Privacy & Information Technology Paper

Implementation & Operational Guidelines

Prepared by The External Liaison Committee, Canadian Information Processing Society August, 1997

Approved by The CIPS National Board of Directors October, 1997

To download a .pdf copy of this report, please click here.

Table of Contents

Preface

This report contains commentary and guidelines pertaining to the implementation of the Canadian Standards Association's (CSA's) Model Code for the Protection of Personal Information (Model Code). The CSA owns the copyright on the Model Code. The CSA has

given permission to the Canadian Information Processing Society to use portions of the Model Code in this report. The CSA portions of this report are printed in italics.

The Canadian Information Processing Society is responsible for the commentary pertaining to each CSA principle.

Acknowledgements

A report of this nature builds on the contributions of those that have contributed in the past. The Canadian Information Processing Society wishes to thank Ted Barnicoat, I.S.P., who developed the Society's 1988 guidelines on this topic: The Protection of Privacy in Information Systems: Operational Guidelines. Attesting to the quality of that report, certain portions of that report appear verbatim in this report.

The Society would also like to thank the Canadian Standards Association for granting permission to reproduce their model privacy code in this publication. The Society recognizes the difficulty of developing consensus on these issues.

The Society would also like to thank John Boufford, I.S.P., Past President of the CIPS Kawartha Section and Member of the External Liaison Committee, for his efforts as the principal contributor to this position paper. He has been an invited speaker on privacy issues at two national conferences during 1997, and is the CIPS delegate to the Standards Council of Canada's working group to determine Canadian views on the need for an ISO privacy standard. John brought to this project, an understanding of both information technology and privacy issues.

Finally, CIPS would like to thank its Members and others who took the time to comment upon the draft version of this paper.

Executive Summary

Privacy is a human right which means different things to different people. To some, privacy is synonymous with confidentiality. To others, privacy is the right to be left alone or remain anonymous.

There is a renewed emphasis among businesses, information technology practitioners, and privacy advocates to deal effectively with the issue of privacy, although each may be approaching the problem from a different perspective. Business is justifiably concerned about the so-called European Directive which will prohibit the transfer of personal information from a European country unless the receiving country also has a data protection scheme. This would put Canadian businesses at a competitive disadvantage in the global marketplace.

Members of the Canadian Information Processing Society (CIPS), all of whom are information technology professionals, may be confronting the issue of privacy because it is an ethical issue, or because their employer is bound by a legislated or voluntary privacy scheme. And the privacy advocate - he or she is trying to pursue the advancement of a fundamental human right.

This report deals with the issue of "informational privacy" or "fair information practices". The privacy principles are taken from the Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information. This CSA Model Code - a voluntary code - was developed with broad consultation and participation of industry and other stakeholders. The CSA principles, as they relate to information technology, are described in this report.

Through the liberal use of examples, this report attempts to improve the information technology professional's understanding of privacy, and to provide guidance pertaining to the implementation of the privacy principles within information systems. Other key objectives of this report are:

- to remind CIPS Members that the adoption of these privacy principles is linked to their Code of Ethics;
- to raise awareness that there are tangible benefits which can be derived from implementing the privacy principles;
- to raise awareness that there are significant commercial opportunities for companies that develop software which is sensitive to the privacy concerns of an informed public, or that develop privacy-enhancing technologies.

There is a general perception that implementation of the privacy principles is a costly business overhead. However, the principles can be implemented with little overhead beyond that required for efficient information management practices. Furthermore, the implementation of these practices may reduce operating costs, and actually increase market share for those companies which are sensitive to the privacy concerns of an informed public.

Summary of the Canadian Standards Association Model Privacy Code Principles

The Canadian Standards Association Model Privacy Code consists of ten inter-related principles. These principles are prescriptive in nature. Since this privacy code is linked to the CIPS Code of Ethics, those principles that contain the words "must" or "shall" reflect the minimum requirements.

The major principles follow.

- **Principle 1: Accountability**
  An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

- **Principle 2: Identifying Purposes**
  The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

- **Principle 3: Consent**
  The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

- **Principle 4: Limiting Collection**
  The collection of personal information shall be limited to that which is necessary for the purpose identified by the organization. Information shall be collected by fair and lawful means.

- **Principle 5: Limiting Use, Disclosure, and Retention**
  Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

- **Principle 6: Accuracy**
  Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

- **Principle 7: Safeguards**
  Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

- **Principle 8: Openness**
  An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

- **Principle 9: Individual Access**
  Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

- **Principle 10: Challenging Compliance**
  An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Background

The emergence of the information highway, in its broadest sense, is one of those rare events which has the ability to reshape society in ways which are as fundamental as those attributed to Gutenberg's printing press. The information highway has the potential to unleash unforeseen benefits to society as well as providing an infrastructure for secure business transactions. However, if society does not soon come to grips with issues of human rights and how individuals interact with each other on the 'net, we may very well lose the best, and perhaps the only, opportunity to create a cyberspace which reflects society's values.

