to fully reflect the CSA Code. Our position on this issue is set out in greater detail in response to Question 9.

We agree with the proposal to limit the collection, use or disclosure of personal information to purposes a person would consider appropriate in the circumstance. In our view, there should be an explicit limitation on the extent of collection – the purpose for collection should be legitimate and justifiable and the collection of personal information should be limited to that which is reasonably necessary for the purpose. Additional information should not be collected. The collection limitation principle means that it is very important that the purpose for collection be carefully identified.

We also support the proposed approach to limit the organization's use of personal information. Under the legislation, the organization should only be permitted to use personal information for the purposes to which the individual has consented. The organization should be required to obtain consent for any additional collection, use or disclosure of personal information beyond that to which the individual has consented. When an organization uses outside assistance to do things involving personal information, both parties should be accountable for what happens to the information. Organizations should be required to keep records about disclosures of personal information, which should be made available to individuals upon request.

We also support what are proposed as the organization's obligations with respect to the retention and disposal of personal information. Personal information should be retained only as long as necessary to fulfill the purposes covered by consent and to comply with any record retention required by law. Organizations should dispose of personal information either by destroying the records or by anonymizing them.

In addition to the obligations set out in the consultation paper, it is our view that organizations should be required to establish or adopt a written policy for the retention and destruction of records. This policy should address the disposal issues raised in the consultation paper, such as where personal information cannot be deleted without harming the validity of the rest of the document.

How Can Your Organization Obtain Consent?

Question 3: Should "opt-out" consent be clearly permitted as an element of a contract, agreement or notice?

In general, positive, informed consent or "opt-in" should be required under the legislation. Opt-in, which requires individuals to clearly choose to allow specific collections, uses or disclosures of their personal information, are superior from the standpoint of privacy protection. As indicated in the consultation paper, explicit opt-in consent can be obtained in a number of ways – orally, in writing or electronically. We concur with your statement that, in general, consent should be obtained directly from the individual.

We recognize, however, that opt-out consent may be sufficient for low-risk purposes, when the personal information is not considered to be sensitive and when the potential effects of providing consent are likely to be minimal. Where opt-out consent is permitted, at a minimum, the legislation should limit its use as proposed in the consultation paper.

Specifically, in the limited situations where opt-out options are to be allowed, there should be an obligation on the organization to clearly and prominently disclose the opt-out option, in an understandable manner. We agree that it would not be acceptable for an organization to simply have a policy of permitting opting-out if asked. As stated, the organization would have to make very clear what the individual is consenting to and it would be obliged to provide a straightforward and cost free means of opting-out.

We strongly approve of your statement that organizations not be permitted to refuse to deal with individuals simply because they will not consent to secondary uses of personal information that are not necessary to the transaction or activity. The legislation should include safeguards to prevent any such restriction of services. We applaud this effort.

In this context, we wish to note our view that the collection of sensitive personal information should require express, positive and informed consent. Ideally, when sensitive personal information is collected, used or disclosed, our preference is that consent be:

- voluntary and informed, including being made aware of any consequences of refusing consent;
- obtained prior to, or at the time of collection;
- revocable;
- obtained directly from the verified individual or a lawfully authorized agent;
- recorded; and
- time limited.

When Would My Organization Be Able to Make Use of "Implied Consent"?

Question 4: Should the legislation set out limited circumstances where implied consent would be appropriate, i.e., transactions that only involve internal and limited use of personal information?

It is important to understand that implied consent is generally less desirable from a privacy perspective than express consent. However, as noted in the consultation paper, we recognize that, in certain instances, implied consent may be all that is necessary or practically feasible. Organizations should understand that the quality of consent impacts on an individual's ability to control his or her own personal information. The importance of the ability to control the collection, use and disclosure of one's personal information increases with its sensitivity.

As stated in the consultation paper, the proposed legislation should set out limited circumstances where implied consent would be appropriate, such as transactions that only involve limited use of personal information (e.g., for quality control records of transactions) and where it would be unnecessary for the organization to expressly identify its purposes. Setting out these exceptional circumstances in the legislation would help clarify the issue and thereby prevent disputes as to when it is reasonable to imply consent.

In any case, we agree that implied consent should not apply when an organization uses personal information for purposes not directly related to the original activity, such as marketing other products or services. This prohibition should apply equally in non-commercial situations. As stated, implied consent should also be insufficient when personal information is disclosed to or collected from a third party. We also concur with the proposal that, upon request, an organization should be obliged to fully and promptly explain how an individual's personal information was used or disclosed.

What Safeguards Does My Organization Have to Take to Protect the Security of Personal Information?

We agree that the legislation should require organizations to establish and apply security measures appropriate to the sensitivity of the personal information they hold. In addition, security measures should be appropriate for the level of risk of unauthorized or inappropriate access to the personal information. Security measures would have to be sufficient to prevent inappropriate or unauthorized access, and accidental or improper modification, use or disclosure of personal information. Security measures should be designed to protect personal information throughout its life cycle, from the time when it is first collected until its final disposal.

Question 5: Should organizations be obliged to explain their safeguards?

