Information
and Privacy
Commissioner/
Ontario

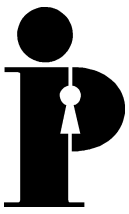
Balancing Access and Privacy:

How Publicly Available Personal Information is Handled in Ontario, Canada

Symposium on the Protection of Information in Local Governments

The Administration and Use of Personally Identifiable Information in a Global Society

Tokyo, October 2000



Ann Cavoukian, Ph.D.
Commissioner

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

Commissioner Ann Cavoukian gratefully acknowledges the assistance of Mary O'Donoghue, Legal Counsel, for her assistance in the preparation of this paper.

This publication is also available on the IPC website.

Table of Contents

Introduction

Common issues and concerns associated with the public disclosure and use of publicly available personal information have been identified in many jurisdictions. Privacy concerns have become more acute with the computerization of lists, directories and databases containing the personal information of individuals. As you are all aware, computerization removes the practical difficulties of locating and accessing information that is held in paper records in multiple locations, and extracting and copying relevant information. A computerized record may be searched under many different fields (including the names of individuals), manipulated, linked, mined, copied and disclosed without difficulty to many. Because of the ability to manipulate and manage information, computerization has been accompanied by a surge in the value of personal information as a commercial commodity. At the same time, computerization has provided opportunities for enhancing public access to information.

The privacy concerns discussed in this paper relate to personal information that is held in both computerized form and in paper copies, and which is maintained and disclosed by both government and the private sector. Government-held public data may contain information that relates to businesses, or may contain the personal information of identifiable individuals. Publicly available data collections containing personal information include personal property securities registrations, land transfer registries, property tax assessment rolls, registrations of death, court records, voters lists and driver's licence databases.

Publicly available information in the private sector includes telephone directories, e-mail directories, customer lists that are traded between businesses, and material that is published by the media. Public information maintained by private sector organizations under statutory authority include lists of members of professions and their specialties, such as lawyers or physicians, or lists of securities dealers.

The basic question is whether information that has entered the public domain is public for all purposes and without any limitations on its use and disclosure or whether some of the rules with respect to fair information practices continue to apply to the information.

Many would argue that once personal information has been made public, there can be no reasonable expectation of privacy relating to that information, and therefore, privacy protection rules no longer apply to it.

The commodification of personal information as a valuable commercial asset leads to intense pressure on business and government to make personal information available for commercial gain. Robert Gellman noted in his paper entitled *Public Registers and Privacy: Conflicts with Other Values and Interests*, (21st International Conference on Privacy, Hong Kong, September 13, 1999) that many of the practices of government in making personal information available to

sectors of the public, and especially business, have developed over time. Those entities, accustomed to access to the information and who rely on it for their business, exert significant pressure on government to continue disclosure, and render it politically difficult to alter the practice. Government-held information is considered to be quite accurate and up-to-date, and accordingly, in many cases more commercially valuable than that held by the private sector. In times of restraint and tax cutting, it is tempting for governments to generate non-tax revenue by selling personal information in its holdings.

However, many of the disclosures were practices developed at a time when the predominance of paper records provided a practical protection for personal information. It was just too difficult for any but the most determined to locate and copy personal information, which was held in many different locations. The value of "practical obscurity" has been eroded by computerization, and so disclosure now takes place in an entirely new context. This new context, in my view, necessitates a review of government practices in the sale of personal information.

Government collects personal information from its citizens for a variety of reasons and purposes. It also makes the personal information that it collects publicly available for various public policy purposes, for example, a voters list may be available for public inspection to prevent voter fraud, or to ensure that the names of deceased voters are removed from the lists. The public is granted access to a personal property securities register in order to ensure that the property, which it proposes to purchase, is free of encumbrances.

Given that the personal information has been collected from the individual, in many cases by compulsion of law, is it fair that the information be made available for commercial or other purposes, without the consent of the individual, and for reasons unconnected to the purpose for its initial collection?

When members of the public become aware that their personal information which has been collected for a specific reason, is now being made widely available for possibly unconnected reasons, they make it known that this practice is unacceptable. In a postscript to Order P-1316, (1996) former Commissioner Tom Wright said:

> Earlier this year the City of Victoria [in British Columbia] made [property] assessment information available on its Internet website. This lasted for one day at which time the mayor shut down the website. Why? The public complained in large numbers that they didn't like the fact that anyone connected to the Internet could have such ready access to assessment information. Yet the exact information has been and remains available on paper at city hall.
>
> I believe this example amply demonstrates that the public feels that it does make a difference when information which has been publicly available in a paper-only world becomes available electronically.

Similarly, when the U.S. company Toysmart had financial difficulties, it decided to sell its most valuable asset — its customer database. The company's privacy policy stated that it would never disclose this information to unauthorized third parties. The resulting public outcry necessitated the intervention of the Federal Trade Commission.

It is my belief that personal information, once made public, is not necessarily public for all purposes, and is not necessarily public forever. Publicly available information should be subject to some fair information practice rules, which may be appropriate in the circumstances.

Personal Information Held by Government in Canada

Personal information may be collected by government from individuals under compulsion of law. In Canada, an individual must identify himself to the state for the following reasons:

- to register birth, death or marriage
- to pay provincial, federal and sales taxes
- to vote
- to enroll in a government health plan
- to enroll in public school
- to enter the country
- upon arrest or charge by the police
- to police while on parole or probation
- upon request by police while driving a motor vehicle
- to apply for a licence or state benefit
- to apply to change one's legal name
- to supply a change of address to Canada Post (a quasi-government body)
- for periodic census (may identify by name all who are resident or staying in house)
- for municipal property tax collection

While the individual must identify himself to the state in Canada, our liberal democratic tradition restricts the power of the state to require information from citizens, except where provided by law. For example, except where one is in charge of a motor vehicle, where one has been observed committing an offence, or upon arrest or charge, the citizen is not obliged to identify himself to the police. Those who hold a driver's licence are required to notify the Ministry of Transportation of the province of any change of address, and this information is made available to the police, when required. If one does not drive, there is no requirement to inform the province or the police of a change of address. One must provide a current address to the federal taxation authorities, but only upon filing an annual tax return.

The various levels of government (federal, provincial and municipal) do not ordinarily share a single database of information about individual citizens, although more sharing of this nature is taking place between federal and provincial government agencies on taxation matters.

The Canadian constitution provides protection to citizens from unlawful searches or seizures, including seizures of information by government (*Canadian Charter of Rights and Freedoms*, section 8). This constitutional provision has at its heart the protection of the privacy, autonomy and dignity of the individual. The Supreme Court of Canada has formally recognized these values. In *R. v. Plante* (1993), 84 C.C.C. (3d) 203 Mr. Justice Sopinka said the following about the nature of an individual's right to control information about himself or herself:

> [1] … In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. (see excerpts at pp. 211–213)

The power of Canadian governments to deal with personal information is further regulated by various privacy enactments in federal Canada and in the provinces. The Parliament of Canada has passed the *Privacy Act* and the *Access to Information Act*, which are designed to be read together. Most of the provinces have enacted a Freedom of Information and Protection of Privacy Act, which regulates both access to government information and the protection of personal information.