This paper describes guidelines and responsibilities for the implementation of the Canadian Standards Associations Model Code for the Protection of Personal Information as it relates to information technology.

This paper is not the first position that CIPS has developed on the issue of privacy and information technology. Rather it is a revision of an earlier position paper, which has been developed as the regulatory environment, and our understanding of privacy, has evolved.

In 1987, the Canadian Information Processing Society (CIPS) approved and adopted the 1980 Organization for Economic Cooperation and Development (OECD) guidelines on the Protection of Privacy and Transborder Flows of Personal Data. One influencing factor in the CIPS recognition of the Guideline was the leadership of the Government of Canada (proclamation of the federal Privacy Act, adoption of the OECD Guideline, and their call for a voluntary response from industry).

In 1988, the Society approved an operational guideline on The Protection of Privacy in Information Systems to assist Members in complying with its amended Code of Ethics. In this way, CIPS linked a moral/ethical issue to its own self-regulating process.

Since that time, several provinces have enacted legislation which provides for protection of privacy in the public sector.

In 1994, Quebec became the only jurisdiction in North America to enact a data protection scheme which provides for privacy of personal data in the private sector.

In 1996, the Canadian Standards Association published a model privacy code and the Canadian Bankers Association published a privacy code which is specific to that industry.

In September 1996, Justice Minister Rock announced that the federal government will enact privacy legislation which applies to the federally-regulated private sector before the year 2000.

Concurrent with these developments, advances in information technology have caused some public concern about real and perceived threats to their privacy.

As a result, the Society called for a review of its existing position on the OECD guidelines and its operational guidelines.

What is Privacy?

In his comprehensive 1989 work on privacy protection (note 1) , David H. Flaherty, the current Information and Privacy Commissioner for British Columbia, identified the privacy interests of individuals in information about themselves. These are:

- the right to individual autonomy
- the right to be left alone
- the right to a private life
- the right to control information about oneself
- the right to limit accessibility
- the right of exclusive control of access to private realms
- the right to minimize intrusiveness
- the right to expect confidentiality
- the right to enjoy solitude
- the right to enjoy intimacy
- the right to enjoy anonymity
- the right to enjoy reserve
- the right to secrecy.

This understanding of privacy is important since other privacy concepts (e.g., confidentiality, limiting accessibility, etc.) remain in effect even after an individual has consented to the collection of personal information for specific purposes.

While privacy is a right, it is not an absolute right. In some cases, society has determined that societal benefits outweigh the privacy rights of the individual. In these cases, governments have created public records. In other cases, an individual's right to privacy must be balanced against the legitimate data collection requirements of law enforcement and national security. In yet other cases, individuals may choose to waive certain privacy rights in order to obtain a benefit such as a credit card, mortgage, or a government service.

Privacy touches on all aspects of our lives. Notwithstanding the pervasive nature of privacy, adequate privacy protection does not seem to be fully implemented in business information systems. Certainly, information systems professionals are quite comfortable incorporating access controls and other technical security features into information systems. However, privacy protection encompasses much more than the implementation of information technology safeguards.

In the field of information technology, privacy protection can be achieved through "fair information practices". These practices provide for some equity between the data subject (i.e., the individual to whom the information relates) and the organization that is collecting and using that individual's personal information. Fair information practices, which are sometimes codified in legislation, provide for certain standards in the collection, use, disclosure, accuracy and disposal of the data subject's personal information. A right of access and correction is also a basic requirement.

What is Personal Information?

The Canadian Standards Association defines "personal information" as "information about an identifiable individual". This definition is quite broad and would include for example, information about the individual's telephone number which is generally publicly available, as well as sensitive information about individual's age, sex, sexual orientation, medical, criminal and educational history, or financial and welfare transactions. Personal information would also include biometric information, such as blood type, fingerprints, and genetic makeup. This list is not intended to be complete.

This paper uses the terms "individual", "person" and "data subject" interchangeably.

What is the Problem?

> "Privacy is not now and never has been primarily a technical problem; rather, it is a management problem. There are sometimes management solutions to technical problems; there are NEVER technical solutions to management problems."
> - Adapted from a presentation on Distributed Heterogeneous Security Management,

November, 1992. Source otherwise unknown.