We agree that the proposed legislation should clearly require that organizations explain their security safeguards. However, it should be noted that security safeguards are only one component of an effective privacy policy. Therefore, contrary to what was proposed in the consultation paper, we believe the legislation should adopt the CSA Code's Openness Principle. The Openness Principle states that an organization shall make information about its policies and practices readily available to individuals. It is not clear how an organization's practices could possibly be "apparent and understandable" to individuals in the absence of any requirement for the organization to make information about its policies and practices relating to the management of personal information readily available.

Since all organizations will have to establish or adopt policies and procedures to facilitate implementation of the legislation, we can see no reason why an obligation should not be placed on organizations to inform individuals about these policies and procedures. It is our view that, in addition to explaining their security safeguards, organizations should be required to make available information regarding policies and procedures for: the collection, use and disclosure of personal information; access and correction of personal information; retention and destruction of records; and resolving privacy complaints and disputes. Organizations should also be required to take reasonable steps to ensure that their stated policies and practices are factual, accurate and complete. This type of openness is a prerequisite for individuals to exercise their other rights under the legislation. The availability of policies and procedures is also invaluable in resolving privacy complaints.

What Happens When An Individual Requests Access to Personal Information?

Question 6: Are the proposed rights of access and treatment of accuracy issues appropriate?

We agree that, under the proposed legislation, individuals should be entitled to review their personal information, including information collected before the proposed legislation comes into force. We also endorse the statement that individuals should be entitled to be informed about how their information is used or disclosed to other organizations. As well, we favour limiting the time allowed for organizations to respond to requests for personal information. We would add that should such a time limit not be adhered to, this should constitute a deemed refusal by the organization and the organization should not be permitted to charge a fee, regardless of whether access is eventually provided. Also, as we suggested in our response to Question 2, organizations should have an obligation to explain to individuals how they obtained their information, if it was not directly collected from the individual.

The proposed focus on access, correction of false information, and flagging disputes is appropriate. The proposed rights of access and correction, as described in the consultation paper, appear to mirror those rights as they exist in Ontario's public sector privacy (and access) legislation. We have found that this system works well. To the extent that the private sector system can duplicate the public sector system in regard to these issues, public understanding and ease of use of the legislation will be enhanced.

In addition to providing a general right of access, the legislation should contain provisions to help minimize any potential barriers to access. Specifically, we recommend that organizations should have an obligation under the legislation to assist individuals in clarifying their requests for access to their own personal information. Whenever possible, organizations should be required to make the information available to the individual in the format requested (e.g., electronic or paper).

With respect to accuracy, it is our view that the proposal outlined in the consultation paper does not go far enough in terms of ensuring the accuracy of personal information. Although we agree that the accuracy of information should not be a statutory requirement in the sense that all disputes would have to be resolved, organizations should be required to take reasonable steps to ensure the accuracy of personal information before it is used or disclosed. A reasonable way to fulfill this requirement would be for an organization to inform an individual that he or she may be denied a good or service, based upon the individual's personal information, and that he or she can review the information to ensure its accuracy. Where the individual and organization do not agree about the accuracy of personal information that is factual in nature, the oversight body should have the authority to resolve this dispute. However, generally where the personal information reflects a judgment or opinion, if no agreement can be reached, disputed information should be flagged and a statement of disagreement attached. Accuracy is discussed further in response to Question 9.

As a corollary to the above, there should be a statutory requirement that any correction or statement of disagreement be stored in such a way that it is normally retrieved with the original information (e.g., a flag indicator on a computer file or a notice attached to a paper file).

We believe that the "reasonable limits" on the obligation to provide access (the example given in the consultation paper being where it is impractical to locate the information) should be defined in the legislation.

As well, parental rights of access and correction of children's information should be set out in the new legislation. Establishing one's identity and thereby one's entitlement to such rights should be subject to a statutorily required verification process.

Another issue that needs to be considered is a relative's right of access to the personal information of a deceased loved one. Although Ontario's public sector privacy legislation does not provide any special right of access to the personal information of a deceased person, Quebec's private sector legislation grants a broad range of access to information relating to the cause of death contained in the deceased's medical file. Public sector privacy legislation from Alberta and Manitoba also contain provisions which recognize the importance of disclosing personal information in compassionate circumstances. Accordingly, we would suggest that the new legislation in Ontario contain provisions to ensure that family members have a right of access to this information, in appropriate circumstances.

We recognize that an organization may incur some expense in responding to a request for access. Nevertheless, our preference would be for organizations not to require individuals to pay fees for accessing their own personal information. At a minimum, any fees that may be charged under the legislation should not present a barrier to access. The proposed full cost recovery scheme may not be appropriate under all circumstances. Under such a scheme, individuals could potentially be charged prohibitively high fees if an organization fails to implement an appropriate records management system that readily provides access to personal information.

To ensure that fees do not become a barrier to access, we would suggest that there be a schedule of fees, similar to that prevailing for access to personal information in the public sector privacy legislation in Ontario. In our view, this would balance the interests of organizations and individuals in this area. Further, we agree that individuals should be entitled to review, without charge, information that was used to deny a benefit or service or increase a charge. In addition, we would suggest that if fees are permitted, there should be at least two hours of free search time and no fee to appeal a decision about access to one's own personal information.