Freedom of Information and Protection of Privacy in Ontario, Canada

I would like to turn to my experience in Ontario in order to illustrate the kind of challenges we face in maintaining some level of privacy protection for personal information which is made public.

The Access and Privacy Acts

In 1988, the Ontario government enacted the *Freedom of Information and Protection of Privacy Act* (the provincial *Act*), which regulates the information management practices of provincial government institutions, including government ministries, boards and agencies, community colleges and public hospitals. In 1991, the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*) was passed, covering municipal governments and agencies and school boards. (The municipal *Act* mirrors the provincial act in all essentials, and I shall refer to provisions of the provincial *Act*.) In all, over 2000 government institutions in Ontario are regulated by the two *Acts*.

The purposes of the *Acts* are to:

- provide a right of access to government-held information;
- provide a right of access to an individual's own personal information held by government;
- protect the privacy of personal information held by government; and
- provide for independent review of government action in the areas of access and privacy.

The Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner was established under the *Act*. The Information and Privacy Commissioner is an Officer of the Legislature who provides independent review of government action with respect to access to information and protection of privacy. In order to preserve her independence, the Commissioner does not report to a minister of government, but directly to the Legislature, through the Speaker. She is appointed upon the address of the Legislature, through a tri-partite process and serves a five-year term, which may be renewed.

The Commissioner maintains an office that is separate from government and engages her own staff. She has the power to hear appeals and make orders, respond to privacy complaints and make remedial recommendations, conduct public education and research, comment on the implications of government legislation and programs, report to the Legislature on compliance with the *Acts*, and, after hearing the "head" of a government organization, order them to cease a collection practice or to destroy a collection of personal information.

Appeals to the Commissioner

The right of access to information under the *Acts* is not absolute. Information may be exempt from disclosure under certain provisions of the *Acts*. However, the exemptions must be "limited and specific," and thus not accorded an over broad definition. Exemptions may be mandatory or discretionary. For the purposes of our discussion, a most important mandatory exemption from disclosure is that prohibiting the disclosure of personal information to a person other than the person to whom the information relates, unless disclosure "would not be an unjustified invasion of personal privacy." (Section 21)

Where a person makes a request for access to information within the custody or control of government under the *Acts*, the person may appeal to the Commissioner any decision of the institution arising from the request. Therefore, an appeal may be made where access to the requested information has been denied or only partially granted, where a request for correction has been refused, where the government has decided not to respond to the request on the basis that it is frivolous or vexatious, or where the government has charged a fee. An attempt is made to mediate a resolution of the appeal, and this is successful in the vast majority of cases.

If mediation does not result in settlement, an inquiry is held, and an order is issued, which is binding on all parties, including the government. Where the Commissioner finds that the institution was not justified in claiming an exemption from disclosure, she may order the institution to disclose the information. There is no appeal of the Commissioner's order. However, an application may be made to the Superior Court for judicial review of the Commissioner's order, on jurisdictional or procedural grounds.

Privacy Complaints

Part III of the *Freedom of Information and Protection of Privacy Act* provides rules for the protection of the privacy of the individuals whose personal information the government holds. These rules (or fair information practices) are as follows:

- personal information should, to the extent possible, be collected directly from the person to whom the information relates, unless indirect collection is necessary and authorized;
- institutions should collect only that personal information which is specifically authorized by statute, necessary for a lawfully authorized activity or for law enforcement;
- individuals should be notified by the collecting institution when their personal information is collected and the notice should contain the legal authority for the collection and the name, title and telephone number of an employee of the institution who can answer questions;

- individuals have a right of access to their personal information being held by institutions, subject only to legitimate exemptions from disclosure;
- individuals may request correction of their personal information being held by institutions, or should have the right to attach a statement of disagreement to the record;
- institutions should only use personal information for the purpose for which it was collected or for a consistent purpose. A consistent purpose is one which would have been reasonably expected by the individual. An individual can consent to a new use for the information. Information may, of course, be collected for more than one use, but all potential uses should be identified prior to collection, and all of the main uses should be disclosed to the individual at the time of collection;
- institutions should not disclose personal information except as permitted under the *Act*, or upon the consent of the individual to whom the information relates;
- institutions should use only personal information which is accurate and up to date in making decisions affecting an individual; and
- institutions should provide for the proper secure custody of personal information in their possession, and should provide for proper secure disposal of the record.

The Commissioner receives complaints from persons who feel that their personal information has not been treated in accordance with the privacy requirements of the *Acts*. The complaint is assigned to a member of staff, who looks into the matter and attempts to resolve the complaint through mediation. If unsuccessful, an investigation report is issued, in which findings are made as to whether the institution's activities were in compliance with the *Acts*. If a finding of non-compliance is made, remedial recommendations are included in the report, with follow-up procedures to ensure compliance.

Publicly Available Information

As in the privacy legislation of many jurisdictions, that of Ontario makes provision for "publicly available" information. The Quebec public sector privacy act, for example, states specifically that its access rights do not apply to information in certain public registers, namely those with respect to land transactions, civil status and matrimonial regimes.

Prior to the enactment of the Ontario legislation, a Public Commission under the chairmanship of Dr. Carleton Williams examined the issues of access and privacy with respect to government-held information. The Williams Commission Report, Volume II, at page 332, contains the following excerpt:

A third situation in which disclosure should be the general rule relates to those collections of personal information gathered by the government for the purpose of creating a public record or register. The Ontario Personal Property Security Register, described in Chapter 27 of this report, is an example of this phenomenon. There are many other registers of this kind maintained by provincial and local government institutions in Ontario. The statutory provision should clearly indicate that public access to registers of this kind is not inhibited in any respect by the privacy exemption.

The Report recommended, at page 335, that the proposed legislation include a provision taking into account the following:

1. An exemption to the general principle of access should be made to protect personal privacy. The exemption should contain these features:

    a. a list of situations in which there is an overriding interest in disclosure;

. . .

2. With respect to item 1(a) the following is proposed:

    No individually identifiable record shall be disclosed by any means of communication to any person other than the individual to whom the record pertains unless the disclosure is:

    . . .

    c. of information collected and maintained specifically for the purpose of creating a record that is available to the general public;

The decisions of the Information and Privacy Commissioner/Ontario (the IPC) regarding publicly available information involve information which is computerized, in hard copy, single items of information and vast databases. Some cases involve requests for bulk access to data, while others involve the disclosure of the contents of a single file.