The problem is that privacy is a cultural value which is not universally held in high regard. Arguably, some industries knowingly collect personal information in a manner which is inconsistent with fair information practices because that is the nature of their business, or because, in their view, the collection "levels the playing field" when they deal with potential clients. One need only review the agendas of conferences and seminars which feature data warehousing and data mining topics to realize that this is a growth area which threatens individual privacy. As a result, there is a pressing need for a better understanding of privacy and adherence to fair information practices.

Another aspect of the problem is the transborder flow of personal information in support of global business activities. The European Economic Community has enacted legislation which will prohibit the transfer of personal information to another country unless the receiving country also has a data protection scheme. In the global economy, Canadian businesses wanting to do business in Europe could find themselves at a disadvantage if Canada does not have a data protection scheme which applies to the private sector.

Prior to the wide spread use of information technology and the explosive growth of the internet, privacy was protected through the inefficient search and retrieval techniques that were available. Data matching was impractical since manual search methods would have to be employed. Now computer matching and profiling is more common than most individuals would prefer.

Some examples might help to illustrate the problem. Many people use personalized cards in the supermarket in order to obtain in-store discounts and to obtain cheque cashing privileges. When the card is passed through the reader, the individual leaves a data trail about his or her purchases which could be used for target marketing, product research, and creation of lifestyle databases about the data subject. The latter use could conceivably be used by insurance companies to determine the data subject's eligibility for life insurance (e.g., the person's diet is too high in cholesterol).

In the United States it has been reported (note 2) that more than 100 property-insurance companies are using credit ratings from credit reports, not to determine whether a person can pay the premiums, but to determine whether he or she is a good risk. According to a consumer columnist, "They [insurance companies] claim that people who don't pay their bills are more likely to file a theft, fire, or accident claim".

The issue here isn't one of whether these uses should be permitted. Barring those instances where the collection or use is illegal, adults should be able to, and indeed do, make informed choices about their privacy. The issue is one of fair information practices and the obligation of the company to comply with privacy principles such as those set out in the CSA's Model Code.

Privacy intrusions also result when inadequate safeguards are applied to the information management life cycle. For example, when an individual has had his credit card stolen, the individual will challenge the amount owing and not pay the offending charges. The individual's credit report will reflect that fact. Reports from the United States indicate that when the

individual repairs his credit record at the credit bureau, the individual assumes that the damage has been rectified. However, the following month the amounts owing on the stolen card still have not been paid. The credit granter downloads new information about the delinquent accounts and the individual's credit history is again incorrect. And so the cycle goes. It is in the best interest of business to maintain an accurate record. Therefore, this privacy intrusion could have been easily avoided if the system had been designed with a view to maintaining data integrity and to protecting the privacy of the individual.

Without trivializing the very real threats to an individual's privacy, the issue of privacy also presents opportunities. There is a strategic advantage to be gained by companies that accommodate the privacy concerns of an informed public. There are also reports emerging from Quebec, that companies that implement data protection schemes in conjunction with improved information management practices reduce their operating costs either through cost reduction or increased productivity (note 3).

Very real opportunities also exist for information technology workers who develop technologies to enhance privacy. Some of these technologies include encryption, biometric encryption, and anonymous payment systems. Or from another perspective, John Hagel III and Jeffrey F. Rayport, writing in Harvard Business Review, predicted that consumers will take control of their personal information and will market it in exchange for enhanced services or profit. (note 4) The information-rich data will be collected by the consumers themselves (in their personal accounting systems, web browser, or other software) and made available to vendors where the consumer wants enhanced services. From a theoretical perspective, this is a problem because the consumers themselves are reduced to a commodity. But from another perspective, the consumer decides for himself whom he will share the information with. The underpinnings of privacy are predicated on that control. Software developers might want to capitalize on this important concept.

Voluntary vs. Regulatory Data Protection Schemes in Canada

In Canada, there is a patchwork of legislated privacy schemes. The federal Privacy Act (1983) provides for the protection of personal information in the federal public sector. Several provinces and territories (i.e., Alberta, British Columbia, Manitoba, Newfoundland, Northwest Territories, Nova Scotia, Ontario, Quebec, and Saskatchewan) have enacted public sector privacy legislation. These data protection schemes apply to different public bodies in each jurisdiction. Government departments and their agencies are normally subject to the legislation. Less commonly, municipalities, school boards, hospitals and professional bodies are bound by the legislation. The British Columbia Act also applies to many self-regulating professions.

New Brunswick is currently conducting public hearings with respect to a proposed privacy act.

Quebec is unique in North America because it is the only jurisdiction which has a legislated privacy code - An Act Respecting the Protection of Personal Information in the Private Sector - which applies to the private sector.

There is also a plethora of other legislation which applies to the collection, use and disclosure of medical and other personal information.

In all cases, readers should seek appropriate legal advice about the requirements of regulatory privacy schemes which apply to their industry.

