Information
and Privacy
Commissioner/
Ontario

Privacy Guidelines for Municipalities Regulating Businesses Dealing in Second-hand Goods

Ann Cavoukian, Ph.D.
Commissioner
September 2007

The Commissioner gratefully acknowledges the work of the Policy and Legal Departments in the preparation of this paper. Only through their efforts and dedication is such outstanding work possible.

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

This publication is also available on the IPC website.

Table of Contents

I. Introduction

In Ontario, personal information is protected under three statutes: the *Freedom of Information and Protection of Privacy Act* (*FIPPA*),[1] the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA),*[2] and the *Personal Health Information Protection Act*.[3] The Office of the Information and Privacy Commissioner of Ontario oversees all three pieces of legislation which are premised on widely accepted fair information practices such as those found in the Global Privacy Standard (Appendix A).

Under these statutes, the Office of the Information and Privacy Commissioner of Ontario has a mandate to offer comment on the privacy protection implications of proposed programs, conduct public education programs, and provide information concerning Ontario privacy legislation. Municipalities and municipal police services are "institutions" governed by *MFIPPA.*

Over the years, some municipalities have attempted to build on and expand a scheme for the collection of personal information authorized under the *Pawnbrokers Act*[4] by enacting local by-laws requiring second-hand goods shops to collect, retain, and disclose information on second-hand goods transactions. Generally, pawnbrokers and second-hand goods shops ('businesses') collect and keep the personal information on site, where it is available for inspection. A number of municipalities allow businesses to maintain paper-based documents. Some municipalities, however, are taking steps to computerize this flow of personal information. In some settings, businesses are encouraged or required to routinely transmit this information to the police, using particular systems and software. While record-keeping software and internet capability may assist in the standardization of information collected on goods and sellers, it also facilitates the automatic and routine transmission and disclosure of sellers' information.

Some by-laws relating to the licensing of businesses will not be valid after the Ontario Court of Appeal decision rendered in *Cash Converters Canada Inc. v. Oshawa (City)* ('*Cash Converters*') which declared a municipal by-law of "no effect" on the basis that it conflicted with *MFIPPA*.[5] Such by-laws are enacted pursuant to a municipality's authority to license businesses under the *Municipal Act*.[6] This authority is confined to the accomplishment of listed purposes that include consumer protection. Law enforcement is not a listed purpose for which a municipality may pass a by-law, while consumer protection remains such a purpose. In light of *Cash Converters*, municipalities must determine whether the provisions in their by-laws related to the collection and disclosure of personal information are still valid.[7]

In accordance with the mandate of her office, Commissioner Ann Cavoukian, prepared these *Guidelines* to provide Ontario municipalities with a framework to meet the privacy requirements under *MFIPPA.*

1 *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31.

2 *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M. 55. **[*MFIPPA*]**

3 *Personal Health Information Protection Act*, S.O. 2004, c.3, Schedule A.

4 *Pawnbrokers Act*, R.S.O. 1990, c. P.6. Under the more than 100 year old *Pawnbrokers Act*, pawnbrokers have a statutory obligation as part of their financial transactions, to collect, record, and disclose specific personal information about individuals who bring goods to their businesses.

5 *Cash Converters Canada Inc. v. Oshawa (City)* [2007] O.J. No. 2613 **[*Cash Converters*]**.

6 *Municipal Act*, S.O. 2001, c. 25.

7 And see IPC Order MO-2225. Some pawnbrokers and second-hand goods shops may be licensed under separate municipal by-laws or under the same set of rules. In regard to pawnbrokers, some of those by-laws may *exceed* the requirements of the *Pawnbrokers Act*. Municipalities that license pawnbrokers or second-hand goods shops must comply with and not exceed the *Municipal Act, 2001*, the *Pawnbrokers Act*, and *MFIPPA*. These *Guidelines* are not intended to preclude the enforcement of the *Pawnbrokers Act* itself. Nonetheless, institutions are advised to consider and employ the privacy protective principles herein in implementing that *Act*.

