Canada sets the standard on implementing privacy codes

The Canadian Standards Association's initiative to adopt a privacy standard will be a world first if finally ratified this year. No other country has attempted to integrate the widely accepted "principles of fair information practice" into its standards-setting machinery (see PL&B Feb 1995 p.2), explains Colin Bennett in this edited version of his report summary.

The CSA Model Code for the Protection of Personal Information is being developed at a time when there is a growing debate about a range of innovative approaches to the protection of personal data on the "information highway."

The CSA Model Code has now been approved by the Technical Committee, and now needs only final ratification as a "standard." This should happen this year. No decision has yet been reached about a certification or registration procedure and debates are continuing within the CSA and within one of its branches, the Quality Management Institute (QMI).

The CSA standard might form the basis of federal framework legislation, as advised by the Canadian Direct Marketing Association. (PL&B Dec. 1995 p.7) This innovation raises, therefore, a number of challenging questions about the implementation of privacy standards that have never been fully addressed before.

Part One - Summary of CSA Model Code

Canada is one of the few advanced industrial states that has not passed comprehensive legislation governing the collection, use and disclosure of personal information by all private sector organisations. The public sector is relatively well regulated through the 1982 Privacy Act and corresponding provincial statutes. But, with the exception of the new Act respecting the protection of personal information in the private sector in Quebec (Bill 68), privacy protection in the private sector in the rest of Canada has emerged in an incremental and piecemeal fashion.

Existing private sector provisions

Most provinces have statutes protecting the collection, use and disclosure of credit-reporting information. The new Telecommunications Act (Bill 62) empowers the Canadian Radio-Television and Telecommunications Commission (CRTC) to regulate to protect privacy interests. A number of confidentiality provisions exist for personal information within other federal and provincial laws and regulations.

The principal response in most sectors has been to develop "voluntary" privacy codes of practice. However, the term "privacy code" describes a diversity of mechanisms. The five main types are: *Individual Company, Functional, Sectoral, Technical and Professional Codes.*

They also vary according to the extent of compulsion. Most operate within a complicated and fluctuating range of regulatory, international, technological, cultural, and business incentives. The term "voluntary" needs to be used with considerable caution.

An analysis of the major privacy codes existing in Canada bears out these differences.

The *Sectoral Codes* of the Canadian Bankers Association, the Canadian Life and Health Insurance Association (CLHIA), the Insurance Bureau of Canada, and Stentor are models designed by these trade associations for the membership to implement at the company level.

The *Functional Code* of the Canadian Direct Marketing Association gives the Association a greater role in mediating complaints and promoting consumer awareness, with a threat of expulsion of a member company for non-compliance.

The privacy policy of the cable television industry operates according to a *foundation model,* under which the Canadian Cable Standards Council administers cable television service standards (including privacy) under the oversight of the CRTC.

None of these codes, however, has any explicit statutory force, in contrast with the privacy codes developed under the mandate of legislation and the oversight of a data protection agency.

Codes of practice play a valuable role under a number of regulatory regimes. In the Netherlands and New Zealand, codes are negotiated according to the data protection principles in the respective statutes, approved by the respective supervisory agencies, and thus given the force of law. These systems are designed to combine the flexibility of

self- regulation with the force of legal sanction and redress.

Without such framework legislation, experience of code development and implementation in Canada is diverse. There is variability in the *regulatory conditions* under which codes have been promulgated, in the *scope* of coverage, in the *processes through which they have been developed,* and in the *implementation mechanisms.*

Four objectives for the CSA Model Code
Given these conditions, the CSA Model Code might attain four interrelated objectives:

1. to increase the *level of consistency* for the development and application of data protection policy,
2. to promote greater *consumer awareness* of privacy rights,
3. to provide a *yardstick* for the measurement of the adoption and implementation of data protection policy,
4. to promote an organisational ethos that *raises the level of responsibility* for personal information management.

These objectives guide the remaining analysis.