In the absence of legislated privacy requirements, a number of voluntary privacy codes - all based upon the OECD Guidelines - have emerged in Canada. The Canadian Standards Association approved a Model Code for the Protection of Personal Information (CAN/CSA Q830-96) in 1996. The CSA Model Code may become the framework for the proposed federal privacy legislation which will apply to the private sector.

As noted above, Canada seems to be moving in stages towards a legislated data protection scheme. One Canadian jurisdiction (i.e., Quebec), and government agencies in several provinces already work under a legislated data protection model.

However, these Guidelines deal with implementation of the Canadian Standards Association's Model Code for the Protection of Personal Data - a voluntary code - as it relates to the information technology profession. This Code is similar in principle to legislated data protection schemes. Where there is a legislated privacy scheme, these operational guidelines are a useful aid in implementation.

CSA Model Code for the Protection of Personal Information Principles
CSA Principle 1: Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The

organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

1.4 Organizations shall implement policies and practices to give effect to the principles, including:

a. implementing procedures to protect personal information;

b. establishing procedures to receive and respond to complaints and enquiries;

c. training staff and communicating to staff information about the organization's policies and practices; and developing information to explain the organization's policies and procedures.

Commentary

The successful implementation of the privacy principles depends, in large part, upon the direct involvement of a "champion" or "sponsor". For the purposes of this report, the designated individual in Principle 1, is the Chief Information Executive.

The Chief Information Executive is responsible for the management and coordination of the information resources policies and procedures of the organization. This position must have authority, and a voice that is heard by executive management. Because of the real cost to the organization of breaches of security and privacy, this individual must have a good general knowledge of business functions of the organization, as well as an in-depth knowledge of information management techniques, computers and telecommunications.

In large organizations, responsibility for this function will be at the vice-president level. Smaller organizations may combine this function with the responsibilities of another executive. This individual should have the following responsibilities:

- Establish and update information protection policies and procedures, including those dealing with the protection of privacy, for executive approval. These policies must permeate every activity and program area in the organization. They must be reflected in the electronic environment, filing cabinet, desk drawer, and the manner in which employees generally deal with personal information in the workplace. Policies should clearly assign responsibilities to systems analysts and programmers, computer operations staff, security officers, information auditors, suppliers, and information custodians and users.

- Prepare privacy impact assessments of both current and proposed information systems.

- Ensure that the organization's privacy policies and practices are implemented by other organizations to which data processing functions are out-sourced.

- Establish the criteria for the classification of information and assist information custodians to classify the information in their management areas according to these criteria.

- Undertake an information classification study, and review it regularly to ensure that the classification of all information reflects its current value and sensitivity.

- Provide information on the information assets of the organization, their classification, accessibility, location and custodian.

- Maintain an access list for information users and review it regularly to ensure that access is provided to sensitive information on a need-to-know basis.

- Evaluate the physical and logical accessibility of all sensitive information, especially automated information, and ensure that corrective action is taken where necessary.

- Provide education to the organization on the importance of information protection.

- Stay abreast of technical and legal developments in this field in order to enable management to maintain the highest reasonable security standards and to minimize the organization's exposure to liability.

Information technology professionals are responsible for implementing the CSA Model Code (or privacy legislation which is applicable to that organization) in projects in which they are involved. When these principles cannot be reasonably implemented, the I.T. professional should advise the Chief Information Executive in writing.

All Members of CIPS are required by their Code of Ethics to identify to the organization's Chief Information Executive, situations where those projects for which the CIPS Member is accountable are not in compliance with the CSA Model Code or privacy legislation that is applicable to that organization.

CSA Principle 2: Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

2.1 The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Principle 8) and the individual access principle (Principle 9).

2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Principle 4) requires an organization to collect only that information necessary for the purposes that have been identified.

2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be orally or in writing. An application form, for example, may give notice of the purposes.

2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Principle 3).

2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

2.6 This principle is linked closely to the Limiting Collection principle (Principle 4) and the Limiting Use, Disclosure, and Retention principle (Principle 5).

Commentary
Identifying purposes for the personal information which is to be collected allows organizations to focus their data collection on only that information which is necessary for the stated purposes, or to find alternatives to the collection of personal information. This is critical to effectively limiting collection (principle 4). This should not be viewed as a constraint on the organization. Since data collection and maintenance is expensive, "identifying purposes" is the first step in reducing operating costs.

CSA Principle 3: Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing the personal information.

3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

3.2 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

3.3 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

3.4 The form of consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a magazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

3.5 In obtaining consent, the reasonable expectations of the individual are also relevant.

For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that the information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

3.7 Individuals can give consent in many ways. For example:

a. an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

b. a check off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

c. consent may be given orally when information is collected over the telephone; or

d. consent may be given at the time that individuals use a product or service.