II. The public policy underlying Ontario's privacy laws

The Williams Commission Report, which led to the passing of *FIPPA* in 1987 and *MFIPPA* in 1989, concluded that privacy protection should "attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives."[8] The Ontario Court of Appeal in *Cash Converters* stated:[9]

> The Williams Commission identified three specific concerns respecting government data banks: (1) where government collects personal information, the individual is unlikely to have an effective choice to refuse to supply the information; (2) because its activity is so broad, government holds very extensive personal information about individuals; (3) there is public anxiety about government agencies sharing their holdings of personal information and building comprehensive personal files on individuals (*Public Government for Private People: The Report of the Commission on Freedom of Information and Protection of Individual Privacy/1980*, Vol. 3 (Toronto: Queen's Printer, 1980) at pp. 504-505). The commission concluded that
>
> > a privacy protection policy intended to preserve informational privacy would therefore attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives and would attempt to maximize the control that individuals are able to exert over subsequent use and dissemination of information surrendered to institutional records keepers (at p. 667).
>
> This approach underlies the three standards for the collection of personal information that are set out in s. 28(2) of *MFIPPA*: the collection must be either expressly authorized by statute, used for the purposes of law enforcement, or necessary to the proper administration of a lawfully authorized activity.

To demonstrate necessity, governments and institutions should be prepared to show that the objective to be served by a data-gathering law is sufficiently important to warrant collecting sellers' personal information. The law should exclude trivial objectives or those discordant with the principles of a free and democratic society. For example, the objective of the law should relate to societal concerns which are pressing and substantial. Institutions should be able to show that the collection of personal information is reasonable and demonstrably justified. This justification should be evidence-based, showing the existence of a serious problem in the specific area that will be effectively addressed by the proposed scheme. For this, the law must be fair and not arbitrary, and carefully designed to achieve the objective in question -- the means chosen must be rationally connected to that objective. In addition, the means should impair privacy rights as little as possible. Lastly, there must be proportionality between the effects of the data-gathering law on privacy and the objective. For example, the more severe the effects of the law on privacy, the more important the objective of the law must be.[10]

8 *Public Government for Private People: The Report of the Commission on Freedom of Information and Protection of Individual Privacy/1980*, Vol. 3 (Toronto: Queen's Printer, 1980) at p. 667.
9 *Cash Converters, supra* note 5 at 30-31.
10 *R. v. Oakes*, [1986] 1 S.C.R. 103.

The question of whether or not the collection of personal information is "required" to regulate the sale of second-hand goods arises in the Ontario Court of Appeal *Cash Converters* decision. The decision supports a significant privacy principle known as "data minimization," meaning, the collection of personal information should be kept to a strict minimum. This principle, implied in various sets of fair information practices, has been well expressed in the Global Privacy Standard. The Information and Privacy Commissioner of Ontario was instrumental in harmonizing various sets of fair information practices[11] into a single Global Privacy Standard so that businesses and technology companies could turn to a single instrument for evaluating whether their business practices or information systems are actually privacy enhancing in nature and substance (Appendix A).[12]

Second-hand goods by-laws that **do not** provide for the collection and automatic disclosure of personal information by businesses **do not** attract privacy concerns.

11 Some of the standards that became the GPS include the standards by the Canadian Standards Association and Organisation for Economic Co-operation and Development, the latter of which were released in 1980.

12 The standard was tabled in November 2006 at the 28th International Data Protection Commissioners Conference in the United Kingdom, and is the first privacy standard to include the principle of data minimization.

III. Is the collection of personal information justified?

The intent of *MFIPPA* is to ensure that the collection and retention of personal information is strictly controlled and justified.[13] Second-hand goods by-laws that require the amassing of a large amount of detailed personal information into an electronic database, and transmission of this information to the police on a routine basis, without a warrant or judicial oversight, raise serious privacy concerns.

Pursuant to section 28(2) of *MFIPPA*, no person shall collect personal information on behalf of an institution unless three conditions are met:

1) the collection is expressly authorized by statute,

2) used for the purposes of law enforcement, or

3) necessary to the proper administration of a lawfully authorized activity.

Collections which do not meet one of the three conditions set out in s. 28(2) of *MFIPPA* are unlawful. Institutions bear the onus of justifying the collection of personal information. The principle that collection should be necessary to meet legitimate social objectives underlies all three s. 28(2) conditions. Note that consent is not one of the three conditions set out in s. 28(2) that allows the collection of personal information by or on behalf of a municipality and cannot be substituted for those conditions.[14]

Institutions contravening *MFIPPA* in relation to the collection of personal information can be subject to a Commissioner order to cease collection practices and to destroy collections of personal information.[15]

Municipalities may hold the following beliefs:

1) The belief that the collection of personal information about second-hand goods sellers is authorized by the *Municipal Act*. It is important to note that in relation to the 'expressly authorized by statute' condition, the Ontario Court of Appeal in *Cash Converters Canada Inc. v. Oshawa (City)* held that the *Municipal Act* does not contain specific authorizations to collect personal information and therefore this *Act* does not meet the 'expressly authorized by statute' condition. In this regard, the Court was clear that, without a specific statutory authorization,[16] a municipality cannot authorize the collection of personal information by merely enacting a by-law: "The structure of the *Act* [MFIPPA] indicates that it was not the intention of the legislature to allow municipalities, simply by virtue of their power to enact by-laws, to determine the type of personal information that can be collected."[17]

13 *Cash Converters, supra* note 5 at 51.
14 *Cash Converters, supra* note 5 at 34.
15 *MFIPPA, supra* note 2 at s. 46(b).
16 In *Cash Converters*, the Court referred to the *Pawnbrokers Act* as an example of a statute that does expressly authorizes the collection of personal information.
17 *Cash Converters, supra* note 5 at 37.

In addition, even under the authority of a statute, municipalities should "attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives."[18]

2) The belief that the second-hand goods sellers' personal information will be used for law enforcement purposes and its collection is therefore authorized under *MFIPPA*. To the extent that a municipality seeks to rely on the second condition in requiring the routine collection of personal information under a licensing by-law, it must do so within the scope of its law enforcement powers. As indicated above, a municipality's authority to regulate businesses is confined to the accomplishment of purposes listed under the *Municipal Act*. Law enforcement is not a listed purpose for which a municipality may pass a by-law. Although some of the information collected may ultimately be used for law enforcement including for a prosecution under a by-law or in a specific criminal investigation, on its own, this does not provide a municipality the authority to enact a by-law requiring the routine collection and disclosure of personal information to the police.[19] In addition, municipalities should "attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives."[20]

3) The belief that the collection of sellers' personal information is "necessary to the proper administration of a lawfully authorized activity." In order to demonstrate that this condition applies, a municipality must first determine what the "activity" is, and whether it is "lawfully authorized." Municipalities are authorized to license businesses under the *Municipal Act* for one or more listed purposes. Having identified the appropriate purpose, the municipality must demonstrate that the collection of personal information is "necessary to the proper administration" of the lawfully authorized activity. Accordingly, municipalities must show that each item or class of personal information that is to be collected is "necessary" to properly and effectively administer the lawfully authorized activity. Information that is merely helpful is not "necessary," and institutions must choose another route if the administration of the activity can be achieved without the collection of personal information.[21] Evidence demonstrating the necessity of a data gathering activity may come from task force reports, statistical studies, or other objective reports or studies showing the magnitude of the regulatory problem and the necessity of collecting personal information to effectively address it. Anecdotal evidence will generally be insufficient for the purposes of satisfying the necessity test. In addition, municipalities should "attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives."[22]

18 *Cash Converters, supra* note 5 at 30.
19 *Cash Converters, supra* note 5 at 38.
20 *Cash Converters, supra* note 5 at 30.
21 *Cash Converters, supra* note 5 at 40.
22 *Cash Converters, supra* note 5 at 30.

IV. Definitions

In these *Guidelines*:

Pawnbroker – Is "a person who carries on the business of taking by way of pawn or pledge any article for the repayment of money lent thereon."[23]

Pawn – Means providing a good to a pawnbroker as security for money lent. In other words, pawnbrokers lend money on the security of a good provided to the pawnbroker. The good can be retrieved if the individual pays back the pawnbroker's loan within a certain amount of time, otherwise the pawnbroker can sell the item to recover the cost of the loan.

Personal information – Is recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. It includes the name, address, telephone number, fingerprints, identifying numbers, photograph and employment information of an individual.[24]

Record – Is any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.[25]

Second-hand goods shops – Refers to any person who carries on a business involving the acquisition and disposition of second-hand goods other than by way of pawn or pledge.

Second-hand goods – Refers to goods of any kind acquired or disposed of by pawnbrokers or second-hand goods shops.[26]

Business – Refers to pawnbroker or second-hand goods shop.

Seller – Refers to a person who pawns, sells or consigns his or her goods to a business.

23 *Pawnbrokers Act, supra* note 4 at s. 1.
24 *MFIPPA, supra* note 2 at s.2.
25 *Ibid.*
26 Typically, jurisdictions exclude or enumerate certain types of second-hand goods from licensing by-laws, either by list (e.g. books, clothing, baby furniture) or by value (e.g. goods valued at less than $1000).

V. Privacy guidelines for municipalities regulating businesses dealing in second-hand goods

To ensure that municipalities regulate second-hand goods in a privacy protective manner, the Office of the Information and Privacy Commissioner of Ontario encourages municipalities to be guided by these key practices.

1. Do not enact a by-law to collect personal information unless you can first empirically demonstrate the necessity to collect personal information.

   Municipalities must:

   - **Ensure collection is necessary**, not merely helpful. Municipalities are obliged to choose less personally-intrusive measures if the objective of the by-law can be accomplished without the collection of personal information.

   - **Justify collection** by determining an achievable purpose for collecting each element of personal information, and showing that the collection is rationally connected to those achievable purposes.

2. If you need to collect personal information, do so in the most privacy protective manner:

   - conduct a privacy impact assessment

   - narrow the scope of the by-law

   - minimize the personal information collected

   - require notice of the collection

   - limit use of personal information to the purpose for which it was collected

   - do not disclose personal information to third parties such as police without specific justification

   - specify security safeguards for personal information and information systems

Each of these guiding practices is described in more detail below.

1. Do not enact a by-law unless you can first empirically demonstrate the necessity to collect personal information

Municipalities must first:

> **Improve enforcement** of existing by-laws that do not require the collection of personal information to ensure that businesses are not accepting goods that could be stolen or altered to avoid detection.
>
> **Review licensing criteria** to permit the municipality to revoke or suspend a license of a business that contravenes the by-law requirements related to stolen goods.

Municipalities should also:

- **Focus on property, not people** by collecting, using, retaining, and disclosing information about the goods themselves such as serial numbers, detailed descriptions or even photographs of the goods, rather than information about the seller.
- **Notify the public** of businesses violating by-laws so that consumers can make informed decisions to reduce their chances of buying stolen goods. Require businesses to prominently display licenses.
- **Provide municipal contact information** to enable the public to report possible violations of second-hand goods by-laws.
- **Raise consumer awareness** on how to protect goods from theft, recording serial numbers to facilitate recovery of goods, and purchasing goods only from properly licensed businesses.

2. If you can prove the necessity to collect personal information, do so in the most privacy protective manner

If a municipality can prove that the collection of personal information is necessary, and has justified the collection of each element of personal information, then a municipality should:

Conduct a privacy impact assessment and take steps to mitigate identified privacy gaps. A privacy impact assessment is a process that helps to determine the effects that new technologies and proposed programs or policies may have on personal privacy, and the ways in which any adverse effects can be mitigated.[27]

27 Guidance on privacy impact assessments can be found on the Ontario Government website, see **http://www.accessandprivacy.gov.on.ca/english/pub/screeningtool.html**.

Narrow the scope of the by-law, such as, to those goods identified as being prone to theft, or goods exceeding a certain value.

Minimize the personal information collected by not requiring personal information beyond that which is justified and proven to be necessary.

Require notice of the collection of personal information to the seller in clearly written signs, prominently displayed on the premises of businesses.[28]

Limit use of personal information to the purpose for which it was collected, for example, businesses should not use sellers' personal information for direct marketing purposes without consent, in accordance with the federal *Personal Information Protection and Electronic Documents Act*.[29] In addition, if police access the personal information, they should not use it for any secondary purposes except in accordance with *MFIPPA*.

Do not disclose personal information to third parties such as police, without specific justification

In requiring the collection of personal information by businesses and its disclosure to police, a municipality is engaging in the constructive collection and disclosure of personal information.[30] To the extent that collection and disclosure are part of a co-ordinated scheme, both the collection and the disclosure must be justified.[31] Simply because the collection of personal information is proven necessary does not mean that disclosure of that personal information is proven necessary. By-laws cannot mandate the indiscriminate disclosure of personal information. The court in the *Cash Converters* decision said that "[t]he intent of *MFIPPA* is to ensure that the collection and retention of private information is strictly controlled and justified."[32] The court also said that of significant concern was "the wholesale transmission to the police of a significant amount of personal information about individuals … before there is any basis to suspect that the goods that were sold to the second-hand dealer were stolen."[33] Accordingly, the court ruled that a municipality must prove that the disclosure of each element of personal information is necessary before it can require any routine disclosure of these elements by businesses.