There are three provisions of the *Act* which make important distinctions for "publicly available information." These are statutory exceptions to some of the access and privacy principles. The first provision is section 21(1)(c) which provides an exception to the general prohibition against disclosure of personal information in response to a request:

21(1) A head shall refuse to disclose personal information to any person other than the individual to whom the information relates except,

    (c) personal information collected and maintained specifically for the purpose of creating a record available to the general public;

The second provision is also an exemption from disclosure by the institution, but only because the information is available elsewhere:

> 22. A head may refuse to disclose a record where,
>
> (a) the record or the information contained in the record has been published or is currently available to the public;

The third provision dealing with publicly available information creates an exception for that information from the privacy rules in Part III of the *Act*:

> 37. This Part does not apply to personal information that is maintained for the purpose of creating a record that is available to the general public.

The term "available to the public" is not defined in the *Acts*, nor is there a requirement for a statutory basis for a determination by an institution that a record will be "available to the public."

Issues regarding publicly available information arise in both access to information appeals and privacy complaints. Requests are made for access to government-held data either on a record-by-record basis or in bulk form, and complaints are made about disclosures where institutions claim that the privacy rules did not apply to the information because it was publicly available.

Examples of information which we have found to be "currently available to the public" include a transcript of a court proceeding which could be obtained from the Provincial Court Reporter's office (Order P-123), documents which are available to the public for inspection through the Supreme Court of Ontario (Divisional Court) (Orders P-191, P-368 and P-775), policy and procedural manuals related to municipal tax assessment that were available at a Ministry reading room qualify (Order P-906), forensic services manuals which are used in Ontario psychiatric facilities and available for viewing by the public in the Forensic Unit of each of the ten psychiatric hospitals in the province (Order P-664), court transcripts (Order M-314), a decision of an arbitrator in a grievance hearing available from the Office of Arbitration of the Ontario Ministry of Labour (Order M-295), a copy of a report on race relations where the information contained in it was available in public libraries (Order M-369) and information published in Hansard, the official record of statements in the Legislature. (Order P-124).

Is Information "Publicly Available?"

In a 1992 case regarding the application of s. 22(a), the party to whom the records related offered to provide them directly to the requester. The Assistant Commissioner rejected the argument that this offer rendered the records "currently available to the public." He stated that to qualify, the records:

must either be published or available to members of the public generally, through a regularized system of access, such as, for example, a public library or a government publications centre.

He also said that an institution wishing to rely on s. 22(a) has a duty to inform the requester of the specific location of the publicly available records. Furthermore, the institution must ensure that the information is actually available from the alternative source. (Order P-327, Ministry of the Attorney General, July 14, 1992)

In order for an institution to establish that a "regularized system of access applies," it must show that a system exists, that the record is available to everyone and there is a pricing structure which is applied to all who wish to obtain the information. (Order P-1316, Ministry of Finance, December 16, 1996.)

To qualify as "publicly available," information must be made available to the general public.

Driver's Licence Information

A person who traces the unidentified heirs to estates of deceased individuals requested access to the names and driver's licence numbers of all Ontario drivers. The requester claimed that the section 21(1)(c) exception to the personal information prohibition on disclosure applied, because the information was "collected and maintained specifically for the purpose of creating a record available to the general public."

The Ministry of Transportation informed the IPC that individual requests for driver licensing information are not processed unless specific identifiers, such as the name or driver's licence number are provided by the requester. The Ministry had a special bulk access policy which deals with large volume requests by individual requesters. Requests are screened to ensure that planned uses of the bulk information enhance road safety and do not involve uninvited solicitation. A requester must apply for Authorized Requester status, and, if granted, must enter into a formal agreement with the Ministry. The agreement controls the subsequent use of bulk information disclosed by the Ministry.

Assistant Commissioner Mitchinson held that because the Ministry requires that a requester provide either the name or driver's licence number, it cannot be said that the Ministry routinely provides access to the general public to the name **and** licence number. He also found that because of the bulk access policy, bulk disclosures are not a routine matter for the Ministry, but are subject to constraints and a review process. He found that the section 21(1)(c) exception did not apply to bulk access to the names and licence numbers of Ontario drivers and that disclosure of the information would be an unjustified invasion of privacy.

The Assistant Commissioner considered the bulk requester policy and agreement.

One of the stated objectives of this authorization process is to enhance security and privacy protection through controls on the use of records containing sensitive information. If I were to accept the appellant's position and order the disclosure of this bulk data, the Ministry's security measures would be rendered meaningless. There would be nothing preventing an appellant from, for example, creating a new database and passing the personal information along to any number of users.…

The drivers licence number is essentially a key that may be used to access information beyond simply a driver's name. As the Ministry explains in its representations, the drivers licence database contains a great deal of sensitive personal information, including a listing of a driver's address, date of birth, sex, etc., much of which is accessible by anyone with access to a key identifier such as a driver's licence number. Disclosure of a list of all Ontario drivers and their licence numbers would provide the appellant with the means to access significant amounts of personal information, with no controls over potential use. (Order P-1144, Ministry of Transportation, March 13, 1996)

Is Information that has been Publicly Disclosed "Publicly Available" and Exempt from Protection?

We frequently receive arguments that once personal information has been made publicly available from one source, that personal information is subsequently free from restrictions in the hands of institutions other than the institution by which it was made publicly available.

Information available from Human Rights Board of Inquiry

We received a complaint that a school board had disclosed to the public the fact that the complainant had made a complaint to the Ontario Human Rights Commission. The school board claimed that the information about the human rights complaint fell within section 37, being "available to the general public." This was because there had been a Board of Inquiry under the *Ontario Human Rights Code*, and the hearing had been open to the public. The school board referred us to two newspaper articles containing the fact that the complainant had made a human rights complaint.

We said the following:

> It is our view that personal information maintained by an institution may be excluded from the application of the [privacy protections] of the *Act* only if the personal information is maintained by that institution for the purpose of creating a record which is available to the general public. Other institutions cannot claim the benefit of the exclusion for the same personal information, unless they too, maintain the personal information for that purpose.

We ruled that it was the Human Rights Board of Inquiry which maintained the records for the purpose of making it available to the general public, and not the school board, for the purposes of section 37. We also said that while the complainant may have disclosed to the press that he had filed a complaint, this did not render "public" the information that was later disclosed by the Board within the meaning of the section, because the Board was not maintaining this personal information specifically to make it available to the public. (I95-024M, January 31, 1996)

Information in Arbitration Decision

We made the same decision in another privacy complaint where the personal information in an arbitration decision was disclosed by one school board to another. The arbitration decisions were maintained by the Education Relations Commission in its library, and made available to the public. Summaries of the arbitration decisions were routinely made available to schools. We ruled that while section 37 applied to the use and disclosure of the decisions by the Education Relations Commission, the section exception to the privacy rules was not available to the two school boards, which did not maintain the records for the purpose of making them available to the general public. (I93-009M, August 11, 1993)

Therefore, the fact that personal information might fall within the "publicly available" exception to privacy protections for the institution which maintains the information for public access does not mean that the personal information loses its protection in the hands of another institution which does not maintain it for the purposes of public access. Where another institution holds the same information, it must adhere to the privacy rules under the *Act*.