Commentary

Informed or enlightened consent is the underpinning of fair information practices. Sometimes the purpose for which the information is collected is obvious. For example, an individual that inserts a long distance card into a telephone reasonably expects the telephone company to use the personal information for the purposes of billing the card holder. This purpose so closely aligns with the data subject's expectations that consent can be implied by their act of inserting the card into the telephone. Nonetheless, the individual has a right to know what the principle purposes of the collection are, or indeed that there are no other intended purposes for the information. Therefore the application which the individual completes in order to obtain the card should identify the purposes.

Notwithstanding the need for enlightened consent, the list of purposes need not be so inclusive that individuals will not read or comprehend it. Simple statements, which are not designed to mislead the reader, may imply certain consistent purposes. For example, a statement that personnel and payroll information is used for the purposes of human resources management, would include purposes such as disclosure to the individual's manager for performance management purposes, disclosure to a staff or external lawyer when the information relates to a

grievance, and disclosure of payroll information to Revenue Canada for taxation purposes, and to Employment Canada on the "separation certificate". Care must be taken to ensure that consistent purposes are reasonable and not contrived because this principle requires a full disclosure of purposes.

Consent can be obtained by any reasonable and convenient means. Examples include printed notices on applications, or poster displays at entrances to premises, or on-line for internet transactions. However, in some instances, the law requires that consent be in writing.

Internet "cookies" violate this principle. Although the browser informs the user that the web site is attempting to send a cookie (assuming of course that the browser has that capability), and the user can refuse to accept the cookie, this acceptance or reject does not constitute consent. The primary reason for this is the cookie notification does not contain any description of the use or uses of the cookie, or who is collecting the information and how to file a complaint if the information is misused.

Individuals should have the opportunity to opt out of data collection and to request deletion of that personal information which has already been collected. In this case, the individual may be subjected to certain consequences because of this decision. For example, some credit granters may agree to an individual's request not to provide certain information to a credit reporting agency. However, in the absence of a credit history on file at the credit reporting agency, the individual might find it difficult to obtain further credit.

Clause 3.7(b) provides for individuals to withhold consent or "opt out" of secondary uses of personal information by checking a box. Individuals who do not check off a box which withholds consent would be assumed to have consented to the secondary use.

From a privacy perspective, this method of opting out is contentious. According to a major survey of Canadian privacy attitudes, the public does not want their personal information sold for direct marketing purposes. The public view is that privacy should be the default condition and explicit consent should be obtained for secondary uses.

The use of a checkoff box to opt out is analogous to the reverse-marketing option, where the onus is on the individual to opt out of new services for which he might be charged. The extent of public aversion to the reverse-marketing option can be gauged by the cable television example of a couple of years ago. In that situation, the cable industry had intended to charge customers for services which the customers had not explicitly cancelled. As a result of the negative public reaction, the cable industry reversed its marketing strategy. The Chief Information Executive might want to weigh the implications of a checkoff box for opting out purposes very carefully.

Surreptitious data collection, except where explicitly permitted by law, is intrusive, unethical and contravenes the CSA Model Code. For example, collection of information by internet web sites about their client's interests (as inferred from the web sites visited) is unethical unless the clients are advised about the collection, and consent to it, prior to the collection taking place. An unsuspecting public does not expect this data collection.

CSA Principle 4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purpose identified by the organization. Information shall be collected by fair and lawful means.

4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations should specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Principle 8).

4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which the information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.3 This principle is linked closely to the Identifying Purposes principle (Principle 2) and the Consent principle (Principle 3).

Commentary

Collection of personal information is always intrusive. However, for some purposes, individuals may choose to trade off some of their privacy in order to gain a certain benefit. For example, an individual may reveal information about their income, assets and expenses in order to allow a lender to determine their credit worthiness. As a result, the CSA Model Code only permits the collection of information which is necessary to perform a serious business function.

In some cases, the collection of personal information is illegal or questionable at best. For example, collection of information about age, sex and marital status on an employment application would contravene the applicable human rights code. In other cases, collection of information about household income is entirely unrelated to activities such as product warranty registration. And certainly, the collection of household information from children that visit internet sites is unjustified.

The public is quite concerned about the private sector collection and use of information about the public, and its retrieval by some form of government-provided identifier, such as the social insurance number. Such techniques allow databases which have been collected for unrelated purposes to be linked in ways which are subject to unacceptable rates of error. Alternatives to collecting, storing and retrieving personal information by government-provided identifiers are now available. However the application of these alternatives may not be robust enough to generate unique database identifiers for all applications. Nonetheless, these alternatives do have a place in the arsenal of the well-informed analyst.