Nuisance requests may be minimized if fees for access are charged. We do not object to a reasonable, strictly defined and limited provision to control those that may occur. Standards should be prescribed in the legislation for determining what constitutes reasonable grounds for an organization

to conclude that a request is a nuisance request. Some examples could be that the request is a part of a pattern of conduct that amounts to an abuse of the rights under the legislation and that answering it would interfere unduly with the operations of the organization. A nuisance provision would have to include procedural safeguards, such as an obligation to provide notice to the individual of the decision not to deal with the request along with the reasons for that decision.

Any decisions made by the organization in regard to correction requests, fees, the obligation to provide access, and nuisance requests should be appealable to the oversight body.

Would My Organization Be Able to Move Information Outside Ontario?

Question 7: Should the proposed Act address moving information outside Ontario?

It is our understanding that the federal *Personal Information Protection and Electronic Documents Act* will apply to personal information that is transferred from Ontario to another province for commercial purposes. However, this legislation does not provide any protection for personal information that is transferred from Ontario to another country, or for personal information that is transferred from Ontario to another province for non-commercial purposes.

To ensure that there are safeguards for the full range of personal information that may be transferred outside of the province, we agree that the proposed legislation should address moving information outside Ontario. Specifically, the legislation should include provisions that require organizations to take reasonable steps to ensure that the privacy protection provisions of the legislation are respected when personal information is used or disclosed outside Ontario.

It is becoming an increasingly common practice for privacy legislation to include provisions governing the use and disclosure of personal information beyond jurisdictional boundaries. For example, *Directive 95/46/EC of the European Parliament and of the Council of the European Union, on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, states that member states shall not transfer personal data to a non-member country, unless the non-member country ensures an adequate level of protection.

The proposed private sector privacy legislation in Australia includes a privacy principle which would prevent organizations from disclosing personal information to a recipient in a foreign country that is not subject to a comparable information privacy scheme, except with the consent of the individual. Where personal information is transferred by an organization to another jurisdiction for use by another part of the same organization, Australia's proposed legislation provides for the extra-territorial operation of the legislation. In our view, the Australian model represents a reasonable approach to this issue.

Under Australia's proposed legislation, the limited circumstances in which personal information may be transferred to a recipient in a foreign jurisdiction are set out in the legislation. One of the circumstances is where there is a "contract which effectively upholds principles for the fair handling of the information that are substantially similar to the National Privacy Principles." We support this approach as one of several mechanisms for ensuring that the privacy protection provisions of the legislation are respected when personal information is transferred outside of Ontario.

The inclusion of provisions to address moving information outside Ontario would help to prevent organizations from circumventing the privacy protection requirements in the province by moving personal information to jurisdictions with less stringent requirements. It would also prevent organizations from disclosing personal information without ensuring adequate privacy protection to other organizations operating in jurisdictions without comparable legislation. Without such provisions, an organization operating within the province of Ontario would be able to transfer personal information to organizations outside of the province that are not bound by the legislation or avoid compliance with the requirements of the legislation by moving its data processing operations into a jurisdiction that does not have any private sector privacy legislation.

What Would My Organization Have to Do Regarding Existing Personal Information Records?

Question 8: Is the proposal for transition as an Act comes into force appropriate?

We support the proposal to require organizations to respect the privacy protection requirements of the legislation for all personal information, including existing records. In our view, a privacy protection scheme that did not apply to pre-existing records would be completely unworkable. We also agree that the proposed transition period of one year is appropriate. However, during this transition period, it is essential that the government make a commitment to allocating sufficient resources to build public awareness of the legislation – to inform individuals about their rights and to inform organizations about their obligations under the new legislation. Specifically, we would suggest that the oversight body should be provided with adequate resources to undertake a formal role in educating both the public and private sector organizations about the legislation, prior to its coming into force.

Many organizations operating within the province that collect, use and disclose personal information have already voluntarily implemented privacy policies based on the CSA Code. Other organizations, which operate at a national level, have voluntarily applied to their Ontario operations, a privacy policy based on Quebec's private sector privacy legislation. For these organizations, the transition from a voluntary privacy code to a legislated code should not pose any difficulties. However, for organizations that do not already have a privacy policy, significant resources may need to be allocated in order to successfully implement the legislation.

A transition period of one year will provide organizations with time to review their existing practices with respect to the collection, use and disclosure of personal information and, where necessary, implement new policies and procedures to fulfill their obligations under the legislation. It will also give organizations an opportunity to review their existing collections of personal information to determine whether or not the necessary consents have been obtained for any use or disclosure that may take place after the legislation comes into force. In some cases, organizations may have to contact individuals to obtain consent, if they wish to continue to use or disclose existing collections of personal information. In addition, a one year transition period will provide time for organizations affected by the legislation to educate and train staff about new policies and procedures to facilitate implementation of the legislation.

Evaluating the Proposed Approach to Reflecting the CSA Standard (MCCR page 15)

Question 9: Does the approach of the proposed Ontario Privacy Act strike an appropriate balance between meaningful privacy protection and clear, workable rules?

While the proposed framework which incorporates part of the CSA Code would provide greater privacy protection than that which currently exists, it is our view that the proposal does not go far enough in striking an appropriate balance between meaningful privacy protection and clear, workable rules. This conclusion is based on the fact that three of the 10 privacy protection principles from the CSA Code appear to have been excluded from the proposed legislation. Specifically, the principles of accountability, accuracy and openness have not been included. In some cases, a principle may have been omitted because it is deemed to focus on process rather than outcome. Although it was not specifically stated, the implication is that the inclusion of these principles would impose an undue regulatory burden on organizations.

