Privacy standards: an innovation in national and international policy

It is only rarely that a true innovation enters the world of privacy and data protection. Colin Bennett, Associate Professor, University of Victoria, British Columbia, Canada, explains.

The network of commissioners, officials, advocates, academics and others that make up this diverse and amorphous policy community have generally got used to the idea that the only conceivable way to protect personal data is to establish a legislative framework based on the familiar "fair information principles," and to secure its implementation under the oversight of a small data protection agency.

A few years ago, the advent of public-key encryption questioned some of the traditional assumptions behind data protection. It is now commonly agreed that "privacy-enhancing" technologies offer an indispensable tool for the international data protection community. Can the same be said about the latest innovation - the privacy standard?

The traditional role for standards

Standards have always played a very peripheral role in the protection of personal data, and have generally been confined to more technical standards for data security and the like. With the agreement and publication of the Canadian Standards Association's Model Code for the Protection of Personal Information, however, the potential for a broader privacy standard now demands careful consideration. For this too is a potentially important innovation in the history of the privacy protection movement.

In 1992, a number of different motivations persuaded representatives from government, consumer groups and business to meet under the auspices of the Canadian Standards Association (CSA) to negotiate a *Model Code for the Protection of Personal Information.*

Advantages to government, business and consumers

For the government participants, the CSA offered a useful arena for consensus-building, a way to by-pass controversial constitutional debates and a potential method to forge an accommodation that might form the basis for future national legislation.

For business, the CSA process provided the opportunity to develop a common yardstick for the development of voluntary codes of practice, a way to harmonise rules across provinces and sectors, and also, it must be said, a way to avoid regulation.

For consumer groups, the CSA code offered a more effective instrument for redress, and a potential method to certify business practices to a common standard.

These various incentives were sufficiently strong to overcome periodic conflicts along the way. The *Model Code* was agreed to without dissent in September 1995, subsequently ratified by the Standards Council of Canada, and formally published in March 1996 (PL&B April '96 p.1).

Current status of the CSA Model Code

At the moment, the *CSA Model Code* is little more than a Canadian-made version of the OECD Guidelines. It rearranges, updates and translates the key privacy principles into the Canadian context. It offers a model (supplemented by a comprehensive and practical Workbook) that any organisation or association can use and adapt to their specific circumstances.

The negotiation of the standard did serve a valuable educative function, and it has established an agreed consensus of the basic principles. The existence of this consensus undoubtedly influenced the decision of the Canadian Direct Marketing Association to call for national privacy legislation in October 1995, and cleared the way for the Industry Minister to announce in May 1996 that the government would "bring forward proposals for a legislative framework governing the protection of personal data in the private sector."

How a standard differs from a code of practice

The major element that distinguishes the *CSA Model Code* from other codes of practice, however, is that it is a *standard* that can be integrated into the certification and registration systems implemented through national and international standards bodies. It therefore offers a more common yardstick and can act as a more effective instrument to monitor the claims made by

organisations about their practices. In the same way that a company might be forced by market or regulatory pressure to register to an ISO 9000 standard to convince its clients and customers that it offers a level of "quality assurance," a similar system of accreditation could be developed to the privacy standard. Then we could obtain a more accurate picture of which companies have adopted privacy-friendly practices, and which have not. The price of maintaining registration to the standard would be an agreement to be subjected to regular and independent privacy audits.

Establishing a registration scheme

The Quality Management Institute (a division of CSA) is currently developing its own registration system to the privacy standard. If a credible registration process is established, the *CSA Model Code* ceases to be a "voluntary" mechanism for any organisation that decides to register. Organisations would have to produce a code of practice, and related set of operational guidelines and be subjected to regular and independent auditing of their practices. Such a system would build a more consistent and credible verification process than occurs at the moment. In addition, it would offer greater reassurance that the claims made in publicity and in contracts are in fact reflected in the practices of the organisation.

"The price of maintaining registration to the standard would be an agreement to be subjected to regular and independent privacy audits"

Registration to a privacy standard

Privacy, of course, is not the kind of measurable "hard" standard with which these bodies are familiar. The implementation of the standard therefore requires some different elements. First, it requires a sensitivity to the needs of large and small businesses; clearly the kind of inspection that might be necessary for a large consumer-credit company would not be appropriate for the corner video store.

How then to encourage registration, without providing an opportunity for purely symbolic compliance?

1. Any registration scheme requires an appropriate balance between the encouragement of registration on the one hand, and the prevention of symbolic claims about policies and practices on the other.
2. The registration scheme for privacy needs some clear procedures to deal with the interpretative problems that will inevitably arise. Any public claim about an organisational privacy policy should be allowed only after the verification of an organisation's policy by a process that is both transparent and consistent for all.
3. There needs to be an effective instrument for publicity - perhaps a "Privacy Good Book" that anyone could consult and that could encourage a competitive drive among organisations.

There are many inducements for businesses to register to the standard. These may stem from market pressures: moral persuasion, the desire to avoid or limit adverse publicity; the drive to gain competitive advantage and so on. Registration to the standard could also stem from regulatory actions:

- from governments that need to ensure privacy standards when personal data processing is "contracted-out;"
- from inter-provincial pressures (such as the enforcement of Quebec's privacy law covering the private sector);
- from the referencing of the standard in contract and legislation; and finally
- from the implementation of the "adequacy" provisions of the EU Directive's Article 25 on transborder data flows.

Standard will not substitute for a legislative framework

At the end of the day, however, the standard can never offer comprehensive data protection. Registration would inevitably be incremental and piecemeal. Privacy advocates in Canada need to continue to press for a legislative framework.

However, legislation would not render the standard redundant. In any legislated data protection scheme (in Canada and overseas) a

standard can be used as a very valuable tool to force compliance with data protection principles. Environmental standards (in the ISO 14000 series), for example, are already used to enforce court judgements. *I would like to see privacy and data protection authorities in Canada given explicit authority to order registration to the standard,* and thus to relieve them of expensive and time-consumer compliance auditing work.

Standard could assure enforcement

On the international level, I would also contend that the use of a standard offers the *only* possible way that Article 25 of the Directive can be enforced. The scrutiny of contracts provides no assurances to European data protection agencies that those rules are complied with in the receiving jurisdiction. There is no reason why these authorities cannot currently use the CSA standard in this way. Moreover, organisations in any country can adopt the CSA standard. Standards registration bodies outside Canada can offer their own registration schemes to the CSA model.

Full ISO standard would be better

It would be better for all, of course, if the CSA standard could be elevated to the status of a full ISO standard. This would provide a truly international instrument and would carry far greater weight and credibility than the current Canadian version. The process for the development of an ISO standard has begun through the international organisation of consumer representatives within ISO (COPOLCO). But it needs greater impetus. A technical committee within ISO needs to be convened to negotiate an international standard that is consistent with the CSA model, "adequate" to meet the stipulations of the EU Directive, and fully certifiable by national standards bodies.

The value of a standards approach

Standards are not sufficient to protect privacy, but they will be increasingly necessary in the more fluid, decentralised and globalised communications environment of the 21st century. Data protectors in all countries should consider the potential value of an ISO standard, and place the appropriate pressure on ISO and on their own standards organisations to take personal data protection as seriously as they do "quality management."

This paper is based on a presentation to the July 1996 Annual Conference of *Privacy Laws & Business,* St. John's College, Cambridge, by Colin J Bennett, Associate Professor, Department of Political Science, University of Victoria, British Columbia, Canada.