Disclosure of Information to Politicians

Occasionally, politicians feel that they are entitled to access to their constituents' personal information in order to carry out their responsibilities. We received a complaint that three cities had provided incumbent councillors with access to information including the names and addresses of purchasers and vendors of residential properties within the cities, purchase prices, lot sizes, total prices, cash down, classes of properties, locations, lot and plan descriptions and parking data. The cities maintained a central property database and some councillors were provided with online access to the database.

The cities stated that the information in question was obtained primarily from Land Registry information, Assessment Roll information and building permit application information, all three of which were described as "public record of information."

We established during our investigation that the public did not get access in the manner in which it was made available to councillors. While a member of the public may attend at civic centres and look at assessment rolls or request the name of the owner of a property or building permit

application, this access is provided on a record-by-record basis. The cities did not provide direct public access to the complete database or hard copy record.

Therefore, although some of the cities' information may have been obtained from sources whose databases are made available to the public, we held that the cities could not claim the exclusion of s.37 because the cities themselves did not maintain this information as a public record.

In addressing the information needed by politicians in order to discharge constituency responsibilities, we said:

> In our view, Councillors do not need the information of all constituents in order to discharge their responsibility to help those who request assistance with respect to a particular building permit, planning or other similar matter. It is our view that section 32(d) [disclosure made to an officer or employee who needs the record in the performance of his or her duties] does not apply to the routine disclosure of or access to personal information of a large group of City residents where this disclosure does not directly relate to a particular land use or planning matter. We are also not persuaded that activities such as welcoming new residents to a ward are sufficiently connected to the City's service functions to fit within the scope of section 32(d).
>
> . . .
>
> We accept that Councillors should be able to respond to issues raised by constituents and to have access to information necessary to properly discharge their responsibilities. In circumstances where the personal information of a constituent is required in order to meet this need, it should only be disclosed to the Councillor in compliance with section 32 of the Act. This can be achieved, for example, under section 32(b), which permits the disclosure of personal information with the consent of the person to whom the information relates. (Investigation MC-980018-1, October 28, 1998)

Is the Information "Personal Information?"

"Personal information" is defined in our *Acts* as recorded information about an identifiable person. This definition has been interpreted to include only information about a natural person or individual, and largely to exclude information about a person in his or her business capacity.

> The use of the term 'individual' in the *Act* makes it clear that the protection provided with respect to the privacy of personal information relates only to natural persons. Had the legislature intended 'identifiable individual' to include a sole proprietorship, partnership, unincorporated association or corporation, it could and would have used the appropriate language to make this clear. The types of information enumerated under subsection 2(1)

of the *Act* as 'personal information' when read in their entirety, lend further support to my conclusion that the term 'personal information' relates only to natural persons. (Order 16)

However, business information may also be personal information. "It is, of course, possible that in some circumstances, information with respect to a business entity could be such that it only relates to an identifiable individual, that is, a natural person, and that information might qualify as that individual's personal information." (Order 113)

Building Permit Information

In Order M-197 (1993), a township received a request for building permit data including the names of persons who obtained permits, the property location and the type of construction. The record at issue was a list which contained "columns of information under the following headings: owner's name and property description, permit fee, type of structure and the estimated cost of the project. The property description consists of a legal description of the property referring to the parcel, lot and concession number within the Township." The Township granted partial access to the records responsive to the request but denied access to owners' names, property descriptions and permit fee information contained therein, relying upon section 14(1) of the municipal *Act*.

We held that where the owners are natural persons, their names would constitute personal information. We upheld the Township's decision to withhold the names of individual owners who were natural persons, but where the owner was a business entity, the name and address were not considered personal information.

Land Transfer and Mortgage Information

A request was made to the Ministry of Finance for access to copies of completed land transfer and mortgage forms all of which relate to specific properties. The forms were created pursuant to the *Land Registration Reform Act, 1984*. We held that the records contained personal information such as the name of the chargor, chargee, transferor and transferee of the properties.

However, the documents are available in their entirety to the public upon request at land registry offices. They were provided to the Ministry by an individual who indicated they were obtained as a result of a title search at the land registry office. As such, it could not be said that disclosure of the personal information contained in these documents would constitute an unjustified invasion of the personal privacy of the individuals referred to in these records. (Order P-480, Ministry of Finance, 1993)

Property Tax Information

Similarly, we have held that information about property tax liability is personal information. A requester sought access to a list of all properties whose municipal taxes are in arrears, as well as

the amounts owing, the term, the property owner, and any other information about arrears that would be recorded on title." Information responsive to the request included: registered owner of the property, property address, actual arrears and accounts receivable charges.

> Where a listing indicates that the property is owned by an individual or individuals, I find that the names, property addresses and associated entries for these listings qualify as personal information for the purposes of section 2(1) of the Act. Unlike other circumstances where the owner of a property may not be responsible for activities involving a property, municipal property taxes are the responsibility of the property owner, and if there are arrears it is always the owner whose name would appear on any arrears listing.
>
> Where a listing indicates that the owner of a property is a sole proprietorship, partnership, unincorporated associations or corporation and not a natural person, I find that the information contained in these listings does not qualify as personal information (Order M-800, 1996).

If Information is Publicly Available, is it Available as Bulk Data?

The manner and format of access to publicly available personal information is critical in determining whether privacy protections may be maintained for this information. In a 1997 appeal we noted that information about arrears of property taxes might be available by searching at the Registry Office. However, the Registry Office allows searches in relation to a particular property, whose address or legal description must be known to the searcher in advance.

> By contrast, access to the information in the context of the Townships' accounts would identify, potentially in a comprehensive way, all individuals and properties for which tax registrations were undertaken during the period covered by the accounts and in my view, disclosure in that context would…. constitute an unjustified invasion of privacy. (Order M-981, Townships of Belmont and Methuen, July 31, 1997)

Driver's Licence Information Bulk Access

The Ministry of Transportation received a request for bulk access to the names and driver's licence numbers of all Ontario drivers, found in the Ministry's driver license database. Assistant Commissioner Mitchinson decided that although the names of vehicle drivers and their licence numbers are individually available to the public under section 21(1)(c) (information available to the general public), a list of all names and numbers did not meet the requirements of this exception to the mandatory personal information exemption claim. For the bulk information to fit within this section, it would have to be routinely released **in the form requested**, which it was not, and the

Assistant Commissioner found that the bulk information was not "collected and maintained specifically for the purpose of creating a record available to the general public." (Order P-1144, supra, Ministry of Transportation)

Land Registry Information Bulk Access

The issue of bulk access to land registry records arose in a 1999 complaint. A complainant was of the view that information from Ontario's land registration database was being sold in bulk to commercial mortgage lenders. The information included the mortgage renewal dates of property owners. The Ministry of Consumer and Commercial Relations operates 55 Land Registry Offices in Ontario, the main functions of which are to register, store and preserve documents, deeds, mortgages and plans of survey. The records are maintained in an automated land registration database. The mortgage renewal dates can be found in a document that includes the names of both the borrower and the lender, the amount of the mortgage, the interest rate, the monthly payment and the date on which the mortgage matures.