We would argue that the proposal not to include some of the privacy principles of the CSA code will not alleviate the administrative burden on organizations. On the contrary, it is our view that incorporating only some of the privacy principles into the new legislation will pose more of an administrative burden on organizations than would incorporating the CSA Code in its entirety. The reason for this is that made-in-Ontario legislation based on part of the CSA Code would not be consistent with the federal *Personal Information Protection and Electronic Documents Act*, which incorporates all of the principles of the CSA Code. If the provincial legislation is not harmonized with the federal legislation, organizations that operate inter-provincially or at the national level may be forced to contend with more than one set of privacy standards.

It is our view that the protections provided under the CSA Code should not be sacrificed in favour of minimizing the administrative burden on organizations entrusted with personal information. Even if the exclusion of the accountability, accuracy and openness principles were to minimize the burden on the information custodian, it would also make it more difficult for individuals to exercise their rights under the new legislation. The principles set out in the CSA Code reflect a consensus established through consultations with a broad range of industry groups. There is no evidence that private sector organizations are opposed to or will have difficulty complying with any of the requirements set out in the CSA Code.

As noted previously, openness is a prerequisite for individuals to exercise their rights under the proposed legislation. In our view, the absence of a requirement for organizations to adhere to this principle renders the other rights conferred under the legislation meaningless. For example, before individuals can access or correct their own personal information or lodge a privacy complaint, they need to be able to obtain information about procedures for accessing and correcting their own personal information and procedures for challenging an organization's compliance with the privacy principles.

With respect to accuracy, it is our view that the legislation should require organizations to take all reasonable steps to ensure personal information will be as accurate as necessary for the purpose for which it is being used or disclosed. If there is no requirement to ensure the accuracy of information before it is used or disclosed, personal information that is inaccurate, incomplete or out of date could be proliferated throughout a number of databases and used to make decisions that will adversely affect individuals. Ensuring the accuracy of personal information, before it is used or disclosed, is an important fair information practice that should not be sacrificed to lessen the burden on organizations.

With respect to the accountability principle, in his 1995 report for the Canadian Standards Association, *Implementing Privacy Codes of Practice*, Colin Bennett stated:

> The appointment of a designated individual, the name of whom should be publicly available, is now seen as a necessary condition for any effective data protection regime. The appointment of a "Data Controller" appears as the last principle within the 1981 OECD *Guidelines*. It has rightfully been given initial prominence in the CSA *Model Code*. Most public sector privacy legislation requires agencies to designate a similar officer.

Professor Bennett further noted that the designation of one official does not seem to be a difficult principle for industry to accept, although the roles and responsibilities of this individual may vary depending on the size and complexity of the organization.

The designation of one or more individuals who are responsible for compliance can not only facilitate the organization's implementation and compliance with the privacy rules, but can also facilitate individuals in exercising their rights under the legislation by providing a single point of contact with the organization regarding privacy matters.

Providing Flexibility for Unique Privacy Needs (MCCR page 15)

Sectoral Codes to Respond to Unique Privacy Needs

We agree that the proposed legislation should be technologically neutral and suitable for a broad range of organizations and types of personal information. We also recognize that, in some cases, specialized rules may be necessary for specific sectors.

The consultation paper suggests that the legislation will include two mechanisms for establishing specialized privacy standards – a schedule setting out the privacy rules for the health sector and a process for establishing or adapting privacy rules for specific sectors or types of personal information.

With respect to the first mechanism, it is not clear what process is being envisioned in establishing a schedule for the health sector. Before we can comment on the appropriateness of this mechanism, we need to know how the schedule will be developed, what types of privacy requirements will be included in the schedule, whether the health sector organizations will be subject to the same type of oversight as other organizations covered by the proposed legislation, and the process through which the schedule will be modified. It is our view that whatever process is put in place for developing and revising the privacy requirements for health information, there must be openness and accountability to the public. As mentioned previously, our specific recommendations for privacy requirements for the health sector will be outlined in a separate submission in response to the consultation paper of the Ministry of Health and Long-term Care.

Question 10: Does the proposal for sector codes subject to a legislated process make sense?

As stated earlier in this submission, we are not opposed to the inclusion of provisions for sectoral codes in the new legislation. While sector specific codes are one mechanism for enhancing flexibility, they should be used to enhance or expand upon privacy protection standards as set out in the legislation rather than to diminish those standards.

We enthusiastically endorse the portion of the proposal for sectoral codes in the discussion paper that would require the proposed legislation to set out a rigorous and transparent process for developing or changing the code and the requirement for participation by representatives of the sector and the public interest, as well as experts.

We are pleased with the statement that a sectoral code could not simply be a vehicle to advance the views or interests of one group at the expense of others. We also support the proposed requirement that any code would have to improve the overall privacy regime in Ontario, and recommend that this statement or a similar one be incorporated into the statute itself.

We also support the proposal that a sectoral code require the final approval of the government, as long as the approval process incorporates a high degree of scrutiny by the public and the oversight body.