Part Two - Learning about privacy

Previous analysis suggests that a privacy policy should be based on a thorough review and understanding of the privacy implications of each service and product. This may involve an *information audit, a privacy analysis, and a technology analysis.* It may also involve *external consultation* with consumer representatives, with the offices of the federal and provincial Information and Privacy Commissioners, and with experts in privacy and data security. *Opinion polls and consumer focus groups* also sensitise organisations to wider perceptions and interests.

There is an advantage in developing a more consistent practice for the codification of an organisational privacy policy. A distinction may be drawn between the *Privacy Code,* a set of Operational Guidelines to translate the Code into practical advice for employees, and a *Statement of Consumer Rights* for external promulgation. Privacy policies also require *a training and implementation plan, a public communications programme, and periodic review.*

Consumer Awareness of Privacy Rights
Companies and trade associations, Information and Privacy Commissioners, public interest groups, the Better Business Bureaux, and labour unions might play a useful educational role.

The CSA Model Code obliges personal-data users to implement procedures that provide individual redress and participation. These include notifying data subjects of the reasons for the collection of personal-data and of permissible uses and disclosures. They also include procedures for the exercise of access and correction rights. Organisations are also expected to put procedures in place to receive and respond to complaints. Suggestions of effective mechanisms to allow individuals to access their data and challenge compliance are offered.

The Code also obliges organisations to obtain consent, implied or expressed, if information is to be used for purposes other than those identified at the time of collection (unless a legal requirement is involved). Opt-out provisions should be meaningful, easy to execute, offered as early as possible, regularly and voluntarily.

Accountability
The assumption of accountability requires the appointment of an individual who is responsible for the implementation of the principles. This may require a blend of experience in both consumer complaints resolution and personal information management. Organisations need to ensure that their combination of duties does not place these persons in situations where privacy interests are compromised by other demands. Moreover, privacy responsibility needs to be located at a sufficiently high level in an organisation to permit these interests to be articulated at the earliest stages of service and product development.

A range of other instruments may be used internally in order to ensure compliance with the privacy principles. Education and training programmes have proven successful in some larger organisations. Many financial institutions need regular signing of statements of compliance by all employees who access personal data.

Privacy audits can be used to educate employees about their obligations, rationalise information collection and retention with attendant cost-savings, evaluate the effectiveness of the standards, and anticipate potential complaints and

problems. Audits may be of four types: internal, external, external reviews of internal audits, and audit trails through computer programming to identify instances of unauthorised access.

Security Mechanisms

Security Mechanisms should be applied as appropriate to the sensitivity of the information. They include a range of technological, organisational and physical measures. Some of the most notable breaches of security could have been prevented by quite mundane and common-sense precautions, such as keeping offices and filing cabinets locked and changing computer passwords regularly. The recent commercial availability of public-key cryptography offers a solution that can anonymise personal data and permit verification of a range of personal data transactions.

Contracts can ensure a comparable level of protection while information is being processed by a third party in Canada or overseas. Canada's information highway is also a gateway to the global information infrastructure. Contractual mechanisms will play an increasingly important role in personal data protection, as direct contacts become fewer between individuals and those processing their personal information. The CSA Model Code can potentially improve upon the provisions within other "model contracts" for transborder data flows by providing a mechanism by which data importers in Canada could satisfy their contractual obligations to overseas exporters.

Part Three - Monitoring

Three different institutional mechanisms might be involved in the monitoring process:

Oversight Responsibility

The Offices of the Information and Privacy Commissioners might appear the most logical location for *oversight responsibility*, given the way that privacy codes have been developed in the past. These offices have developed the greatest expertise in privacy, and draw upon an unrivalled experience of balancing rights of the individual with demands of the data user. Any other option would be granting responsibility to an organisation that may have competing responsibilities.

Not all provinces have public sector privacy legislation with well-established oversight agencies. Such a significant expansion of the responsibilities of these offices would require amendments to existing legislation, with potential constitutional implications for federal/provincial jurisdiction.

Certification by the CSA

This second option is more applicable to "harder" product standards which are amenable to objective testing and verification programmes. There are areas of privacy protection (such as encryption, telecommunications products and smart-cards) where certification may have a place.