Any individual or other entity can, upon payment of the prescribed fees, examine both the abstract indices, which summarize registrations pertaining to a particular property, and the individual registered documents. The individual registered documents are available in either a paper format, on microfilm, and/or electronically within the automated databases. Each microfilmed record is a compilation of a number of individually registered documents. Before a microfilm relating to a particular property can be located, specific information must be provided by the individual conducting the search, such as a unique property identifier, owner's name, street address and individual instrument number and all information is available on a record-by-record basis. The same applies to electronic access and it is not possible to obtain a listing of all mortgages or any document type registered in a particular area.

The Ministry indicated that it was aware of lending institutions that employ individuals who compile data from the land registry records. Those individuals, like all other members of the public, obtain data on a record-by-record basis. We found that the Ministry had not disclosed the personal information in question in bulk to any lending institution.

We agreed that the *Registry Act*, the *Land Titles Act*, and the *Land Registration Act* provide the statutory authority for the collection and disclosure of the information, and that the Ministry had a duty the make land registration records available to the public. The legislation places no restrictions on who may have access to the information or in what manner. We therefore found that the records were maintained specifically for the purpose of creating a record available to the general public.

We became aware of other disclosures of its records by the Ministry during the course of our investigation, and decided to address them in our Investigation Report. The Ministry stated that

it made microfilmed records available to two municipalities and two real estate boards. The Ministry also advised that, "for the purposes of verifying property assessments", the microfilmed documents are also provided to the Ontario Property Assessment Corporation. The Real Estate Boards use the information to assist property assessors in determining property values based upon recent sales. The municipalities used the information to update property assessment records.

The Ministry had not entered into written agreements controlling the subsequent use, disclosure, retention and destruction of the information with the boards or municipalities. The arrangements had been made some time ago in response to individual requests, but the practice was being discontinued due to resource constraints. Because of the discontinuance, we made no finding as to the disclosure, but we indicated our concern as to the lack of controls in place to regulate the handling of the personal information. We made a recommendation that the Ministry give notice of discontinuance to the municipalities and real estate boards and that it take steps to ensure that the boards and municipalities protect the microfilmed records, so that controls are put in place concerning subsequent use, disclosure, security and disposal of the records.

The Ministry planned to continue its disclosures to the Ontario Property Assessment Corporation. We said that the individual land registration is considered to be "maintained for the purpose of creating a record that is available to the general public" because these records meet certain criteria of public availability, such as:

- the Land Registry personnel have a statutory duty to make this information available to the public;
- at Land Registry Offices there is a regularized system of access to the information on a record-by-record basis; and
- at Land Registry Offices, a standardized fee is charged to all persons seeking access.

Since the information in question is available only one record at a time, there is also a practical limit to the ability of recipients to obtain and possibly abuse the personal information in the documents.

In its original submissions the Ministry explained that "all information contained in the land registration documents, plans and records is available for review on a record-by-record basis." Therefore, it does not appear that "bulk" access is provided to users of the information.

We held that the bulk disclosure of the personal information in the microfilms to the Corporation does not conform to the criteria set out above. The Land Registry personnel do not appear to have a statutory duty to make the microfilms available in bulk to the public, nor does there appear to be a regularized system of bulk access to the microfilms. Accordingly, we found that the personal information contained in the microfilmed records, which are being disclosed in bulk to the Corporation, was not maintained for the purposes of creating a record that is available to the general

public. Therefore, the Ministry could not claim the exclusion in section 37 of the *Act* in making bulk access available to the Corporation. (Investigation PC-980049-1, Ministry of Consumer and Commercial Relations, June 22, 1999)

Police Arrest Records Bulk Access

The issue of bulk access also arose in an appeal involving access to police arrest media reports. A reporter requested access from Metro Toronto Police Services Board to "major news reports, arrests" in computer format. The appellant wanted copies of all records since the Police began storing these documents on a word processing system, estimated by him to be in 1994 or 1995.

The Arrest Sheets contained the name and address of the person who has been charged, the charges, and a description of the facts leading to the arrest. The names of any young offenders were not included, and complainants were generally not identified. We held that the Arrest Sheets contained the personal information of the individuals who have been charged.

The appellant argued that the Police release paper versions of the Arrest Sheets on a daily basis to various news media outlets. In his view, the Police have created records available to the general public, and he was simply asking for a computerized version of these records.

The Police stated that the records were created for internal information purposes, and were made available at Police Headquarters for the media and the public, upon request. The Police argued that any media or public access was secondary to the specific reasons why the records were created. Assistant Commissioner Mitchinson held that the records were not maintained **specifically** for the purpose of creating a record available to the general public. The secondary use of making them available to the public does not satisfy the requirements of section 21(1)(c) exception from the prohibition against disclosure. "It is clear that the names, addresses and other identifying information about an arrested person were collected for the purpose of prosecuting a crime, not for the purpose of creating Arrest Sheets and making them available to the general public. Although these records may be released to the public on occasion, in my view, this is a secondary use which does not satisfy the requirements."

The Assistant Commissioner said that the appeal turned on the question of whether personal information, which is disclosed by the Police on an individual basis in paper format, changes in nature when disclosed in bulk in computerized format.

> Arrest Sheets differ in content but not in type. Paper versions are produced on a daily basis and disclosed by the Police without the need for a formal request under the Act or the need to consider and apply any exemption claims. The Compliance Department of this office has determined that individuals charged with criminal offences can reasonably expect that personal information concerning these charges would be disclosed by police organizations to the community, and that the purpose of this type of routine disclosure is

consistent with the original purpose of obtaining and compiling this personal information (section 32(c) of the Act). (See for example, Investigation I96-018P.)

In this case, the records were computerized. The appellant pointed out the difficulties of using the paper versions: it was virtually impossible to search for information in paper records, spot trends or conduct any analysis. The computer excelled in records management and sorting capabilities.

However, the Assistant Commissioner was not sympathetic to those concerns. He was of the view that computerized access would unacceptably limit restrictions on use:

> If the appellant is provided with an electronic version of the Arrest Sheets, the restrictions on usage will disappear. He will be able to develop a computer database of records, where various fields of data, including those containing personal information, can be easily searched, sorted, matched and manipulated for a wide variety of purposes. Although section 32(c) of the Act permits disclosure of this personal information at the time of the arrest, in my view, it is not reasonable to conclude that the individuals identified on the Arrest Sheets could have expected that this same personal information would similarly be distributed in bulk and in computerized format. Therefore, I find that section 32(c) does not extend to the disclosure of the electronic version of the Arrest Sheets.

