An International Standard for Privacy Protection: Objections to the Objections

Colin J. Bennett
Department of Political Science
University of Victoria, B.C.
CJB@Uvic.Ca
www.cous.uvic.ca/poli/bennett/

The following are some what I believe to be some contemporary realities about privacy protection in a globalized economy.

- Privacy standards are being "traded up" rather than "dumbed down." The extra-territorial impact of the EU Data Protection Directive has, on balance, led to a diffusion of privacy-enhancing instruments (regulatory, self-regulatory and technological) around the advanced industrial world.
- Private and public organizations that wish to participate in global trade will need to be able to receive and communicate personal data on employees and consumers.
- They will also need to be able to demonstrate, not just in words but in deeds, that they have implemented the basic set of privacy principles upon which all international and domestic privacy standards are based.
- In a globalised economy, organizations will increasingly wish to know that their competitors are pursuing the same privacy principles. In a climate of "trading-up" free-riders will be increasingly exposed and will be less tolerated by responsible market players.
- **There is a manifest need for the negotiation of an international, technology-neutral, certifiable, management standard for the implementation of the information privacy principles that may be implemented by any public or private organization that collects, uses, processes and discloses personal information via the Internet, or through any other public or private network.**

The aim of this paper is to make the case for an international privacy standard by refuting some of the most commonly stated objections to this idea. [1]

Background

In September 1996, as a result of some initial pressure from the consumer associations' committee (COPOLCO) of the International Organization for Standardization (ISO), the General Council of ISO recommended that work should begin on the development of an international standard for the protection of privacy. The 12 member Technical Management Board (TMB) of ISO then met in January 1997 and decided to refer the issue to an Ad Hoc Advisory Group (AHAG) which was to pave the way for a positive TMB resolution in 1998. As there has been some confusion about this initiative, I was asked by the Standards Council of Canada to write a background paper on the "Prospects for an International Standard for the Protection of Personal Information."[2]

The expected resolution, however, did not materialize mainly as a result of some very intensive lobbying by certain US multinational interests. The AHAG was maintained for another year in order to study the issue further, but was disbanded in June 1999. A meeting in Hong Kong in September 1999 hosted by the Standards Council of Canada concluded that some other useful instruments, short of a full-fledged standard, could be negotiated. And there has also been some attempt to raise the issue in other standards bodies. The Centre Europeanne de Normalisations (CEN), responsible for the negotiation of standards within Europe, has begun to study the feasibility of an international privacy standard, prompted in part by the Article 29 Working Party which is responsible for overseeing the implementation of the European Data Protection Directive.[3] However, the idea still tends to be confronted by a number of objections.

Objection No. 1: Privacy is a fundamental human right and has no place within the standards arena.

For those in the more technical world of standards setting and verification, the world of privacy protection might seem far removed. Privacy obviously has a long history within national and international rights jurisprudence. It is a value that is inherently and inescapably subjective. Its importance varies between and within different cultures. It is also a value that may protect individuals from a wide range of potential intrusions: from the overly inquisitive press, from overzealous law enforcement, from interference with the right to make private decisions about intimate family matters, from the nuisance of repetitive and inconvenient direct-marketing, from surveillance in the workplace, from the surreptitious gathering of personal information on the Internet, and so on. The range of issues and concerns subsumed under the broad heading of "privacy" is expanding and becoming increasingly complex.

However, there is a common international consensus on what it means to treat *personal information* in a privacy-friendly manner. At this level, privacy protection (or data protection) is defined as the regulation of the way organizations collect, store, manage and disclose personal information and is therefore a value that needs to be implemented within some highly complex organizations deploying the most sophisticated technologies. A privacy standard could therefore operate as a management standard, rather than a technical standard, which can measure for consumers, clients, competitors and regulators the extent to which organizations do indeed treat the personal information under their control in appropriate ways.

One model for such a standard is the Canadian Standards Association's *Model Code for the Protection of Personal Information* (Q830), which was finally published in March 1996.[4] This standard is organized around ten privacy principles, which organizations must adopt in their entirety – no "cherry-picking" in other words. A accompanying workbook, giving more practical advice about the development and implementation of a privacy policy, was also released.[5] The tricky task in the implementation of any privacy standard is to develop a conformity assessment scheme that allows lighter self-declaration where appropriate, and more systematic registration where necessary.[6] The CSA's Quality Management Institute (QMI) announced in September 1996 a recognition program, which

hopefully is sensitive to the needs of different stakeholders. Thus, what it means to "adopt" the *CSA Model Code* is clearly specified. A few Canadian companies are beginning to certify in this way.