Registration

The CSA Model Code, is more properly described as a "softer" performance standard. It is therefore, more amenable to verification through the kind of registration process administered by an accredited Registrar such as the Quality Management Institute (QMI). There are interesting parallels between the privacy standard and the ISO-9000 series of quality assurance standards.

Three options for registration of the CSA Model Code are analysed: Registration with Annual Audits; Registration with Triennial Audits; and Registration to a Rating-System. Each has costs and benefits. The test of any registration system is to find a balance that will encourage adoption and implementation of the Code, but also prevent organisations from making symbolic claims that their privacy policies meet the standard.

Under any registration scheme it will be necessary to publish a *Privacy Register* of organisations that comply with the Code. This would establish a reliable method to evaluate the impact of the standard and to encourage a spill-over effect in different sectors. Organisations shown to be flouting the code may be de-registered.

In addition, it will probably be necessary to establish an ongoing Advisory Committee, representing the stakeholder groups. This might have the following functions:

1. to resolve interpretative issues when disagreements arise between the Registrar and the applicant
2. to review progress with registration
3. to review the CSA Model Code
4. to judge the validity of claims made by organisations, and

5. to advise on questions involving possible de-registration.

A system of formal registration to the Code by an accredited Registrar like QMI has a number of attractive features. Such a system *promotes a greater awareness of rights and obligations.* It encourages *greater organisational responsibility.* It *establishes a measurement and evaluation tool.* And it forces *a greater level of consistency to the same standard.*

On the other hand, no accredited Registrar in Canada currently has the expertise in privacy issues to tackle the enormous variety of complex and highly technical problems that will inevitably arise. It would be necessary for the Standards Council of Canada to begin to accredit Registrars in privacy, as well as privacy auditors. Also, in no registration scheme can the Registrar offer the direct resolution or mediation of complaints.

Evaluation

Ultimately, the success of the CSA Model Code will depend on the various incentives that might operate to encourage registration. It is possible to legislate for the Code, in the same way as happens for around one-third of CSA's other standards. This might occur as a result of scandal, or in response to the unintended market consequences of differential policies being applied within the same sector. It could occur at the provincial and/or the federal level.

Planning for the Future

These illustrations still envisage the building of privacy protection in a piecemeal and incremental fashion. Beyond this, the CSA Model Code could be the basis for more general framework legislation. Compliance with the privacy principles could be enforced and monitored in a number of ways. Registration to the CSA's privacy standard can complement almost any current or future provisions for personal-data protection, whether contracted or regulatory, sectoral or comprehensive. Moreover, it would establish an essential mechanism for compliance auditing, which many scholars have regarded as a necessity within the increasingly networked information highway environment of the future.

The success of the CSA Model Code will depend upon commitment from government, industry, and consumers. It necessitates a multi-faceted attack on the problem with involvement from a wider range of groups, agencies, and interests than has been the case in the past. The technical and managerial image of the standards-setting process should not be allowed to overshadow the fact that the CSA Model Code tries to protect nothing less than a fundamental and perennial value - the right to privacy.

Case Studies

The CSA Model Code, while being a voluntary instrument, is subject to a complicated and fluctuating set of pressures and incentives within different markets. The following scenarios attempt to show how fictitious organisations might be motivated to register to the CSA Model Code. *Collectively, these examples show how self-regulation may extend its reach and provide a variety of inducements to registration.* They are listed in an increasing scale of compulsion.

Moral Persuasion The CSA Model Code will, it is hoped, provide *the* common reference point for personal data protection in the private sector. Widespread publicity for the code should increase its visibility and promote a greater number of questions about why Organisation "A" does not have a compatible privacy policy. This may come from trade associations, consumer groups, labour unions, privacy experts and advocates, and from the media. "A" registers to the CSA Model Code because it is the "right thing to do."