He referred to Order M-68 in which he found that the fact that information about criminal convictions was available to the public from the courts did not mean that that information would be freely and routinely available to anyone who asked for it. "Similarly in this appeal, although the appellant may have already been provided with a paper version of the Arrest Sheets he is seeking in electronic format, in my view, this does not mean that an easily retrievable computerized record of all Arrest Sheets should be disclosed." He cited a decision of the U.S. Supreme Court, *Whalen v. Roe* 97 S.Ct 869 at page 872 where the Court stated:

> In sum, the fact that 'an event is not wholly private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information.

Having considered the sensitivity of an arrest record, and the degree of publicity, he found that a disclosure of computerized version of the Arrest Sheets would be an unjustified invasion of privacy.

In a postscript, Assistant Commissioner Mitchinson addressed the question of the police intention to place all arrest records on the Internet, an issue that had been raised by the appellant. The police confirmed this intention. The Assistant Commissioner was concerned that this type of disclosure could circumvent the requirements of the *Act*:

> If the Arrest Sheets are put on the Police's Internet website, the appellant and others will be able to download these records for storage on a computerized database. The information

contained on the records, including the personal information which I have found qualifies for exemption in this order, could then be used in the same manner as if the records were provided directly by the Police in electronic format. The fact that the records are only on the website for a specified period is irrelevant as far as electronic access to the information on the Arrest Sheets is concerned.

Because of the privacy concerns associated with Internet access, our office would discuss the matter with the police. (Order M-849, Metropolitan Police Services Board, October 16, 1996)

Professional Information about Physicians

In another case involving bulk access to personal information, a request was made to the Ministry of Health for access to information from the database of the College of Physicians and Surgeons of Ontario regarding all members of the College, including name, address, telephone, year of qualification, specialty and status. The College is not an institution under the *Act*.

There was a statutory requirement for the College to make the information available to the public, and to provide a copy. However, there was no requirement for the **Ministry** to make the information available to the public, and it held the information for a different purpose. The Assistant Commissioner said that there was an important distinction between "one-off" or limited group requests and request for bulk data. The approximately 30,000 physicians listed clearly brought the scope of the request within the category of bulk access, and bulk access raises unique privacy considerations. A consideration in this case was the absence of choice for physicians on whether to be listed the database. Mr. Mitchinson said, "the absence of choice would have weighed against, rather than in favour of, a finding of implied consent.... Consent implies choice...."

Personal information changes its character where it is disclosed in bulk rather than on a one-off basis. The purpose of making the register available to make information about a particular physician available to the public to facilitate informed decision-making about medical care. Access to the entire database is not necessary for that purpose, and would not have been reasonably expected by the physicians.

The Assistant Commissioner agreed that the *Health Professions Procedure Code* did not contemplate bulk access, which, if provided in electronic format would provide the means to access significant amounts of personal information with no controls over potential use. It would enable a requester to develop a computer database of records that could be easily searched, sorted, matched and manipulated for a wide variety of purposes. Scanning technology extended this reasoning to hard copy bulk access as well.

The example of information the disclosure of which could harm those who work in abortion clinics illustrated how information which would arguably be non-controversial on a one-off basis can be

characterized as highly sensitive in bulk format, particularly when disclosure is not restricted to a specific requester but is disclosure "to the world." This factor alone would outweigh any factors favouring disclosure. The Assistant Commissioner held that the bulk disclosure would be an unjustified invasion of privacy. (Order P-1635, Ministry of Health, December 30, 1998)

Can Ontario's *Acts* be Improved with Respect to Publicly Available Information?

The provisions creating distinctions for publicly available personal information under the *Acts* are not particularly detailed, and are capable of expansive interpretation, providing little or no privacy protection for the personal information. In 1994, the Standing Committee on the Legislature of the Ontario Legislative Assembly conducted a statutory review of the *Municipal Freedom of Information and Protection of Privacy Act*. The IPC made submissions to the Standing Committee recommending amendments that would strengthen the privacy requirements.

One of our recommendations was that Part II of the *Act* be amended to specify privacy protection provisions for public registers. We said that the balance of protection and the legitimate "right to know" was a key consideration. We pointed to the New Zealand Public Register Privacy Principles, (see below) as an example of a regime which could further privacy principles without diminishing access rights.

We also recommended an amendment to address personal information that could be used for mailing lists, suggesting that it be made a specific exemption — the issue of mailing lists is specifically addressed in the privacy legislation of British Columbia and Nova Scotia. A third recommendation was for a requirement that the Commissioner be consulted prior to data matching exercises involving personal information.

Our recommendations have not been enacted so far.

Public Information Challenges in Other Jurisdictions

Other jurisdictions in Canada and elsewhere face many of the same challenges with respect to publicly available personal information, in endeavouring to give effect to the public policy purposes for which personal information is made publicly available, while providing some measure of control over subsequent disclosure and use of the information.

The Canadian federal *Privacy Act* does not apply to personal information that is publicly available (s. 69(2)). The federal *Access to Information Act* does not apply to published, library or archival material (s. 68) and an institution may disclose any requested record if the personal information is publicly available. (s.19(2)(b)). The latter provision has been interpreted to prohibit further disclosure of a military offence record, which had inadvertently been disclosed to the press. The court held that the publicly available provision was not applicable since not all of the information was disclosed and the disclosure was inadvertent. (*Erwin Terry M.D. v. the Minister of National Defence* File # T-845-94, Federal Court, 1994)

The issue of access to driver's licence information is one that is a significant concern in many jurisdictions. Driver's licence information can include highly specific identifying information such as name, home address, date of birth, personal identification number, sex, height/weight/ eye colour, vision correction, physical handicap/medical condition, photograph, organ donor status. (*Public Registers and Privacy: Conflicts with Other Values and Interests*, Robert Gellman, 21st International Conference on Privacy, Hong Kong, September 13, 1999)

The United States federal *Driver's Privacy Protection Act* was passed by Congress in 1994, in order to balance issues of access and privacy regarding this kind of information. Because regulation of motor vehicles and driving is a state rather than a federal matter, the law was challenged, but was upheld on a division of powers basis by the U. S. Supreme Court this year.

Under the Act, state motor vehicle licensing offices are prohibited from disclosing identifiable records for marketing or in response to individual requests, unless the data subject previously had the opportunity to opt out of such disclosure. The Act also provides specifically for other disclosures, both mandatory and discretionary. Mandatory disclosures include programs for driver safety and theft; emission control; recall; performance monitoring of vehicles; and other federally required vehicle regulatory activities.

The states have the power to make twelve discretionary types of disclosures, including to government agencies; to verify information submitted to a business; to prevent fraud; to pursue legal remedies; to collect debts; for use in judicial proceedings; for use by insurers; to provide notice to owners of towed cars; for use by private toll roads and with data subject consent.

As noted by Mr. Gellman, "what the federal law illustrates is how a public register compiled for one purpose can develop a wide range of users whose purpose sometimes bears little relationship to the purpose of the register."