Harmonization with federal law

If the sectoral codes derogate from the legislated privacy standards, this raises a concern about how to ensure that individual codes are consistent with standards set out in the federal *Personal Information Protection and Electronic Documents Act*. It is intended that Ontario's privacy standards mirror those set out in the federal legislation as much as possible, a goal which we support. However, the federal law does not make provision for sectoral codes that impose different standards of privacy than the framework legislation. It is not clear to us how Ontario codes will be harmonized with the federal regime. This may be a concern for organizations that are regulated by provincial law but carry on activities across provincial borders, such as insurance companies. They may be faced with the situation of being subject to differing rules, depending on whether their activity is covered by an Ontario sectoral code or the federal law.

Principles for development, use, and monitoring of sectoral codes

Should the privacy legislation contain provisions for sectoral codes, we recommend that the following principles be considered to ensure that codes improve the privacy regime in Ontario:

- Codes should have the force of law and be approved by the government in an open and accountable manner.
- Codes may modify or explain the application of the legislated data protection principles/ standards, however, our preference is that codes be used to enhance or expand upon data protection standards articulated in the statute, not to diminish those standards.
- Codes should not limit or restrict individuals' rights to obtain confirmation that an organization holds their personal information, to request the correction of their personal information held by an organization, or to request that a statement be attached to any such information if the correction sought was not made.
- If a code is going to modify the legislated data protection standard, there should be safeguards to ensure that the intrusion on privacy is necessary and minimal. The safeguards should include: statutory criteria for exempting; public notice of intention to create an exemption; exemptions to be done by statute or regulation, rather than by Ministerial fiat or order-in-council; and consultation with data subjects and data controllers before approval of the exemption.

- Public notice and meaningful consultation must be undertaken prior to the approval, amendment or revocation of a code. Once a code is issued, the public and relevant parties must be notified of its implementation.
- Prior to the approval, amendment or revocation of a code, the government must consult with the oversight body for its review and comment.
- Codes may provide for alternate complaint procedures but cannot derogate from the right of complaint to the oversight body.
- Codes should be subject to the oversight, enforcement and offence provisions defined in the data protection legislation.

What Exemptions and Exceptions Would Apply? (MCCR page 17)

Question 11: Are the exemptions and exceptions to the proposed Ontario Privacy Act reasonable?

The consultation paper provides that the exemptions from the consent and/or access requirements in the proposed legislation would address the same issues covered by the federal privacy legislation in order to avoid confusion between the two laws.

In our view, avoiding confusion is a laudable goal. We do not take issue, in general, with the bulk of the proposed exemptions or exceptions that are listed in this part of the consultation paper. When it comes to the exact drafting of these provisions, however, we believe care will have to be taken to ensure that the exemptions and exceptions are as narrow and as justifiable as possible. In addition, the new legislation should clarify that exemptions from the consent and/or access requirements are not mandatory and should only be applied, at the discretion of the organization, in the limited circumstances where they are clearly warranted. With respect to exemptions to the right of access, it should be emphasized that the right of access to one's own personal information may override an organization's claim for an exemption from providing this right. The legislation should make it clear that organizations are expected to consider exercising discretion in favour of disclosure to the data subject, rather than simply applying whatever exemptions are contained in the legislation in a routine manner.

We would like to convey the following more specific comments on certain items from the list, based upon our review of similar sections in the federal privacy legislation as well as in the Ontario public sector privacy legislation:

- **Law Enforcement:** The definition of a "law enforcement agency" is one which particularly requires the narrow drafting suggested previously in order to avoid creating a dangerously broad exemption. The government should consider, for example, having requirements for specialized training and some type of government licencing or classification scheme before anyone can be deemed to be employed in law enforcement.

- **The Welfare of the Individual:** We agree that there is a need for this type of exemption, however, the determination of what is "clearly in the individual's presumed interest" has the potential, absent appropriate safeguards, to be a subjective process. This could be avoided if the proposed legislation sets out criteria for making such a determination.

- **Public Domain Information:** According to the consultation paper, the proposed exemption from consent for collection, use and disclosure would apply to information in the public domain. Our views on this statement depend, in part, on what is determined to be public domain information. This determination is one of the more difficult issues currently facing

the access and privacy community in Canada and abroad. There needs to be some public debate and perhaps harmonization of the approaches taken to determining what information is in the public domain. At a minimum, there should be a recognition of the intended purposes of each public database and uses inconsistent with those purposes should not be permitted under the legislation.

- **Statutory Authorization:** In our view, the proposed exemption should apply where another law, federal or provincial, provides *express* authority for the collection, use or disclosure of personal information.

- **Conflicting Personal Interests:** We are unsure of what is meant by "an individual would not have a right to access personal information if another person's welfare is involved." If "another person's welfare" is a reference to that person's personal information, then we are of the view that there should be a balancing process, such as that set out in section 21 of the provincial *Freedom of Information and Protection of Privacy Act*. The legislation should set out factors to consider in conducting the balancing process; for example, if the personal information is relevant to a fair determination of the requester's rights. At the same time, the principle of severance should operate where applicable, so that a requester could obtain a maximum amount of his or her personal information. However, if "another person's welfare" may be affected, as in the possibility of that person being harmed in some manner, that would already be a factor weighing against disclosure.