The Desire to Avoid Adverse Publicity "B" is a direct marketing company under pressure because it is threatened by adverse publicity about its telemarketing practises. The print and broadcast media have begun to focus on "B"'s record under growing exposure from consumer groups, privacy advocates and Privacy Commissioners. Perhaps the CDMA might be exerting pressure to prevent "B" from tainting the otherwise responsible record of its members. "B" registers under the CSA Model Code to prevent further negative publicity that may harm its market share and/or profitability and taint the reputation of other companies within the sector.

Competitive Advantage "C" is a company in telecommunications, a highly competitive sector and one that is increasingly information-intensive. Most of its competitors have registered to the

CSA Model Code. It begins to see its competitors advertising their privacy-friendly practices and making the appropriate claims on its publicity material. "C" fears a loss of market share and determines that registration under the CSA Model Code is a small price to pay to be seen in the same socially-responsible light as its competitors. It registers to the CSA Model Code.

Referencing the Standard in Contracts "D" is a retail company that regularly uses the services of a credit-reporting agency to determine the eligibility for credit of applicants. The credit-reporting agency has determined that an easy way to enforce the contracts with its clients is to require them to be registered under the CSA Model Code. This also provides for more consistent contracts across the retail sector and provides greater assurances that the information on consumers' credit-worthiness is being used properly. Organisation "D" registers.

ISO-9000 Registration "E" is a financial institution that has come under pressure from many of its manufacturing clients to register to an ISO-9000 quality assurance standard. It decides to "kill two birds with one stone" by registering to the CSA Model Code at the same time as it undertakes a process of ISO-9000 registration with QMI. "E" is awarded IS-9000 registration and thus obliges itself to undergo the annual compliance audits from QMI. It may now be registered in the *Privacy Register.*

Contracting-Out of Government Services "F" is a private sector company that performs a wide range of analysis and data processing services for a government agency in British Columbia. Advised by the BC Information and Privacy Commissioner, the government agency realises it must ensure that the same fair information practices are applied by "F" as the agency applies to its own personal data processing under the BC legislation. The agency determines that the personal data are of sufficient sensitivity to require "F" to register under the CSA Model Code. It establishes this requirement in contract. The policies and procedures of "F" are sufficiently sensitive to privacy for it to decide that registration is a price well worth paying to retain the agency's business.

Pressure from Research-funding Agencies "G" is a university medical research unit in a province that does not have public sector privacy legislation covering institutions of higher education. "G" utilises highly sensitive medical and drug prescription data in its research. The Medical Research Council determines that all recipients of funding should register to the CSA Model Code as a convenient way to ensure adherence to its own ethical research guidelines, compliance with which it has neither the time nor resources to monitor. The same requirement could be established by the Social Sciences and Humanities Research Council (SSHRC) and by the Natural Sciences and Engineering Research Council (NSERC).

Interprovincial Pressures "H" is a life insurance firm with headquarters in Quebec. It regularly needs to send information about its customers to its offices in other parts of Canada. Section 17 of Bill 68 stipulates that enterprises that send information about citizens residing in Quebec to anyone outside Quebec must "take all reasonable steps to ensure that the information will not be used for purposes not relevant to the object of the file." The Quebec Commissioner may determine that the most effective way to enforce this is to require the recipient to be registered to the CSA Model Code, judging the appropriate level of registration according to specific circumstances. The CLHIA advises its members outside Quebec to register to the Code as the most effective way to ensure the continued free flow of such information interprovincially.

International Pressures "I" is an airline with an office that holds data on its British employees in London. The UK Data Protection Registrar, under both the 1984 Data Protection Act, and the recently passed EU Directive, advises "I" that it may not transfer data on its British employees for processing in Canada, because it cannot ensure an "adequate level of protection" for the data in its headquarters in Ontario. The Registrar advises "I" that the European Commissioners have agreed that adequate protection in Canada can only be guaranteed if the company is registered under the CSA Model Code. The airline registers.

***Implementing Privacy Codes of Practice* by Associate Professor Colin J. Bennett, Dept. of Political Science, University of Victoria, Canada Contact: CSA Standard Sales, 178, Rexdale Blvd, Etobicoke, ON, M9W 1R3 Canada. C$40.00 (code PLUS 8830). ISBN 0921347448**