Monitoring of employees, through the use of programs that record employee keystrokes or by displaying the contents of an employee's computer screen, or by screening of e-mail or voice mail, should be limited, or preferably avoided. Employee surveillance violates employee's privacy and erodes employee trust and productivity. In some cases, this surveillance could contravene the Criminal Code of Canada.

Because some employees have downloaded pornography to their workplace computers, some employers are advising employees that their company electronic mail will be monitored. Part of the reason for this surveillance seems to be to protect the employer against criminal charges. This is a dangerous practice. There are certain positions in every organization that are involved in highly sensitive or confidential work. Some of these positions include employee counsellors, workplace harassment advisors, and auditors who conduct internal investigations. The public may deal with certain of these employees on a confidential basis, and the public certainly would not be aware of a company policy to monitor e-mail or voice mail.

The recommendation here is to exercise caution. Once employee monitoring is initiated, it is very hard to protect the integrity of confidential programs.

Another form of surveillance is particularly insidious. Computer logs and lists of various forms (e.g., resource accounting information, network logs, etc.) at first appear innocuous because of the apparent insignificance of each piece of information. However, when combined, these logs can reveal lifestyle patterns and interests about the individual (e.g., the clients of an internet access provider). All forms of computer logging should be deactivated except where the information is necessary for the fulfilment of a serious business purpose (such as billing for services), or where the deactivation will inhibit the efficient operation of the system. At any rate, this background data collection must conform to the principles set out in this document.

Systems analysts should consider the business objectives of data collection. In some cases, the business objective can be satisfied without collecting personal information. For example, where card readers are used by transportation companies instead of tokens, it may not be necessary to collect information about the travel patterns of the individual card holder. The basic information which is required consists of whether the individual is authorized to make the trip, and for capacity planning purposes, that an unidentified person boarded at one point, departed at another, and the time and date of the trip. Anonymous demographic information might also be required for marketing and planning purposes.

The preceding has focused on privacy threats, nuisances and solutions. From a perspective of business efficiency, it is advantageous to collect only that information which is necessary for a serious business purpose. These are some reports coming out of Quebec, that companies that have implemented that province's data protection scheme are experiencing reduced costs for data collection and maintenance (note 3).

The following should be considered systems development best practices with respect to "limiting collection":

Consider privacy as a user requirement and throughout the systems development life cycle. It is always less expensive than retrofitting the capability.

Analysts should rigorously question whether the collection of personal information is "necessary".

Avoid collecting common identifiers (such as social insurance numbers, driver's license numbers, etc.) unless their use is consistent with the original purpose of the identifier.

CSA Principle 5: Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

5.1 Organizations using personal information for a new purpose shall document this purpose (see Clause 2.1).

5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

5.3 This principle is linked closely to the Identifying Purposes principle (Principle 2) and the Consent principle (Principle 3).

5.4 This principle is closely linked to the Consent principle (Principle 3), the Identifying Purposes principle (Principle 2), and the Individual Access principle (Principle 9).

Commentary
Access to personal information within an organization must be allowed only on need-to-know basis. Generally speaking this should be based upon a two-part test:

- the employee must need access to the information in the performance of their duties; and
- the access by the employee must be in support of a legitimate business function of the organization (i.e., they must not use their access privileges for personal reasons).

Computer matching generally involves a search of computer records in two or more databases which have been collected for different purposes, in order to identify individuals based upon the occurrence of some personal identifier (e.g., social insurance number) which exists in both databases. Data profiling involves searching one or more databases to identify certain individuals

based upon a characteristic other than a personal identifier (e.g., list all individuals in a certain postal code that drive a certain make of car).

Computer matching and data profiling are intrusive for two reasons. First, the underlying assumptions in the data may make the results of the "matching" or "profiling" activity invalid. In one commonly cited case, a state government matched welfare records with banking records and, without further verification, discontinued welfare benefits of thousands of people that had sizeable bank accounts in their name. About one-third of the individuals that had their benefits discontinued, had been disqualified unjustly. As it turns out, welfare recipients may have bank accounts in their name but the money is not theirs (e.g., they may be the executor of an estate).

The other, and more important, reason for the intrusive nature of computer matching is that the data sources for a computer matching activity are often assembled for purposes other than the matching activity. In that case, the matching activity probably violates the consent principle.

Therefore, computer matching and data profiling activities should be initiated only after the completion of a business case which includes a privacy impact assessment, identification of the techniques which will be used to validate the result of the matching or profiling activity, and the method of notifying the individuals prior to taking action against them. The business case must be approved by the Chief Information Executive.