- **Research:** We would favour an exception for research that defines a process whereby research review bodies, such as ethics review committees, are required to balance the privacy implications of research against the public good that could flow from it. As well, we suggest that regulations provide for the development of standards for the use of personal information for research and that there be an obligation, where possible, to use personal information in non-identifiable or "anonymized" form.

How Would The Proposed Ontario Privacy Act Be Enforced? (MCCR page 19)

Since the issues arising from Questions 12 and 13 are closely related, we have combined our responses into a single narrative.

Question 12: Should the proposed Ontario Privacy Act provide for appeals without the necessity of going to court?

Question 13: Do you agree with the proposal that the proposed Act provide for the following:

Mediation
Investigation Authority
Compliance Orders
Assurances of Voluntary Compliance
Support for Civil Remedies
Offences

We support the stated aim of the proposed legislation, which is to provide clear, meaningful rules and avoid red tape or undue regulatory burdens. We agree that having a single body responsible for compliance with the legislation is the best way to achieve this goal, although we have a few concerns with some of the details of the proposed system, as discussed below.

Business regulation model vs. privacy compliance model

In our view, the proposed business regulation model, derived from the *Business Practices Act* and the *Consumer Protection Act*, is not the most appropriate one for regulating compliance with privacy laws. We have a fundamental problem with the design approach itself – instead of applying a business regulation model in the privacy context, from our perspective, it would be more appropriate to apply a privacy compliance model in the business context. We believe that a privacy compliance model is preferable in a number of respects, particularly in the areas of review mechanisms, offences, education, and prevention. We will address these issues in more detail below.

Our preference for a compliance model that emphasizes mediation, education, and prevention is based on a number of factors. The proposed law extends beyond the business sector, including non-business organizations such as non-profit corporations, charities, self-regulating bodies, etc., that are not otherwise subject to business-related regulatory schemes, yet will be required to comply with privacy laws. In addition, the privacy-focused compliance model has a proven track record in Ontario and in many other jurisdictions (e.g., Alberta, British Columbia, Quebec, Europe, Australia,

and New Zealand), and is the approach embodied in the federal *Personal Information Protection and Electronic Documents Act*. Finally, a significant body of expertise has been developed in this province in responding to public complaints and concerns over access to, and the collection, use and disclosure of personal information held by public sector organizations. This expertise could now be applied to dealing with similar issues that arise under the proposed legislation.

One level of administrative review

We do not believe the legislation should provide for an appeal from a decision of the oversight body (although judicial review should of course be available in limited cases as it is for the pubic sector privacy legislation). We support the stated goal of having a single body responsible for compliance with all provincial privacy legislation. However, statements later in the paper suggest that the legislation could provide for two levels of administrative review of an organization's action, with a possible further review by the courts. In our view, this would conflict with the stated goal, and would be inefficient and unnecessarily complicated for members of the public. This approach would also result in needless duplication of services, resources and expertise.

We believe it would be far more cost effective and straightforward to have a single, specialized oversight body to fully resolve complaints. This approach is more in keeping with federal private and public sector privacy legislation, Ontario's public sector legislation, and private and public sector models in numerous other jurisdictions (e.g., Alberta, British Columbia, Quebec, Europe, Australia, and New Zealand).

In our view, any concerns about the absence of an appeal from a decision of the oversight body can be addressed through a combination of the availability of judicial review, as well as internal reconsideration mechanisms provided by the common law and routinely implemented by administrative tribunals.

We would also like to point out that we believe the legislation should not prevent individuals from pursuing other potential courses of action against organizations for possible violations of the legislation. For example, under the new legislation, individuals should be able to complain to the oversight body at the same time as they complain to a body that regulates professional conduct. However, it is our view that the oversight body for the new legislation should have the discretion to defer any matter to another review body, whenever it is appropriate to do so.

Initiating complaints

We support the notion that individuals who believe their privacy rights have been breached should first contact the organization in question directly to try to resolve the matter. This could involve informal mechanisms, including mediation established by the organization or to which the organization has access as a result of membership in an association. However, the government may want to consider whether exceptions to this general rule are appropriate in certain circumstances, allowing for complaints to be made directly to the oversight body.

Mediation

We strongly endorse the proposal to integrate mediation into the system. In our experience, the majority of privacy complaints and appeals involving requests for access to personal information can be resolved informally through mediation, which ultimately requires fewer resources and leaves complainants and organizations more satisfied.

It is not entirely clear from the paper where and when mediation would take place, and by whom it would be conducted. In general, we support the availability of mediation at any point in the process, including attempts by an organization to resolve issues before they develop into formal complaints. However, we feel that the oversight body should be given express statutory authority to employ specialized mediators who can apply their expertise to the privacy issues raised by complaints. This will ensure that mediators with specialized knowledge and experience in dealing with privacy disputes will be available to the parties. In our view, non-specialized mediators without privacy expertise would be far less effective in resolving such disputes.

Investigative authority

We fully support providing the oversight body with strong investigative powers. We recommend that the oversight body be given the following explicit powers, in order to fully achieve its mandate:

Initiation of complaints

- receive complaints;
- initiate complaints on its own motion; and
- refuse to conduct an investigation or inquiry on grounds that the complaint is frivolous or vexatious, or made in bad faith.

Notice to parties

- notify affected persons as parties.