In British Columbia, the City of Victoria made assessment information available on its website. Many people complained about the disclosure, and the City removed the material from the site. David Flaherty, the former B.C. Information and Privacy Commissioner issued Investigation Report P98-011, where he made the following recommendations:

- The public should only be able to search real property registries, whether in paper or electronic format, by the address of the property.
- Registry users should be clearly informed of the legitimate purposes for which property registries may be inspected, including prohibitions and limitations on unrelated uses, such as the compilation of mailing lists.
- In the case of bulk sales of property registry data, whether in electronic, microfiche or hard copy format the name of the property owner should be suppressed.
- Where an individual has reasonable grounds to believe that disclosure of their personal information would jeopardize their safety, or that of their family, and they provide an alternate mailing address, B.C. Assessment should amend the Assessment Roll to make this substitution.

The Quebec public sector privacy act (*An Act respecting Access to documents held by public bodies and the Protection of personal information*) states specifically that rights under the Act do not apply to information in certain public registers, namely those with respect to land transactions, civil status and matrimonial regimes.

In June 1997, Quebec Information and Privacy Commissioner Paul-Andre Comeau issued a paper entitled *Privacy and Openness in the Administration at the End of the 20th Century*. The Commissioner was concerned about the use of personal information that has been designated as having a public nature. This information, when held in electronic form, may be used for a purpose different from its original purpose. For example, to avoid election fraud, certain information is deemed to be public. The transmission of whole databases to requesters has given rise to a number of cases, which "clearly show the difficulty of respecting the purpose of the legislator's decision to confer a public character to personal information when a request for access involves a complete data base." The wholesale access to this information could make Quebec "a true paradise of direct marketing." The Commissioner recommended a legislative amendment to restrict the circulation of personal information of a public nature.

Recently, the Government of Quebec proposed amendments to both the public and private sector privacy acts in that province (Bill 122). An amendment to the act concerning the private sector requires that a person using technology must take particular care that the confidentiality of personal information is preserved. The amendments also provide that an enterprise may "without the consent of the person concerned, communicate any information which by law is public information." A third amendment establishes an offence where a person establishes a file on another individual or collects personal information without having developed and applied sufficient security measures to protect the information.

A key change to the public sector privacy act extends coverage to the learned professions that are governed by the Interprofessional Council. Disclosures by one government institution to another for the purpose of data matching require the prior authorization of the Privacy Commissioner. The amendments specifically delineate the personal information about professionals that will be publicly available, but provides that a request for access to the publicly available information must be on a record-by-record basis, and the requester must specify the name of the person concerned. Public consultations on Bill 122 are now underway and public hearings will be conducted by a committee of the Legislature in September.

New Zealand has made specific provision for public registers through its *Public Register Privacy Principles, Privacy of Information Act*, Part VI A, section 58(B). Public Registers are maintained under particular laws in respect of which there is an explicit right of inspection and access. The principles relating to public registers are as follows:

> Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organized.
>
> Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.
>
> Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.
>
> Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.

These Privacy Principles have been admired in many jurisdictions, including our own. However, the Privacy Commissioner of New Zealand, Mr. Bruce Slane, has expressed concern that the availability of technology is driving changes in public record keeping and access without the social impacts, particularly the privacy impacts, being studied first. The Privacy Commissioner has recommended that:

- the public register privacy principles be reformed so that, as far as possible, access to public registers is made consistent with the finality principle;
- bulk release of personal information electronically from public registers be constrained;
- any decision to place public registers on the Internet be taken by Parliament rather than administratively;
- privacy impact assessments be undertaken for major technological projects.

(27th Meeting of the International Working Group on Data Protection in Telecommunications Greece, 4/5 May 2000, New Zealand Report)

Personal Information and the Private Sector

A recent development in Canada is the enactment of legislation that protects the privacy of personal information that is held by entities in the private sector. Until this year, Quebec was the only jurisdiction in North America to enact legislation specifically to regulate the handling of information by the private sector.

On April 4, 2000, the Parliament of Canada passed the *Personal Information Protection and Electronic Documents Act* (Bill C-6). The Act will come into force for federally regulated organizations in January 2001, and will take effect in January 2004 in those provinces that have not enacted substantially similar legislation. The Act regulates the collection, use, disclosure, retention and security of personal information in the hands of private sector organizations, and used in the course of commercial activities. It provides for an independent oversight body in the Privacy Commissioner of Canada, who may delegate investigations and other functions to privacy commissioners in the provinces.

The Act incorporates ten Principles of the Privacy Code developed by the Canadian Standards Association (the CSA Code). The Principles are for Accountability, Identifying Purposes, Consent, Limiting Collection, Limiting Use, Disclosure and Retention, Accuracy, Safeguards, Openness, Individual Access and Challenging Compliance.

The Act requires that the knowledge and consent of the individual as a prerequisite to the collection, use and disclosure of personal information, except in certain circumstances, set out in section 7. One of the exceptions from the requirement of knowledge and consent is where the information is publicly available **and is specified in the regulations**. (s.7(1)(d), 7(2)(c.1),7(3)(h.1 and 7(4)). Provision is made for regulations "specifying information or classes of information for the purposes of paragraph 7(1)(d), (2)(c.1) or (3)(h.1)."

The Department of Industry of Canada, which has responsibility for the Act, is in the process of drafting a regulation that will specify the information or classes of information to be designated as publicly available. It intends to publish a draft regulation, for comment, some time in late September. As part of the preparation of the draft regulation, the Department has released a draft checklist of considerations for use in determining whether information should be publicly available. It is intended to publish this checklist of criteria in the Regulatory Impact Analysis Statement, with the draft regulation.

1. What information or source of information is the subject of the proposal?

2. Is there a statutory basis for the collection of this personal information? Is provision of the information mandatory? Is disclosure by the institution mandatory or discretionary? [Only mandatory disclosures will be eligible for consideration in the regulations].

3. What is the primary purpose of making the information "publicly available?" Is it to support a commercial activity that is recognized as legitimate on public policy grounds? Does the public access requirement relate to a strictly non-commercial purpose, e.g., to allow a homeowner to compare the taxes on his property with those of his neighbour? [In the latter case, the law would not apply to restrict the disclosure].

4. In what sense is it publicly available? How is the information accessed? Is it available to anyone? Is there a fee? It is available in bulk or by specific information item? Is it only available for inspection or can copies be made?

5. What personal data elements are present? What are the reasonable expectations of those whose personal information is included? [Suggested by BC Civil Liberties].

6. Does the source collection include only the information required for the fulfillment of the purposes for which it was collected? Or is there more? If so, what?

7. What personal data elements does the stakeholder want to exempt from the consent requirement?

8. What is the business use, value and impact on the stakeholder of this information? Are there substitutes available? Is it possible to obtain consent?

9. Do individuals have an opportunity to opt out of having their personal information made publicly available for commercial purposes which have nothing to do with the primary purpose of collection (either when the primary collection occurs or as a service offered by the organization which is collecting the publicly available information)?

