Information
and Privacy
Commissioner/
Ontario

Privacy Alert:
A Consumer's Guide to Privacy in the Marketplace

Tom Wright
Commissioner
May 1994

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

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

This publication is also available on the IPC Web site.
Cette publication est également disponible en français.

Table of Contents

What is privacy and why should you care?

Pinning down what privacy is and why it matters so much has been the subject of considerable discussion over the past century.

In 1888, in his textbook on the law of torts, Thomas Cooley referred to the right "to be let alone".[1] Later, Warren and Brandeis "adopted Cooley's discussion of the right to be let alone, and stretched it somewhat to fit their argument in favour of a legal right to privacy."[2] In Canada, in the early '70s the Task Force on Privacy and Computers defined privacy as:

> … a constellation of three realms or zones in which an individual may, as a function of his personality, claim to be let alone to do as he sees fit.
>
> These relate to territorially definable zones in which an individual may seek to be physically removed from and undisturbed by others, the zone occupied by his body which the law has surrounded with an aura of inviolability, and the intellectual zone where he may seek to prevent information about himself from passing into the knowledge of others, particularly by such illicit means as eavesdropping.[3]

Privacy expert Alan Westin has defined privacy as: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[4]

In summary, privacy has been looked at:

> … as a "right", a "value", an "interest", a "claim", a "condition", a "principle", an "ability", a "power", and of course, "a constellation of values, claims and interests in a universe of concurring and competing values."[5]

Although the definitions may vary, especially in the legal context[6], privacy is important to a great number of people. Opinion polls for Equifax done by Louis Harris and Associates in Canada and in the United States have identified privacy as an important public issue. In the Canadian survey, some significant findings indicated that:

> What concerns Canadians in the consumer privacy sphere is how businesses and government agencies are using advanced information technology to collect, amalgamate, and exchange personal data about citizens. The survey shows that 64% of Canadians believe that consumers have lost all control over how their personal information is used by companies; 55% believe that "consumers being asked to provide excessively personal information" is a major problem; 62% believe that the present uses of computers are "an actual threat to personal privacy in this country"; and 56% favour a national law rather than separate provincial privacy rules for the use of consumer information by credit bureaus.[7]

A later study done in Canada and released by Ekos Research in March 1993, found that:

- 81 per cent feel strongly that they should be notified in advance when information about them is being collected;
- 83 per cent strongly believe that they should be asked for their permission before an organization can pass on information about them to another organization;
- 87 per cent strongly agree that when information about them is collected they should be told what it will be used for;
- 72 per cent of respondents said that being in control of who can get information about them is extremely important;
- 67 per cent feel controlling what information is collected about them is extremely important.[8]

You as a consumer can take back some control of your personal information. Learn about your right to privacy. Be aware. Exercise a little caution, a little curiosity and guard your personal information. Ultimately, only you can help to guard your privacy in the marketplace.

How did they get my name?

Imagine that you suffer from headaches. One day you go to your mailbox and find an envelope, personally addressed to you containing a letter and pamphlets on "Headaches… You Don't Have To Live With Them." Swallowing a painkiller you wonder: "How did they get my name?"

"How did they get my name?" This is the consumer chant of the '90s and it is quickly evolving into "Who Doesn't Have My Name?" Few have escaped it, because these days your name is worth its weight in gold. In fact, your name and other bits of your personal information are a multi-million dollar industry. *Maclean's* magazine reported that:

> The collection, compilation and trafficking in personal data has become a huge industry: some privacy experts say that it is worth as much as $300 million a year in Canada. It has grown, in part, because rapidly evolving technologies, including telecommunications and computers, have simply made it easy to do.[9]

You may unwittingly be helping this process along. You may unknowingly be inviting unwelcome intruders into your life. There are preventative measures you can take, however. A little caution, a little curiosity, a little knowledge, can help to guard your privacy.

In the following pages we offer you as a consumer some tips to preserve your privacy and describe the research on privacy in the area of consumer information — by our own staff and others.

This report is about your personal information and the marketplace. "Personal information" as it is used here encompasses any recorded information that may identify you. This report urges you, the consumer, to consider seriously your privacy and what it means to you when engaging in everyday transactions in the marketplace.

Today's reality is that your personal information is readily available to information brokers and direct marketers, and you as the consumer are usually the provider. In many marketplace transactions, most of us have given away our personal information such as name, address, occupation and income. Sometimes this information is understandably necessary to the transaction. But sometimes the information sought may be irrelevant and an invasion of one's privacy.

Although you do not necessarily authorize the resale or renting of your name, address or other personal information, it is likely that the company you are doing business with will, in some way, profit from the use of this information at the expense of your privacy.

Perhaps you thought nothing of providing your employer's name when you were applying for membership in a video club. You may even have provided your average monthly bank account balance in your application to rent an apartment. When you joined a book club or added your name to a mail-order catalogue list you initiated a potential avalanche of junk mail, and provided another bit of information for a data file somewhere that might be sold or rented.

How to guard your privacy in the marketplace

In Ontario, there are no fool-proof ways to ensure the protection of your personal information in the marketplace. However, you, as an informed consumer, can act responsibly and equip yourself.

Learn about your right to privacy. Once you have, you will acquire more confidence when dealing with the marketplace. Be aware. Be confident. Take control.

The items in the following checklist will not guarantee, but will help to safeguard your informational privacy in the marketplace.

Checklist

General

1. **Ask** to see the company's privacy or confidentiality policy — if it has one.

2. **Give** only the minimum personal information needed to complete a transaction. If you are in doubt about the relevance of any information requested, **Ask Questions**.

3. **Question** the need and purpose for the requested personal information.

4. **Ask** who will have access to the personal information you are providing. **Ask** if the information will be exchanged, sold or rented to a third party.

5. **Ask** to see your file with the company/organization to verify the accuracy of your information and to have the chance to correct any wrong information.

6. **Pay Cash**, thereby minimizing the need to give out any personal information at the time of the transaction.

7. **Guard** against the use of your Social Insurance Number. **Ask** why it is needed, and if necessary, **Ask** which law requires that it be collected.

Credit information

8. **Check** your file at your credit bureau annually. You have a right to see and correct information contained in your file. To make an enquiry, contact the credit bureau for your geographical area by checking under credit bureau in your telephone directory.

9. **Pay** your bills and pay on time. Once you go into debt, information about you begins to accumulate.

Medical information for insurance underwriters

10. **Obtain** a copy of your medical file used by insurance underwriters by writing to the Medical Information Bureau (MIB) P.O. Box 105, Essex Station, Boston MA, USA 02112. The MIB is a data bank with medical information on 15 million Americans and Canadians and is used by insurance underwriters to check medical histories.

Ontario Health Card

11. **Use** your Ontario Health Card **Only** for health services. It is illegal for someone to ask for this card for any other purpose.

Mail and telephone

12. **Find Out** if your telephone company offers a "call blocking" service so that you may block the identity of your number and/or name on outgoing calls.

13. **To Remove** your name from mailing and telemarketing lists, contact the Canadian Direct Marketing Association (CDMA) at (416) 391-2362 or by writing to 1 Concorde Gate, Suite 607, Don Mills, Ontario M3C 3N6. Only member companies of CDMA are covered. It can take 3–4 months for the removal request to take effect.

14. **When a Computer Calls**, you are receiving a call from an Automatic Dialling and Announcement Device (ADAD). Although difficult to control these calls, **Complain** to your telephone company if you have more than two calls in one month.

15. **Think** twice before dialling an 800 or 900 number. Your number could be recorded and sold to a telemarketer.

16. **Special Rebate Offers**, contest forms, free information kits and some warranty cards can be marketing techniques for gathering personal consumer information. If you cannot resist, **try** to provide only minimum information and **request** that the information not be disclosed to a third party.

17. Whenever an 'opt-out' mailing list box is provided, **Check** it.

Code of fair information practices

18. Apply your own individual code of fair information practices to transactions.

    The spirit of fair information practices is rooted in the 1980 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* from the Organization for Economic Co-operation and Development. (See Appendix A) It provides a helpful overall way of thinking about consumer privacy issues in the marketplace. Fair information practices are the foundation of most privacy protection legislation and privacy codes throughout the world. They are divided into three general categories. Although these three categories are designed for collectors of personal information, knowledge of them can also enhance consumer confidence when confronted with potential invasions of privacy in the marketplace. Collectors should:

    1. only collect accurate and pertinent information
    2. grant individuals access to their personal records
    3. limit access to personal data by third parties.[10]

The IPC visits the marketplace

The Information and Privacy Commissioner/Ontario (IPC) follows trends and developments which could have an impact on individual privacy.

Research has shown that some requests for your personal information in the marketplace are completely unnecessary and intrusive. Suggestions for dealing with those types of requests are plentiful and come from a variety of sources. The IPC undertook its own field research under ordinary circumstances of daily life and developed what it considered to be the best advice for guarding your privacy (our checklist, above).

The premise of this approach was that: the extent of personal information collected and sold about individuals is still not well appreciated by the general population; that often, individuals unknowingly provide unnecessary information about themselves and unconsciously contribute to the massive information-gathering industry; and that the IPC has a role to play in drawing public attention to privacy issues in the marketplace, especially in the absence of privacy protection legislation in the private sector.

Several IPC staff kept "privacy diaries" to record incidents they felt, as consumers, were threats to their privacy. This led to the design of a small "snapshot" study. The objective was to examine, experientially, the general awareness and sensitivity levels for privacy in the marketplace from the perspective of the consumer. It was the IPC's reasoning that the information recorded would then serve as a collective snapshot of experiences that anyone might have in the course of daily errands; it could, in fact, reflect quite accurately a day in someone's life from the perspective of his/her privacy in the marketplace. Accordingly, the snapshot study was named "A day in the life".

A day in the life

Today's marketplace is fuelled by information. Ordinary day-to-day transactions that everyone engages in leave a blazing electronic trail of information; practically every transaction you are involved in is recorded in a database somewhere.

It is a brave new marketplace. Checkout scanners and magnetic stripe customer "loyalty" cards at the grocery store, telephones that display incoming numbers and names, interactive multi-media technology, electronic banking and credit, telemarketing and memory chips in service cards are all symbols of the dramatic changes in our consumer culture.

This is the information age, the age of technology. The information superhighway is under construction. Economist Nuala Beck estimates that by the year 2035, a total conversion from the old economy to the new economy — an economy driven by the "engines" of computers and semiconductors, health and medical instruments and supplies, communications and telecommunications, and instrumentation — will have occurred. The key factor in the shift to the new economy is inexpensive microchips.[11] We are now in the transition phase.

In the new economy, the issue of informational privacy will intensify unease for consumers who **are** concerned about guarding their privacy. As the ability of modern technology to collect, store, manipulate and analyze information grows by leaps and bounds, so too will the value of information as a commodity. As the supplier or holder of much of that information, consumers may want to think carefully about the impact of providing personal information on their privacy — what does it mean to you, how do you take care of it, and when are you prepared to give it away. Or, as Lawrence Hunter and James Rule have proposed, to sell personal information — suggesting that consumers should have the right to control the commercial uses of their personal information:

> Needed is policy that would permit individuals to make and implement their own decisions about how and how much to participate in these information flows. Accordingly, we advocate legislation of a new kind of property right over personal information. Under this right, every citizen would own the rights to commercial exploitation about himself or herself. These rights could be retained or sold, much like mineral rights, development rights, or air rights.[12]

It is all quite unsettling. Junk mail may be just an annoying symptom of techno-marketing, but highly sensitive information about your financial and medical worthiness can determine the outcome of major life events and decisions. In the United States, horror stories of invasions of privacy are becoming more well-known. Witness the 1993 publication of *War Stories — Accounts of Persons Victimized by Invasions of Privacy* by Robert Ellis Smith. In the Introduction, Smith says that the collection of stories answers the following question: "What's the worst that can happen?"[13]

Unlike the public sector, the marketplace in Canada (with the exception of Quebec) and the United States is not regulated by privacy protection legislation. In Ontario, personal information held by government organizations is protected by the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. However, the collection, retention, use and disclosure of any personal information you provide to a private sector company is not explicitly covered by privacy protection legislation in Ontario. The same is true federally.

However, Ontario consumers are not without some protection related to the marketplace. In the area of credit, the *Consumer Reporting Act* identifies the type of information that can be collected in your credit record, specifies how this information can be used and protects consumers against the use of inaccurate or outdated information. The *Ontario Consumer Protection Act*, *Business Practices Act*, and the *Collection Agencies Act* also cover various aspects of consumer protection in relation to business practices.

Other influences on the future of the Ontario marketplace exist. Developments on several fronts are indicative of what is to come:

- overseas, a draft European Community directive on data protection is targeted for implementation in 1995 — the directive would allow member countries to block the flow of personal information to countries that do not offer "adequate" personal data protection;
- the Canadian Standards Association (CSA) has established a committee of government and private sector representatives to develop a code for privacy standards — these standards, although voluntary, would offer greater protection for personal information; and
- Quebec has taken the first step in North America of extending privacy protection to the private sector through the enactment of its statute, *An Act Respecting the Protection of Personal Information in the Private Sector*.

The lack of formal government regulation has left the creation of rules for transactional information to the private sector. Some private sector associations/companies have developed voluntary codes of practice that include attention to privacy matters for their members or customers. Some Canadian examples are:

- Canadian Direct Marketing Association Code of Ethics and Standards of Practice
- Cable Television Customer Service Standards
- Major banks have privacy codes based on the Canadian Bankers Association's *Model Privacy Code for Individual Customers*
- Equifax Canada has published *Consumer Information and Privacy*, the company's operating policy on privacy and confidentiality
- Bell Canada's Privacy Policy.

IPC research methodology

The IPC study took a qualitative approach with the methodology of participant-observation. This permitted IPC staff to enter the field as consumers and become "participants" in the study. It also permitted us to approach a number of organizations, perform a variety of consumer transactions and, through observation and questions, actively participate in the study without identifying ourselves as staff of the IPC. As Pearsall stated: "Participant-observation is at once a role, a means of getting data and a methodology for understanding human behaviour and natural context."[14] We felt that this "hands-on approach" would yield the most useful information and best reflect "real-life" experiences shared by other consumers.

For two weeks in December 1993, IPC staff went out into the marketplace as **consumers**. They performed 22 pre-selected transactions; 12 were done in person, nine were by telephone and one was by letter.

This selection sample was based on two main factors: there was a genuine need by the staff member to personally obtain or apply for a service; and the selected transaction represented a common everyday transaction that anyone might need to do. The pre-selected transactions were:

- A credit bureau — to examine one's credit file.
- A charitable foundation — to find out what happens to personal information that is provided when a donation is made.
- A trust company — to find out if the personal information collected pursuant to buying an RRSP mutual fund was appropriate.
- Four retail merchandise stores — making purchases and applications for credit.
- A video rental store — membership applications for two different stores.
- A library — applying for membership.
- A school — request for school records.
- A medical centre — two separate/unrelated requests for one's own medical records.
- A drugstore — inquiring into the information practices for the prescriptions data base.
- A marketing association — two requests for "Do not call" and "Do not mail".
- Medical Information Bureau — one request for one's own personal information.
- A credit union — applying for membership.

In carrying out the transaction, the following four standardized questions were used by staff to probe how the organization dealt with privacy issues:

- Why do you need this personal information?
- What are you going to do with this information?
- Do you keep this information confidential? If so, how?
- What happens if I don't give you this information?

IPC staff also recorded their general impressions of their experiences including "the geography" of privacy — did the "physical set-up" of the transaction area allow other customers to overhear what was being said or see what was being documented.

After each transaction was completed, staff recorded their experience on a standardized form; for telephone transactions the same procedure for questions and probing was followed as for the in-person transactions. The recorded information sheets were then reviewed to determine common themes.

Our findings

The findings that staff recorded as observations or impressions during the study transactions do not represent the definitive statement on the marketplace and your privacy. Rather, these findings relate to anecdotal information and provide some cautionary flags that may be instructive for consumers in their everyday transactions within the marketplace.

To simplify the analysis, two common themes were identified after reviewing the "collective snapshot" of the recorded information:

1. receptiveness to privacy questions and concerns; and
2. relevance of the information being collected for the transaction.

Receptiveness to privacy questions and concerns

In half the transactions, IPC staff found the person serving them to be not only receptive to questions, but generally knowledgeable and informed about privacy issues. For example:

- In one of the video store membership transactions, the staff person was sensitive in a positive way to all questions concerning the use and the disclosure of the information asked for on the application form; receptive and knowledgeable to questions about company policy on confidentiality; concerned and forthcoming about discussing privacy matters.

- The telephone call to the charitable foundation was very positive. All questions and concerns about privacy were answered without hesitation, in a knowledgeable and helpful manner.

- The visit to the credit bureau was also positive from start to finish. Each question asked was answered in meticulous detail. Care was taken to speak at a low volume so others could not hear, and a written policy that was requested was provided.

In the remaining half of the transactions, the person delivering the service was quite or very insensitive to the importance and relevance of privacy concerns and defensive about answering any questions. For example:

- In one video store transaction, one credit card application, and one drugstore transaction, the counter personnel could not answer any questions at all, and were somewhat annoyed at being questioned.

- Requesting school records and asking the basic survey questions caused intense hostility on the other end of the telephone.

- In the two separate requests for files at a medical centre, two entirely different responses were obtained: one IPC staff member was told, with great animosity, that under no circumstances could this file information be released; the other IPC staff member was told to write a letter to the centre and formally request the file information and to indicate why the information was being requested. Same request, two totally different responses.

Relevance of the information being collected

IPC staff noted that some unnecessary information was requested in 10 transactions. When questioned why certain information was being requested, in most cases the response was that the information was optional or not necessary, or the salesperson "didn't know why". Examples include:

- In one retail store, several problems emerged: paying cash for an item required providing a telephone number, otherwise a bill could not be issued; when the general telephone number for the IPC was provided and punched into a computer, a list of other IPC staff appeared on the screen in clear view of anyone standing around the service table; in enquiring about the store's exchange policy, the IPC staff person was told that if the item was going to be returned, then a name would also need to be provided "for the system", otherwise exchange would be "extremely difficult"; during the course of the transaction, IPC staff overheard several telephone conversations where telephone customers' personal information was heard across the store, and there were papers with names, addresses, and credit card numbers sitting on the service desk.

- During one credit card application transaction, at least three items of personal information turned out to be "optional" when the sales person was asked why this information was needed.

- At the library, the IPC staff member was asked for a piece of personal information. When this was questioned, it turned out to be unnecessary.

In isolation, the findings are not profound, but one useful inference can be drawn. The IPC staff who participated in contacting the companies were already in tune with privacy issues and familiar with the standards of fair information practices. This awareness and the confidence it brings definitely influenced how they conducted their transactions and, in turn, the personal information they did or, more importantly, did not provide.

But whether sensitivity to privacy issues will become a front-line customer service feature at the point of transaction in the marketplace remains to be seen. Although some industry responses to consumer demand for privacy protection **are** evident, particularly in part through voluntary codes, these scattered pieces of protection may not be enough to salvage whatever informational privacy you have left — especially at the critical point of doing business at the service counter.

It often comes right down to a face-to-face exchange between you and the employee of the company you are dealing with; and a company privacy code may not be a guarantee that front-line staff are trained in carrying out the full intent of such codes. They may not be aware of why the information is collected, how it is (or is not) protected, and who has access to the information. Clearly, attention given to privacy as a fundamental customer service feature is still emerging.

The IPC seeks your help

We would like to hear about your consumer experiences. If you want to share a good or bad experience related to your personal information and privacy in the marketplace, let us know — **anonymously, if you wish.** Although we will not be able to respond to you, your experiences will help to shape our future efforts to comment on privacy issues in the marketplace.

Please address your experiences to:

Privacy and the Marketplace
Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario
M5S 2V1

Appendix A

Where privacy is concerned, most privacy codes endeavour to emulate the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* established by the Organization for Economic Co-operation and Development (OECD) in September 1980. Canada adopted these guidelines in 1984. The basic principles of the guidelines, referred to generically as "the code of fair information practices", are:

Collection Limitation Limited to the collection of personal data; data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [Purpose Specification Principle] except: a) with the consent of the data subject, or b) by the authority of law.

Security Safeguards Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller.

Individual Participation An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him:

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraph (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability A data controller should be accountable for complying with measures which give effect to the principles stated above.[15]

Notes

1. Thomas M. Cooley, *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, 2nd ed. (Chicago: Callaghan & Co., 1888), p. 29 as cited in Ian Lawson, *Privacy and Free Enterprise*, (Ottawa: Public Interest Advocacy Centre, December 1992), p. 48.

2. Warren and Brandeis, "The Right to Privacy" (1890), 4 *Harv. L.R.* 193 — 204, cited in Lawson, *op. cit.*, p. 48.

3. Canada, Depts. of Communications and Justice, *Privacy and Computers* (Ottawa: Info. Canada, 1972), p. 126, as cited in Lawson, *op. cit.*, p. 51.

4. Alan F. Westin, *Privacy and Freedom*, (New York: Atheneum, 1967), p. 7, as cited in Lawson, *op. cit.*, p. 52.

5. Lawson, *op. cit.*, pp. 61–62

6. In Chapter Two of *Privacy and Free Enterprise*, Lawson discusses a range of definitions of privacy by legal writers, in four categories: the anti-interventionists, the informational self-determinists, the legal pragmatists, and the definitional agnostics.

7. Louis Harris & Associates, *The Equifax Canada Report on Consumers and Privacy in the Information Age*, 1992, p. V.

8. Ekos Research Associates Inc., *Privacy Revealed — The Canadian Privacy Survey*, 1993, p. 11.

9. Barbara Wickens, "New technology has made trafficking in personal data a huge industry", *Maclean's*, April 26, 1993, pp. 20–21.

10. David F. Linowes, *Privacy in America — Is Your Private Life in the Public Eye?*, (Chicago: University of Illinois Press, 1989), p. 174.

11. Nuala Beck, *The New Economy*. From a presentation based on the book, at the Workplace 2000 Conference, Toronto, May 7, 1993.

12. Hunter, Lawrence and Rule, James. *Toward Property Rights in Personal Information*, paper presented to the Ontario IPC, Dec. 17, 1993; now submitted for publication.

13. Robert Ellis Smith with Eric Siegal and James S. Sulanowski, *War Stories — Accounts of Persons Victimized by Invasions of Privacy*, (Rhode Island: Privacy Journal, 1993), p. ii.

14. Pearsall, M. *Participant Observation As Role and Method In Behavioural Research*. In William T. Filstead (ed). Qualitative Methodology. Chicago: Markham Publishing Co., 1970.

15. A complete text of the Guidelines is provided in Wayne Madsen, *Handbook of Personal Data Protection* (New York: Stockton Press, 1992), pp. 992–996. The Principles are covered on pages 994–995.