Investigation

- investigate a complaint, including the power to order production of records, enter premises of an organization, examine records and information systems, compel evidence, examine witnesses, and receive evidence under oath.

Mediation

- refer complaints to mediation and conduct mediation.

Inquiry

- hold inquiries to dispose of the issues in a complaint;
- control the process of the inquiry and set rules and practices as required;
- conduct inquiries in private and permit exchange of submissions; and
- determine issues of fact and law arising in the inquiry.

Audit

- conduct audits to ensure compliance with standards set by or under legislation.

Remedies

- make binding orders disposing of the privacy issues in the inquiry;
- require that a duty imposed by or under the legislation be performed;
- require cessation of collection, use or disclosure of personal information;
- require destruction of personal information;
- require implementation of an information practice;
- order anonymization of research data;
- order production from non-parties;
- require notice to the oversight body of any action taken in response to a decision of the oversight body;

- file an order with the court so that it can be enforced as such;
- state a case to the courts;
- make findings and recommendations, and issue reports, as a result of privacy audits; and
- make other remedies which are proper in the circumstances (not including fines or damages).

Other

- consolidate complaints and inquiries; and
- delegate powers.

Some of these points are elaborated upon below.

Protection for witnesses giving evidence during an investigation

Generally, investigative powers are accompanied by protections for individuals who are interviewed as part of an investigation. We recommend that the legislation make provision for protecting witnesses from civil, criminal or quasi-criminal liability arising out of statements made to the oversight body.

Compliance orders

We agree that the oversight body should have the power to issue orders in certain circumstances. These orders should be final and binding, subject only to judicial review, with appropriate standards of deference that recognize the expertise of the oversight body. In this way, the vast majority of complaints will be resolved far more quickly, and the considerable legal fees associated with a court review will not act as a barrier to members of the public.

This approach has proven effective under Ontario's provincial and municipal public sector laws. Since the inception of the provincial *Freedom of Information and Protection of Privacy Act* in 1988 and the *Municipal Freedom of Information and Protection of Privacy Act* in 1991, the IPC has received more than 8,000 appeals, and issued more than 3,000 orders. About one-third of these appeals stem from requests for personal information, and are comparable to the types of access reviews which would take place under the new legislation. Very few appeals proceed to court (about 1.5%), and only 0.1% of the total appeals have been overturned by the courts.

By contrast, under the federal regime, which allows for appeals to the courts from decisions of the oversight bodies, matters proceed to court at more than twice the Ontario rate.

Where matters do proceed to court, legal fees for a party typically range from $5,000 to $15,000, and the process can last a year or more.

The approach we recommend also would be consistent with that in Alberta, British Columbia and Quebec.

Assurances of voluntary compliance

We support the general concept of organizations agreeing to take corrective action to resolve a complaint. As suggested in the consultation paper, the acceptance of a voluntary assurance should be subject to the discretion of the oversight body. Assurances may be appropriate where the matter is settled between the complainant and the organization, but the complaint may raise broader privacy issues which the oversight body believes should be addressed. Accordingly, the oversight body must have the option of proceeding to issue a compliance order, or other remedy, rather than accept an assurance.

The use of assurances of voluntary compliance should be subject to suitable safeguards to ensure their effectiveness. For example, the requirements of placing time limits on their operation and consulting with affected parties as to the appropriateness of the agreement before accepting it should be considered. The government should also determine an appropriate manner to make these assurances publicly available in order to encourage transparency. In addition, organizations should be required to report back to the oversight body, within a six month period, about the measures that were taken.

Privacy audit

We recommend that the oversight body be given explicit authority to initiate and conduct privacy audits to ensure compliance with standards set by or under legislation. The oversight body also should have the ability to make findings and recommendations resulting from an audit, and to issue a report making such findings and recommendations public.

Support for civil remedies

We support the proposal that under the legislation, individuals be permitted to seek damages in court arising from violations of their privacy rights. The ability to seek civil remedies should be made explicit in the legislation itself, rather than being left to the common law, which otherwise may not support such actions.

Offences

Although we believe that the legislation should provide for offences, our preference would be for the proposed enforcement model to place less emphasis on penalizing "bad actors." In our experience, the vast majority of cases involving privacy infractions are the result of well-intentioned organizations that are either careless, or do not understand or appreciate the importance of good personal information management practices. While the legislation should provide for offences in limited cases involving wilful misconduct, the primary focus should be on educating those organizations that are not complying with the legislation and ensuring the organization takes steps to reduce the risk of any future breaches, especially since, in most cases, the breach has already occurred. In our experience, this approach is far more satisfactory, both to the complainants and to the subject organizations.

We believe the public sector model should be adopted, whereby offence proceedings are initiated not by the oversight body, but by others such as the complainant, the police, the Attorney General, or perhaps the Ministry of Consumer and Commercial Relations, if appropriate. The legislation should explicitly designate an agency responsible for prosecutions, although private prosecutions should not be precluded.

We recommend that the oversight body not be designated as the agency responsible for prosecutions. The oversight body can be most effective in working with organizations to correct personal information management practices, offering its expertise and experience in a constructive and forward-thinking manner. Having the oversight body conduct the prosecution compromises its effectiveness as a compliance regulator.