The Department notes that while the requirements of knowledge and consent will not be applied to publicly available information, the other requirements such as delineation of purpose and limitation on collection will still apply to this information. In its preliminary consultations, the Department indicated that it is considering four categories of information: directories (such as telephone directories), publicly available databases or registries, court records, and published information.

The criteria, set out above, while helpful in the discussion of which personal information may become personal information, do not answer the fundamental question of whether publicly available information will still be subject to subsequent controls on use and disclosure without consent. A key factor for the Department is whether there is an opportunity for the individual to know about any secondary use of the information:

> Certain personal information, be it in directories, data bases, court records or the media, is generally available to the public for a specific primary purpose e.g., to enable individuals to contact one another, or verify title or membership qualifications, for transparency and accountability in the public sector, or to advertise or publicize specific events of information. We think that commercial organizations should be able to use personal information without consent for the primary purpose for which it has been made publicly available. Secondary and unrelated commercial purposes are a separate issue. A consent requirement for secondary uses of publicly available personal information strikes the right balance between the individual's right of privacy and the legitimate business need for the information.

We await the publication of the draft regulation with interest and will likely be providing submissions to the Department.

Another welcome development was the release this summer of a discussion paper by the Ontario Ministry of Consumer and Commercial Relations on a contemplated act to regulate privacy in the private sector in Ontario. Unlike the federal Act discussed above, the Ontario proposal would cover the non-commercial activities of organizations as well as the commercial, and would include hospitals, universities, non-profit organizations as well as businesses. Like the federal Act, it would incorporate most of the Principles of the CSA Code. The paper proposes oversight by a single oversight body with expertise in the area of privacy and information. It is not yet known how the proposed Act would deal with publicly available information. The Government of Ontario is conducting public consultations in during August and early September, and intimates that it contemplates the early passage of legislation. The IPC will be making submissions to the government on the discussion paper, and our submissions will be available on our website. Similar moves to initiate regulation of privacy in the private sector are currently taking place in other provinces.

All of this legislative activity will have a significant impact on the handling of personal information by private sector organizations. The provision of enforcement and oversight will ensure that the entity collecting or holding the personal information will no longer be the sole arbiter of whether its dealing with the information is proper in the circumstances, and individuals will have a forum for obtaining a remedy. Principles and guidelines for the handling of information will ensure new standards of privacy protection, and it is to be hoped, a new appreciation of the value of privacy in both individuals and organizations.

Conclusion

This review of issues arising in publicly available information demonstrates the complexity of the questions to be determined in any particular case.

While we struggle to develop strategies for privacy protection, the quirks of individual personal information collections that are publicly available confront us. We may advocate that personal information should only be disclosed and used for the primary purpose for which it is made publicly available. But in some cases, it is difficult to determine with any degree of specificity the precise primary purpose for the availability. Some disclosure practices have grown over time, with the initial reasons for the original disclosure becoming quite murky. A good example is driver's licence information — initially it was collected by the authorities to enable the regulation of motor vehicle matters. It has since become a major item used for verification of identity by businesses that have nothing to do with motor vehicles, such as credit reporting agencies and private investigators.

A key consideration is whether there is an opportunity for the individual to opt out of secondary uses. However, opt out mechanisms must be real, in the sense of being brought to the attention of and easily availed of by the individual — small print negative optioning is not sufficient to give a true indication of consent.

Many enactments providing for exceptions from privacy rules for publicly available information are quite bare bones in their wording. Often, they simply state that an act does not apply to, or certain provisions do not apply to such information. As in the Ontario provisions, there is no requirement of statutory authority for the public disclosure; the public policy purpose for disclosure is absent; there is no guidance as to whether access is to be record-by-record or on a bulk basis; and no requirement for any ability to opt out in regard to secondary uses. There may be inconsistencies in the statutes creating the public registers, but no overriding privacy statute that prevails in the face of an inconsistency.

These deficiencies in statutory privacy protection regimes may be addressed through legislative amendments, which, because of the increasing computerization of personal information holdings and the increasing commercial value of personal information, are becoming more urgent.

In his thoughtful paper entitled *Five Strategies for Addressing Public Register Privacy Problems*, Blair Stewart, Assistant Privacy Commissioner, New Zealand (21st International Conference on Privacy, Hong Kong, September 13, 1999) offers the following suggestions:

1. Let general data protection laws solve the problems.

2. Apply data protection laws in a limited fashion.

3. Tailor the laws establishing registers to address privacy issues.

4. Look beyond the register to users of register information.

5. Supplement date protection laws with special rules on public registers.

He recommends that all five strategies be used in combination. With respect to the first strategy, he notes that in the United Kingdom public registers must adhere to the registration requirement. He suggests that public registers could be required to be maintained consistently with normal data protection principles, identifying the purposes and ensuring that the information is used for those purposes alone.

Many data protection laws already apply data protection principles in a more limited fashion to publicly available information, so that there is only a partial exemption from privacy rules. For example, correction rights might be maintained. (This is the approach we have taken in Ontario. As I stated earlier, the IPC has interpreted the publicly available information provisions to limit the exceptions to the privacy rules to those institutions which maintain the registers for the purpose of making the information publicly available, and even those institutions may be constrained in making bulk disclosures.)

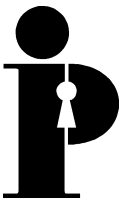
Laws establishing specific registers could be reviewed and amended so as to provide appropriate access and privacy rules. The community could be consulted on this process, and the experience from complaints relating to the registers could be utilized to determine what should be done in response. Technological issues should be reviewed at the same time. Mr. Stewart recognizes that this strategy is a long-term solution, with significant resource implications, but could be used when drafting new and amended legislation.

Strategy Four is to regulate the activities of those who use the information from the registers. With the implementation of the new private sector legislation in Canada, the activities of private sector organizations in collecting, using and disclosing personal information will be subject to regulation, even when they collect publicly available information. Industry Canada has indicated that it takes the position that disclosure is to be used only for the primary purpose, and secondary use will require the consent of the individual.

Strategy Five is to make special laws on public registers. He points to the examples of such rules in Australia, New Zealand, Hong Kong and new South Wales.

I agree with Mr. Stewart that public register issues are difficult, but not impossible to address. As our experience with these issues grows, strategies and solutions emerge, and as the privacy concerns of the public become more urgently known to their governments, I am hopeful that governments will respond.

In the end, it is important to balance the legitimate needs for public access to personal information with the equally important right of privacy. Personally identifiable data has become an extremely valuable commodity. Given that knowledge is power, modern data mining techniques can transform a basic collection of discrete facts about a person into a highly advanced psychographic profile of one's background, finances, purchasing habits and lifestyle. Data protection authorities must remain vigilant and prohibit inappropriate uses of personal information. Equally, organizations seeking to use personally identifiable information must show respect for the individuals to whom the data belong and seek their consent for its use, in the absence of clear legislative authority. Even when a use is permitted by law, independent oversight must be applied to ensure that the use does not stray from its primary purpose. Such data protection measures are vitally important to maintain the privacy rights of individuals.



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