Public records are usually created by government agencies for some purpose which benefits society. For example lists of electors are made public so that individuals can determine if they have been enumerated, and to detect bogus enumerations. Land title information is public so that individuals can determine who the registered owner and lien holders are on a given property.

Other records are public by custom. For example, telephone directories for cities have been publicly available for many decades.

However, a record may be public in one context but not another, nor for all time. For example, a lottery winner agrees to the publication of their name when they win sizeable sums of money. But most winners would object to the lottery organizers subsequently providing lists of winners to financial planners. The use is not consistent with the context in which the record is public.

Nor would the public expect land title information to be available in a manner in which all properties, along with their value and the initial balance of the mortgage, would be retrievable by the name of the owner. There is a public benefit is retrieving the information by property description. When the information is available by the name of the owner or mortgagor, the disclosure becomes intrusive and, in some cases, a threat to physical security. Again, the purpose is not consistent with the purpose for which the original record was made public.

After considering these factors, public records should only be used for purposes, and in formats (e.g., single record, entire database, etc.), which are consistent with the original purpose. The Chief Information Executive is accountable for approving all consistent uses of public records.

This principle also deals with issues of records retention and destruction. Organizations should develop policies regarding the retention of records (production database and e-mail records). This retention period must be long enough to allow individuals an opportunity to exercise their right of access under principle 9. Once this retention period expires, the information should be destroyed in a manner which prevents its recreation.

CSA Principle 6: Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.2 An organization should not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be up-to-date, unless limits to the requirement for accuracy are clearly set out.

Commentary

> "An 81 percent success rate is pretty good if you're shooting basketball free throws. It's abysmally low when you're playing with people's lives."
>
> - Glenn Garvin in Reason magazine October, 1995, on the accuracy rate in the [U.S.] Immigration and naturalization Service's telephone employment-verification hotline (note 5)

Seemingly inconsequential data integrity issues can have significant impact upon the individual to whom the information relates. This CSA principle reflects the relationship between data accuracy and the intended use of the information.

When analyzing issues of accuracy, consideration should be given to possible misuses of the information. For example, in the United States, some credit reporting agencies update the data subject's address based upon the address provided during the last query to the credit database. Reportedly, the system will even accept an address which is used for test purposes within the credit bureau (note 6). This practice of not ensuring data accuracy before updating a database would certainly not meet commonly accepted standards for verifying data, and is a major contributor to the problem of theft-of-identity in the U.S.

Insofar as is possible, personal information should be collected directly from the data subject. This normally improves the quality of the information collected.

Business decisions must be based upon all of the relevant information about the individual. An online system which only maintains a portion of the relevant information denies the individual to a fair assessment of their eligibility for a service or benefit. For example, a credit history file which only records information about payments and amounts owing might not meet the test. Individuals sometimes legitimately disagree with company records. If the individual files a statement of disagreement, and the letter is put in a paper file, credit granters will make their decisions, and probably deny credit, without the benefit of complete information.

CSA Principle 7: Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 3.4.

7.3 The methods of protection should include

a. physical measures, for example, locked filing cabinets and restricted access to offices;

b. organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

c. technological measures, for example, the use of passwords and encryption.

7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

Commentary
Information technology professionals have a special relationship with their organizations. As the gatekeepers to the system, they have the ability and knowledge to access any information on the system. They must discharge their duties in both a legal and ethical manner.

Information technology professionals have been designing and implementing security and access controls for many years. These security measures are normally commensurate with the risk of disclosure.

Privacy is compatible with technology. The following paragraphs briefly describe technological tools and system design techniques which enhance privacy in certain circumstances.

Strong encryption is now available which can prevent unauthorized access or disclosure. As a minimum standard, sensitive personal information should be encrypted when it is transmitted over a network.

Biometric encryption is a technique where a biological features of the individual (e.g., retina scan, fingerprints, etc.) are mathematically codified and then that code is encrypted. Biometric encryption is useful where there is a significant potential for abuse of a service if the identity of the individual is not substantiated. The biometric feature uniquely identifies the individual. Encryption prevents many secondary, and unauthorized, uses of the information. Care should be taken not to collect or use biometric information in an intrusive manner.

Transactions may be anonymous where there is no need to identify the individual. The best information technology example of this is the long distance telephone card which can be purchased in convenience stores, and is pre-loaded with long distance credits. It appears that other forms of anonymous payment cards and other schemes are emerging.