Despite the above, the oversight body should be permitted to participate in any prosecutorial proceedings initiated by others, where the oversight body deems it appropriate. The oversight body may be in a position to assist the court on issues before it, without taking on the role of prosecutor.

In our view, as in the public sector model, the listed offences should apply only where the conduct in question can be considered "wilful."

Whistleblower protection

We support the idea of protection from reprisals for whistleblowers, although consideration should be given to expanding the scope of protection to all individuals, not just employees. This would recognize that non-profit, non-commercial entities will be subject to the legislation. Members of these organizations should be given the same protections when exposing breaches of the legislation as employees.

Other roles for the oversight body

We recommend that the oversight body be authorized by statute to conduct assessments and offer comment on the privacy impact of programs and proposed legislation. We have found that such reviews of the privacy impact of proposed initiatives have been an effective tool in raising both the public and government organization's awareness of privacy.

We also recommend that the oversight body be empowered to conduct public education programs and provide information concerning the legislation and the oversight body's role and activities under the legislation.

Finally, the oversight body should be given express powers to engage in or commission research into any matters affecting the understanding or carrying out of the purposes of the statute; to give advice and recommendations of general application to an organization on matters respecting its rights or obligations under the legislation; and to receive representations from the public concerning the operation of the legislation.

Title of the Proposed Legislation

The consultation paper indicates that the title of the legislation will be the *Ontario Privacy Act*. We believe that this title is highly misleading and the public may find it confusing. We would suggest the title should clearly distinguish this legislation from provincial and municipal public sector privacy legislation. In the province of Quebec, there are two pieces of privacy legislation – one for the public sector and the other for the private sector. The private sector legislation is clearly distinguished from the public sector legislation with the title, *An Act respecting the protection of personal information in the private sector*. In our view, it would be less confusing if Ontario's private sector legislation were clearly distinguished in this manner. For example, a more straightforward title might be the *Ontario Private Sector Privacy Act* or the *Ontario Privacy Act for the Private Sector*.

Conclusion

Once again, we applaud the government for recognizing the need for made-in-Ontario private sector privacy legislation and for moving forward with this important initiative through the release of the consultation paper. The implementation of this legislation now will ensure that rules for the collection, use and disclosure of personal information within the province are consistent with public expectations and this should indeed help to position the province as a trusted marketplace. Without this legislation, individuals and private sector organizations in the province may not be able to take full advantage of the opportunities offered by emerging technologies and the new digital economy.

In general, we support what is being proposed in the consultation paper. In our view, a legislative framework based on the CSA Code will provide the best solution to privacy issues in the private sector. We also like the fact that the CSA Code will be incorporated into the body of the legislation, rather than being appended as a schedule, as is the case with the federal *Personal Information Protection and Electronic Documents Act*.

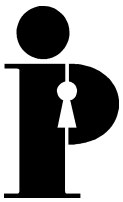
However, we do not support the proposal to exclude some of the privacy principles set out in the CSA Code from the legislation. Specifically, the principles of accountability, accuracy and openness have not been included. With respect to accountability and openness, the rationale for omitting these privacy principles was that the requirements set out under these principles were deemed to be process-related rather than outcome-related, and that excluding procedural requirements, such as these, would lessen the regulatory burden on organizations. With respect to accuracy, it was suggested that privacy legislation is not appropriate or practical for resolving disputes about the accuracy of personal information.

While the exclusion of these principles may minimize the administrative burden on organizations, it may also, in some cases, make it more difficult for individuals to exercise their rights under the legislation. In addition, the exclusion of some of the requirements of the CSA Code will make Ontario's legislation inconsistent with the federal legislation. Consequently, organizations operating within the province could be subject to substantially different privacy requirements, which could be confusing for the public. This would be incongruent with two of the stated goals in developing Ontario's own legislation – to provide comprehensive and seamless privacy protection and compatibility with other laws.

There is no evidence that any of the privacy principles set out in the CSA Code pose an undue regulatory burden on organizations. As noted, the CSA Code reflects a consensus that was established through extensive consultations with representatives of a broad range of industry sectors. It is our view that the protections provided under the CSA Code should not be sacrificed in favour of minimizing the administrative burden on organizations entrusted with personal information.

We also do not support the creation of an enforcement scheme based on a business regulatory model. Such a scheme would encompass principles which are substantially different from those upon which the current public sector privacy protection legislation in the province is based. Since the government is envisioning only one oversight body for all privacy legislation, having two separate enforcement schemes does not make sense administratively or practically. This proposal would be inconsistent with the stated goal to provide efficient, fair and effective enforcement.

In our view, the principles underlying the existing pubic sector model, which emphasizes mediation and education, and requires minimal involvement of the courts, results in an enforcement scheme which is much more accessible to the public than that which is being proposed in the consultation paper. Considerable time and effort has been devoted, within the public sector scheme, to the development and implementation of user-friendly policies and procedures which provide an optimal level of customer service. The public is already familiar with this model and likes it. The proposed implementation of a new scheme for the private sector would only create confusion and pose an unnecessary burden on the oversight body, which would have to implement new policies and procedures to accommodate the new legislation. We see no advantage for the public or for private sector organizations in setting up an enforcement scheme which is inconsistent with the principles underlying the privacy protection scheme currently in place for the public sector in Ontario.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca