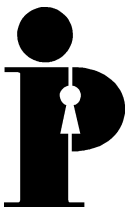
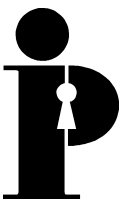
Information
and Privacy
Commissioner/
Ontario

Best Practices for Online Privacy Protection



Ann Cavoukian, Ph.D.
Commissioner
June 2001



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.

Cette publication est également disponible en français.

Table of Contents

Introduction

The online world is creating exciting new commercial opportunities for Canadian businesses. Consumers are drawn to electronic commerce not only because of the products and services available, but also because of the convenience and savings possible with online transactions.

However, there are strong indications that the growth of e-commerce is being impeded by consumers' fears about their privacy online. One recent survey revealed that eight out of ten Canadian consumers were concerned about protecting their privacy when participating in online activities, and that 40% did not believe that online companies honoured their posted privacy policies.[1]

Consumers' fears about privacy are not without foundation, and are reinforced by frequent media stories about poor online practices and unauthorized access to online data. A Canadian study of commercial Web sites showed that:

- half of the surveyed sites did not have a privacy policy;
- 40% did not indicate if they shared the information they collected with a third party;
- 26% of sites used cookies, but did not reveal that to users;
- over half of sites did not provide contact information; and
- more than 60% did not allow users to access information they had submitted.[2]

One of the more troubling conclusions of this study was that Canadian-based sites perform much worse in terms of privacy than sites outside the country that target Canadian users.[3]

Clearly, the need to establish and maintain the trust of customers or potential customers is a significant challenge for online businesses, and a key to lasting commercial success. Protecting privacy is an essential component of building that trust.

In addition to consumer pressures, Canadian businesses are facing an evolving legislative framework for privacy protection in the private sector. To respond to the dual incentives of developing consumer trust and compliance with legislation, companies that wish to succeed in the online world are working to make privacy protection an integral part of their business initiatives.

---

[1] David Akin, "Canadians still not sold on Net privacy policies," *National Post Online*, January 17, 2001, <www.nationalpost.com/tech/story/html?f=/stories/20010117/439311/html>, 01/18/01.

[2] Natalie Southworth, "Canadian Web sites woeful in privacy: survey," *The Globe and Mail*, December 7, 2000, p. B-9.

[3] Michael Geist, "A troubling snapshot of e-privacy in Canada," *The Globe and Mail*, December 7, 2000, p. T-4.

Online businesses need to move quickly to understand their responsibilities to respect their customers' privacy. They need to recognize that:

- if they collect, use or disclose personal information, they must do so responsibly;
- they must maximize customer control over their own personal information online; and
- they must ensure that their information practices are open and transparent to the consumer.

Beyond compliance with the law, privacy protection is critical to competitiveness online. Effective privacy protection is now a necessary part of doing business. There are significant risks and consequences (both commercial and legislative) to businesses that do not adequately address privacy.

To encourage companies to examine their online practices, and to more fully integrate privacy into those practices, the Office of the Information and Privacy Commissioner/Ontario[4] (IPC) has developed a set of best practices for online privacy protection. These best practices outline areas that should be addressed in order to effectively protect the privacy of online customers. They are overlapping and interrelated in nature, which means that in order to adequately protect privacy, all eleven areas must be considered. But these practices are not intended to be adopted in their entirety — they consist of a list from which you may select those most appropriate to your circumstances.

This collection of best practices is intended to serve as an educative tool and is not meant to supercede or compete with existing or future legislation, international agreements, membership requirements for industry associations, or any other mandatory or voluntary provisions with which online companies must comply. It is, however, meant to serve as a useful foundation upon which businesses can build their online privacy practices.

[4] For information about the Office of the Information and Privacy Commissioner/Ontario, please see our Web site <www.ipc.on.ca>.

Best Practices

Respect for Privacy

- Conduct business in the least privacy-intrusive manner possible.
- Understand and comply with applicable privacy legislation, agreements, and standards.
- Understand that personal information includes all information about, or linked to, a personally identifiable individual. This includes such information as name, address, credit card number, income, purchase preferences, and transactional data. E-mail addresses, as well as data collected from automatic tracking methods may constitute personal information if linked to an identifiable individual.
- Recognize that personal information is about individuals who have the right to exercise reasonable control over that data.
- Assess the impact on privacy of any proposed online practice, service, product, or technology, prior to implementation.
- Take special care when dealing with children. If there is a reasonable likelihood of collecting, using or disclosing personal information from or about children, follow appropriate privacy practices (e.g., the Canadian Marketing Association's special considerations for children in its *Code of Ethics & Standards of Practice*).

Openness

- Develop privacy policies and practices requiring personal information to be handled in an open and accountable manner.
- Be open and informative about your organization's policies and practices involving personal information.
- Ensure your stated policies and practices are factual, accurate and complete. Do not misrepresent your company's identity or information practices.
- Inform individuals, upon request, of any records your organization maintains containing their personal information, how you use it, and what data you disclose.

- Provide individuals with sufficient information for them to understand their privacy rights, and give them the opportunity to exercise those rights quickly, effectively, and without prohibitive cost. Information should include the name or title and contact information of the person/area responsible for your privacy policies and practices, as well as details about how individuals can access their personal information in your control.

- Prepare and post a privacy policy on your Web site. Your policy should clearly explain all your responsibilities and information practices. Specifically, your policy should be designed so it is:

    - easy to find, easy to read, easy to print, and easy to understand (e.g., use examples to explain and demonstrate your practices);

    - accessible from every Web page, not just the home page; and

    - written in the same language as the Web site to which it is attached.

- Do not change your stated privacy policies and practices without providing enough time and information for affected individuals to make informed decisions and take appropriate action.

- Inform individuals of:

    - all applicable privacy legislation and agreements, and provide links to the Web sites of the authorities responsible for the administration and enforcement of these instruments;

    - all professional codes of practice, seals, or other programs you must be in compliance with, and provide links to the full text of these agreements, and to the Web sites of the organizations responsible for their proper implementation and enforcement;

    - the consequences to your organization for non-compliance with your privacy policies and practices, and with all other relevant programs and legislation (e.g., audit, penalties or sanctions, revocation of seal, loss of professional membership, complaint forwarded to an oversight body for investigation, or publication of name for non-compliance); and

    - their recourse if they believe you are not complying with your policies and practices, or with any other relevant programs or legislation.

- Explain your use of any type of Web-based tools to collect personal information that may not be readily apparent to a user. This should include use of automatic tracking software, clickstream data, cookies, and clear GIF files (i.e., Web bugs).

- Explain your solicitation practices (e-mail and other means), as well as what personal information you rent, sell, or exchange to third parties for marketing or other purposes.

- Inform individuals:
    - if data you collect, use and disclose online is handled differently offline and why. If it is, specify how, and inform them how they can interact with your organization through other means (e.g., mail, in person, fax, or telephone); and
    - of any security or privacy violations involving their personal information as soon as possible, as well as what action they can take to remedy the problem or minimize the risks.

Accountability

- Ensure privacy protection is a priority for all levels of your organization. Top level commitment to privacy policies and practices is critical for success.

- Understand that if you collect personal information, you accept the responsibility to handle that data in accordance with your stated privacy policies and practices, and to make that information available to the individual to whom it relates.

- Train your staff and make them accountable for adherence to your privacy policies and practices.

- Designate a specific individual or position responsible for protecting privacy and complying with your privacy policies. While in larger organizations it may be necessary to have a team or group involved in developing and implementing your policies, with varying levels of responsibility, there always should be someone with final accountability. Provide sufficient resources and authority to discharge this responsibility in an effective and timely manner.

- Publicize the identity of the responsible individual on your Web site, along with information about how they can be reached online and offline, and your days and hours of operation, if applicable.

- Establish procedures for reviewing your privacy policies and practices to ensure they remain accurate, timely and complete.

- Develop a process to verify your compliance with your stated privacy policies and practices, and to publicly demonstrate that compliance.

- Define your obligation to undertake all necessary action to correct any problems that arise out of your non-compliance with your own policies and practices, or with any legislative requirement.

- Include privacy protection requirements, comparable to your own policies and practices, in your contracts with business partners or third parties who will have access to personal information collected or controlled by you. This is particularly important if you will be sending personal information to jurisdictions without comparable privacy protection regulation. Take all reasonable steps to ensure the contracted party follows the privacy protection measures stipulated in your contracts (e.g., site visits, audits).

- Understand that if you collect personal information, you accept the responsibility to handle that data in accordance with your stated privacy policies and practices, and to make that information available to the individual to whom it relates.

Purpose Specification

- Define the purposes or reasons why you need each piece or type of personal information (e.g., name, address, e-mail address, clickstream data, age, gender, income, etc.) in order to complete a specific, legitimate business transaction. When identifying potential purposes, consider the following:

    - if non-identifiable information (i.e., coded, anonymous, pseudonymous, or aggregated) could fulfil the purpose;

    - how the personal information needs to be collected (e.g., directly from the individual through a subscription, automatic collection of clickstream data, or from a third party) and why;

    - who will need to use the information (within and outside the organization), and why; and

    - to whom it will need to be disclosed, and why.

- Identify any additional reasons to collect, use or disclose personal information not strictly related to the specific business transaction (e.g., incentive programs, target e-mail marketing services, data mining, etc.).

- Understand that your defined purposes should be reasonable in the context of your business.

- Do not define your purposes so broadly as to make them meaningless to the individual from whom you want to collect personal information.

- Document your purposes so that your staff and the individuals to whom the personal information relates can know what they are.

- Identify any new purpose for using previously collected personal information prior to its use.

Individual Knowledge[5] and Consent[6]

- Obtain consent prior to collecting individuals' personal information, whenever possible. Ensure that individuals understand the purposes for which you will be collecting, using and disclosing their personal information prior to obtaining their consent.

- Use express consent provisions whenever possible. Set the defaults on consent options to be the most privacy protective (e.g., do not use a negative option such as pre-checked boxes on registration pages that require individuals to take action in order to indicate what they do and do not consent to).

- Consider the sensitivity of the personal information involved when determining the appropriate type of consent. As a general rule, more sensitive data (e.g., medical or financial information) should have express rather than implied consent.

- Define narrowly the exceptional circumstances when consent is not possible or maybe inappropriate. In very limited circumstances you may need to collect, use, or disclose personal information without any type of consent (e.g., for law enforcement purposes or when the individual is a minor, seriously ill or mentally incapacitated).

- Provide individuals with clear and adequate information for them to make an informed decision about giving their consent, including the consequences of refusing or withdrawing consent, if any. Individuals should be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

- Provide individuals with a simple, clear and secure online mechanism to indicate their consent, refusal or withdrawal of consent, regarding the:

    - collection, use and disclosure of their personal information;

    - storing, altering, or copying of any information on their computers;

    - use of any type of automatic tracking software, by you or a third party, including the automatic disclosure of clickstream data to third parties; and

    - receipt of any online or offline marketing or promotional communications, from you or third parties.

[5] Knowledge is when an individual has an awareness and understanding of the facts and implications of something.

[6] Consent is to give one's permission or to agree to something. Express consent is when it is given explicitly and unambiguously (e.g., "Yes, I agree to you selling my mailing address to third parties"). Implied consent is when it can be reasonably inferred or understood from activity or inactivity on the part of the individual (e.g., if you purchase a book online, it is reasonable that you consent to the book vendor giving your mailing address to its delivery company).

- Do not mislead or pressure individuals in order to obtain their consent.

- Do not make the supply of your product or service conditional on individuals consenting to purposes unrelated to the supply of that product or service.

- Do not withdraw previously accessible services or products if individuals do not consent to the use or disclosure of their personal information for new and unrelated purposes.

- Inform individuals of exactly what is, and is not, covered by your consent provisions (e.g., collection by your Web site only or also by a third party), and if their consent is time-limited.

- Ensure individuals understand when you will not be asking for consent and why (e.g., after initial consent is given, and until such time as individuals take contrary action or notify you of a change in their wishes, permission to use persistent cookies will not be solicited each time they re-visit your site).

- Take reasonable steps to verify that the individual providing the consent is authorized to do so (e.g., is the individual to whom the personal information relates or is the authorized representative).

- Take reasonable steps to ensure that the individual is old enough to give legal consent when your product or service likely involves children. When appropriate, obtain explicit and verifiable consent by a child's parent or authorized guardian prior to the collection, use or disclosure of any personal information related to that child.

- Obtain consent from the individual to whom the personal information relates, prior to using their data for a new and unrelated purpose, unless that purpose is required by law.

- Do not assume that because individuals have visited your site or even made a purchase, they consent to solicitation.

- Do not require individuals to call or write to express their lack of consent for your use of their personal information collected online. At the time of consent, ask individuals if you can follow-up with them, and how they want to be contacted, if at all. Maintain a record of consent and make it accessible to individuals for their review.

- Do not revoke opt-in/opt-out options or change time limitations, without prior and adequate notice to the individual.

Collection Limitation

- Do not collect personally identifiable information, whenever possible (e.g., permit the individual to visit your Web site without capturing clickstream data, or let the individual deal with you anonymously or pseudonymously).

- Collect only the amount and type of personal information necessary and relevant for the identified purpose(s), or as required by law.

- Collect personal information by lawful and fair means, and from reliable sources.

- Do not collect personal information in a covert or coercive manner, or through misleading or deceptive practices.

- Inform individuals, at or before the time of collection, of the type of personal information you intend to collect, including data you collect by automated means.

- Inform individuals, at or before the time of collection, if the personal information to be collected is required by law and, if so, fully explain the specific requirement.

- Collect personal information directly from the individual to whom it relates, except in limited and defined circumstances.

- Inform individuals of the types and sources of personal information you collect indirectly for the purpose of providing services or products (e.g., data collected from third parties). Also indicate why direct collection is not possible or appropriate.

- Do not allow third parties to collect personal information or cookies through your Web site unless they are contractually bound to a comparable privacy standard.

- Avoid collecting unique identifiers (e.g., SIN or driver's license number) unless their use is required by law, or express consent is obtained from the individual. If required to collect unique identifiers (e.g., for tax requirements), explain reasons to the individual at or before the time of collection.

- Comply with relevant legislative restrictions on the collection of personal information (e.g., human rights legislation may limit what may be collected on employment applications).

Use and Disclosure Limitations

- Do not use personal information except in the manner, and for the purpose(s), identified to the individual at the time of collection, unless the individual to whom the personal information relates consents, or by authority of law.

- Do not disclose, distribute, or make personal information available in any way, except for the purpose(s), and to the sources identified to the individual at the time of collection, unless the individual to whom the personal information relates consents, or by authority of law.

- Take all reasonable steps to ensure that the personal information you use and disclose is relevant and necessary to fulfil the identified purpose(s), or the requirements of law.

- Use both policy and technical restrictions to control unauthorized and unrelated uses and disclosures.

- Limit use of persistent cookies to where they are needed for a continuing purpose. The expiry date of a cookie should be consistent with the purpose.

- Inform individuals of any legal requirements you have to disclose personal information, and to whom. Include these requirements in your privacy policies.

- Inform individuals of the circumstances when disclosure may take place without their prior knowledge or consent (e.g., serious and imminent threat to public health or safety). Include these reasons in your privacy policies.

- Do not knowingly disclose or transfer personal information to third parties without adequate privacy safeguards.

- Establish appropriate and effective controls and schedules for information retention and destruction. Ensure that all practices are fully documented.

- Retain personal information in identifiable form only as long as it is relevant and necessary to fulfil the purpose(s) for which it was collected, as required by law, or as needed to give the individual to whom the information relates an opportunity to access and/or correct the data.

- Destroy, erase, or permanently de-identify any personal information no longer needed for its identified purpose(s) or to meet legal requirements.

- Maintain a record of disclosure so you can update third parties who have previously received personal information from you, as required (e.g., in cases when disclosed data are corrected due to inaccuracy).

Accuracy

- Do not knowingly collect, use or disclose inaccurate personal information.

- Take all reasonable measures to ensure personal information is accurate, complete, and up-to-date, having regard for the nature of the data, the purpose(s) for which it is collected, used and disclosed, and the interests of the individual to whom the data relates.

- Take all reasonable steps to minimize the chances of inaccurate data being used to make a decision about an individual. In determining what measures you should adopt, consider the extent of potential harm to the individual should you use or disclose inaccurate information.

Security

- Protect all personal information in your control from loss or theft, and from unauthorized access (within and outside your organization), use, alteration, copying, disclosure, and destruction.

- Establish security safeguards appropriate and proportional to the sensitivity of the personal information, and the nature of the possible risks. In gauging sensitivity, consider the potential harm (e.g., financial loss, loss of benefits or opportunities, discrimination or stigmatization, public embarrassment) to the individual should the information be misused or disclosed in an unauthorized manner.

- Implement effective physical, technical, and procedural measures to secure personal information on your Web site and linked computer systems.

- Develop policies and practices restricting employee access (including information technology staff) to personal information for unrelated and non-business reasons. Include appropriate disciplinary measures for violation.

- Inform individuals of the security measures you will undertake to protect their personal information. Include an outline of these measures in your privacy policies.

- Inform individuals of the steps they should take to conduct online transactions safely and securely.

- Establish appropriate access and verification procedures, audit trails and record integrity controls.

- Take all reasonable steps to ensure communications or transactions through your Web site do not result in unauthorized access to individuals' computers or personal information, or unauthorized modification or destruction of their data.

- Establish secure disposal procedures to ensure personal information cannot be recreated or reconstructed after destruction, and the individual cannot be identified or linked to that data in any way.

- Maintain a record of destruction documenting how and when personal information is destroyed, and the necessary authorization to do so.

- Take all reasonable steps to ensure third parties involved in a transaction (e.g., those renting or leasing the data, as well as any party contracted to your organization to conduct such activities as data processing or data mining) have adequate security.

Right of Access and Correction

- Design your information management systems and practices to facilitate individuals' right to access their own personal information, and to challenge the accuracy and completeness of their personal information in your control.

- Inform individuals of their right to access and correct their own personal information, and how that right may be exercised.

- Establish a simple, clear and secure online mechanism for individuals to find out:
    - what personal information relating to them you have, both online and offline;
    - the purposes for the collection, use and disclosure of that information;
    - to whom it has been disclosed;
    - the full cost of access (costs should be reasonable and demonstrable);
    - the sources of the personal information (whenever possible); and
    - the name and location of the person in charge of the information.

- Provide individuals with a simple, clear and secure online mechanism to:
    - access their personal information, upon request; and
    - review and correct their personal information, if necessary.

- Ensure access is provided to individuals in an understandable format, and without undue delay or expense (e.g., at no or minimal cost), whenever reasonably possible.

- Establish clear and limited criteria for why individuals' requests for access or correction may be denied. Include these reasons in your privacy policies.

- Verify the identity of the individual before granting access to, or correction of, any personal information.

- Correct or destroy personal information found to be incorrect, incomplete, irrelevant, or inappropriate, as quickly as is reasonably possible.

- Provide individuals with the following, if you deny their request to access or correct their personal information:

    - the reasons for that decision, in a timely and understandable manner;

    - an opportunity to prepare a "statement of disagreement" and have it, along with your reasons for denial, attached or linked to the data in question, in the event that their challenge remains unresolved;

    - an opportunity to clarify their request; and

    - a fair opportunity to challenge the decision.

- Take all reasonable measures to inform third parties who have used or accessed personal information within the last year, of the relevant corrected information or unresolved challenges. Provide them with copies of corrected information or the record of unresolved challenge, if possible.

Complaints/Dispute Resolution

- Develop procedures to receive, investigate and respond to complaints and questions about all aspects of compliance with your posted privacy policy and practices. Permit as much secure online interaction as possible.

- Ensure your complaint and dispute resolution processes are effective, fair, impartial, confidential, understandable, easy to use, and timely. They also should be cost effective for all parties involved, to the extent reasonably possible.

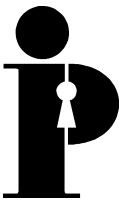
- Respond to complaints, and take corrective action, as appropriate, in a timely manner.

- Ensure your process for receiving and responding to inquiries and complaints, along with the individual's recourse, is fully described and easily found on your Web site.

- Do not charge individuals for the opportunity to exercise their right to challenge your denial of access decisions.

- Inform individuals of any third party investigative and dispute resolution procedures available to them.

- Direct individuals to the relevant authorities (e.g., a Privacy or Data Protection Commissioner, industry association, or seal program), if you cannot resolve the complaint to the individual's satisfaction. Alternatively, make available third party dispute resolution mechanisms on an optional basis. Such processes should be accessible, affordable, fair and impartial for all parties.



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