Where an identifier may be required for internal controls or to detect fraud, pseudo-identifiers may be an acceptable compromise. In this situation, the real identity of the individual is known only to one group in the organization. All transaction information related to the individual is stored using the pseudo-identifier as the key, thus minimizing dataveillance (i.e., surveillance of the individual through the data trail which he or she leaves behind after each transaction). For more information on maintaining anonymity in information systems, visit http://www.replay.com/mirror/privacy/p2.index.html

One safeguard that may be overlooked is deletion of data after the prescribed retention period. Personal information must be destroyed in a manner which prevents its recreation. A normal file deletion does not meet this requirement since several utilities are available to restore it. In order to satisfy this requirement, the file may be over-written (at least three times) or encrypted, or the media physically destroyed. Similar safeguards must be employed when personal computers are sent to suppliers for maintenance or when diskettes are used. Hardcopy files must be shredded.

CSA Principle 8: Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals should be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

8.2 The information made available shall include

a. the name/title and address of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

b. the means of gaining access to personal information held by the organization;

c. a description of the type of personal information held by the organization, including a general account of its use;

d. a copy of any brochures or other information that explain the organization's policies standards, or codes; and

e. what personal information is made available to related organizations (e.g., subsidiaries).

8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

Commentary
No specific information technology commentary is provided for this section except to reinforce that internet and intranet web pages are very effective for disseminating this information.

CSA Principle 9: Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirements should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to

make sensitive medical information available through a medical practitioner. In addition, the organization should provide an account of the third parties to which it has been disclosed.

9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

9.3 In providing an account of the third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization should provide a list of organizations to which it may have disclosed information about the individual.

9.4 An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge should be recorded by the organization. Where appropriate, the existence of the unresolved challenge should be transmitted to third parties having access to the information in question.

Commentary

Individuals have a right to know who has had access their personal information - hence the need to provide for access by the data subject. For example, individuals have a right to know which of the thousands of businesses in a community have accessed their credit history and to satisfy themselves that the access was for authorized purposes and consented to. Audit trails on "read transactions" should be used as appropriate.

Sometimes an organization is legally compelled to disclose personal information to another organization for purposes other than originally intended. These uses and disclosures are referred to as inconsistent use or disclosure. Organizations should record these inconsistent uses and disclosures in a database record which is linked to the original record. These inconsistent uses and disclosures can be easily recorded by making a separate entry point into the system or a separate menu selection.

The record keeping in the previous paragraph is necessary to meet the intended purpose of Clause 9.3 and it is not onerous if it is systematically collected by production information systems.

When using e-mail to provide for individual access, there is a problem in identifying that the complainant is whom they claim to be. Therefore, organizations should develop procedures for verifying the identity of the writer before granting access to the data subject.

Individuals sometimes disagree with the organizations interpretation of the information in their file. For example, a company may believe that an individual's performance was substandard and the individual may have an entirely different interpretation. Similar differences of opinion might occur in a credit history file. Where the organization is satisfied that the information is incorrect, it must repair the information in accordance with this principle.

In those instances where the organization does not agree that the information is incorrect, the individual should be able to file a statement of disagreement which is displayed to authorized staff each time the contentious record is displayed. This capability is not difficult to design into information systems.

This statement of disagreement is important from two perspectives:

- as noted in the above principle, it allows the organization to notify third parties of the unresolved challenge where appropriate;
- it also allows the organization to have full access to pertinent information when assessing the individual's eligibility for a service or benefit.

CSA Principle 10: Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance

10.1 The individual accountable for an organization's compliance is discussed in Clause 1.1.

10.2 Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint process should be easily accessible and simple to use.

10.3 Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint mechanisms. A range of these mechanisms may exist. For example, some regulatory bodies accept complaints about the personal information handling practices of the companies they regulate.

10.4 An organization shall investigate all complaints. If a complaint is found to be justified through either the internal or external complaint review process, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

Commentary

While organizations are responsible for establishing a complaint receiving mechanism, e-mail is not sufficiently secure for this purpose. Individuals should be advised, on the organization's website, how to submit complaints. If e-mail is used for this purpose, the e-mail should be encrypted by the browser. Lessons learned by an organization in the complaint resolution process provide insight into how to prevent complaints in other information systems. Without reference to the complainant, these solutions should become de facto user requirements in similar information systems.

Endnotes

Note 1. Protecting Privacy in Surveillance Societies: the Federal Republic of Germany , Sweden, France, Canada, and the United States by David H. Flaherty, 1989.

Note 2. PRIVACY JOURNAL. FTC: Credit Reports to Insure. September 1995.

Note 3. PRIVACY JOURNAL. Data Protection Saves Money by Pierrot Péladeau. June 1995.

Note 4. The Coming Battle for Customer Information by John Hagel III and Jeffrey F. Rayport. HARVARD BUSINESS REVIEW. January-February 1997. Pages 53-65.

Note 5. PRIVACY JOURNAL. September 1995.

Note 6. PRIVACY JOURNAL. Fraud Happens: Here's How. July 1996.