Assuming such a scheme can be justified as necessary and proportional, having mandated the constructive collection and disclosure of personal information, a municipality would be responsible for attaching conditions to police and other third parties limiting their use and any onward disclosure (to third parties) in a manner consistent with the obligations of a municipal institution under *MFIPPA*.

28 *MFIPPA, supra* note 2 at s. 29(2). Contents of such notice should include: a clear statement of the legal authority for the collection; the specific purpose or purposes for which the personal information is to be used; and the title, business address and telephone number of a contact at the municipality who can answer questions about the collection.

29 *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5.

30 A municipality engages in constructive collection or disclosure when it requires the collection or disclosure on its behalf.

31 *Cash Converters, supra* note 5 at 46.

32 *Cash Converters, supra* note 5 at 51.

33 *Cash Converters, supra* note 5 at 38.

Specify secure safeguards for personal information and information systems:

- Know that privacy is not the same as security and that the terms are not interchangeable;
- Promote the use of privacy enhancing technologies;
- Conduct an end-to-end threat risk assessment before launching or piloting an information transfer system based on wired or wireless technology;
- Mandate businesses to:
    - safely store personal information;
    - dispose of personal information according to a retention schedule;
    - ensure secure disposal of personal information;
    - establish a process to respond to privacy breaches.
- Service providers retained for electronic transmissions of personal information should be aware that their activities are subject to audit and that they may be called upon to justify their methods of handling personal information.

VI. Resources

The first resources that municipalities should consult are the *Municipal Freedom of Information and Protection Privacy Act*, the Global Privacy Standard, the Ontario Court of Appeal's decision in *Cash Converters*,[34] and IPC Order MO-2225.[35]

Prior to drafting a second-hand goods by-law or, for that matter, any new program with privacy implications, municipalities should seek legal advice and consult with their Freedom of Information and Protection of Privacy Co-ordinator. The Ontario Ministry of Government Services' Information and Privacy Office is a useful resource for Co-ordinators.[36]

Depending on the nature of the proposed by-law, municipalities should also consult publications available on the Office of the Information and Privacy Commissioner of Ontario's website (**www.ipc.on.ca**), such as:

- The 7 Laws of Identity: The Case for Privacy–Embedded Laws of Identity
- Wireless Communication: Safeguarding Privacy & Security (Fact Sheet)
- Secure Destruction of Personal Information (Fact Sheet)
- Breach Notification Assessment Tool
- What to do if a privacy breach occurs: Guidelines for government organizations

If municipalities have questions about these G*uidelines*, they should consult with the Office of the Information and Privacy Commissioner of Ontario:

Information and Privacy Commissioner/Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

Telephone: Toronto Area (416/local 905): 416-326-3333
Long Distance: 1-800-387-0073 (within Ontario)
TDD/TTY: 416-325-7539
FAX: 416-325-9195

Pour joindre l'agente des communications bilingue, veuillez composer le 416-326-4804.

34 The decision is available at **http://www.ipc.on.ca/images/Resources/up-cash_converters_CA.pdf**.
35 The order is available at **http://www.ipc.on.ca/images/Findings/up-mo_2225.pdf**.
36 See **http://www.accessandprivacy.gov.on.ca**.

Appendix A – Global Privacy Standard

Objective

The objective of the Global Privacy Standard is to form a set of universal privacy principles, harmonizing those found in various sets of fair information practices presently in existence.

The Global Privacy Standard draws upon the collective knowledge and practical wisdom of the international data protection community.

Scope

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;
- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS informs developers and users of new technologies and systems that manage or process information. The GPS may be particularly useful when developing information and communication technology standards, specifications, protocols, and associated conformity assessment practices.

The GPS can assist public policymakers when considering laws, regulations, programs and the use of technologies that may impact privacy. The GPS can equally assist businesses and developers of technology that may have an impact on privacy and personal information.

The GPS addresses privacy concerns for decision-makers in any organization that has an impact on the way in which personal information is collected, used, retained, and disclosed.

The GPS is not intended to pre-empt or contradict any other laws or legal requirements bearing upon privacy and personal information in various jurisdictions.

GPS Privacy Principles

1. Consent: The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater

the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

2. Accountability: Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.

3. Purposes: An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4. Collection Limitation: The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

   Data Minimization — The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

5. Use, Retention, and Disclosure Limitation: Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

6. Accuracy: Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

7. Security: Organizations must assume responsibility for the security of personal information throughout its lifecycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8. Openness: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9. Access: Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Compliance: Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.