The privacy debate in Canada has obviously been overwhelmed by the introduction of Bill C-6, the *Protection of Personal Information and Electronic Documents Act*, which is in its final stages of parliamentary debate. The bill is based upon the ten CSA principles. A privacy standard, however, is potentially a different type of instrument from either legislation or the typical "voluntary" code of practice. Standards implementation is based on the very simple adage: *say what you do, do what you say, and be ready to have your practices verified.* This Canadian experience suggests, I think, that there is nothing inherently incompatible between the philosophy and procedures of the standards world and those of privacy protection.

Objection No. 2: An international privacy standard would be too difficult to negotiate amongst widely different cultures.

Over the last thirty years a broad international consensus has emerged (at least amongst the industrialized countries) about what it means for an organization to pursue privacy-friendly policies. It means: that the organization must be *accountable* for all personal information in its possession; that it should *identify the purposes* for which the information is processed; that it should only collect personal information with the *knowledge and consent* of the individual; that it should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes; that it should not *use or disclose personal information* for purposes other than those identified; that it should *retain* information only as long as necessary; that it should keep personal information *accurate, complete and up-to-date;* that it should apply appropriate *security safeguards;* and that it should allow data subjects *access* to their personal information and an ability to amend it if necessary.

These commonsense principles appear (obviously in different form) in national data protection legislation, in international agreements, in voluntary codes of practice, and in the CSA *Model Code*. They express a basic and common understanding of how the responsible organization should treat the personal data that it collects, stores and processes, regardless of technology. The historical and cultural sources of privacy concerns may differ in interesting and dynamic ways, but the definition of what it means to be "responsible" has increasingly converged.

Objection No. 3: We already have three sets of Guidelines from the OECD (on privacy, security and cryptography), why another instrument?

The *1981 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* are indeed still in force. They have been a useful template and they have elicited certain commitments from major companies in the United States and Canada to adhere to the privacy principles. They continue to carry considerable force within the debates over the future of global e-commerce. However, the *OECD Guidelines* have been surpassed to some extent by the European Union's *Data Protection Directive*, passed in 1995 to harmonize European data protection laws. Four little words in this Directive will mean that organizations outside Europe will have to take far more seriously their privacy commitments. Personal data should not be transferred outside European Member States unless the receiving jurisdiction can assure an *adequate level of protection.*

At this time, the Europeans are gradually clarifying how this provision is going to be enforced. Central to European concerns is the need to "deliver a good level of compliance with the rules…A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them."[7] It is clear that European data protection authorities will not tolerate the processing of data offshore in order to escape the more protective laws in force in Europe. At the very least, businesses that rely on the free transfer of personal data about European clients, consumers and competitors will have to assure Euro-

peans that their industry and professional codes are *complied with.* A statement of good intentions will not suffice. An international standard could simplify the process of determining adequacy within a highly complex and networked data processing environment.[8]

Objection 4: No organization would adopt an international privacy standard.

If, as many in the private sector claim, good privacy protection is also good business, then there should be a desire to allay consumer and client fears by adopting the standard. A privacy standard is potentially a more efficient way for consumers to know which businesses are privacy-friendly, although there has to be an effective publicity mechanism and an appropriate cachet of privacy-friendliness. It allows advocates to measure business practices according to a common yardstick and gives companies that want to develop a privacy policy a template.

Other more coercive inducements might also operate. A standard (unlike a code of practice) can be referenced in contract either between private enterprises or between government and a private contractor. The same would apply to international contracts and the transborder flow of data. European data protection agencies might enforce Article 25 of the new *EU Data Protection Directive* by requiring any recipient of European data to be registered to the international standard. There are plenty of possible inducements.

The standard might also serve to harmonize the existing, and highly variable, "privacy seals" for websites. The expectation that companies engaged in electronic commerce should post "privacy policies" has predictably led to a wide variation in practice. Some privacy policies are bland statements of good intention. Others are heavily influenced by the input of the corporate legal department. Others are extremely difficult to find [9] If privacy is good business, then the market should be forcing a continual improvement in the presentation and quality of these different self-regulatory mechanisms. This dynamic should also produce a demand that privacy claims are also backed up with evidence of practice. A conformity assessment regime, similar to those that accompany ISO standards, may be emerging through the haphazard process of "trading-up" to standards within a highly competitive e-commerce environment within which privacy is recognized as the most important barrier to consumer participation.

Objection 5: An international privacy standard would be too costly.

Three responses. First, the loss of one's reputation as a responsible corporate citizen because of a privacy scandal can be even more costly. Scandals, such as those involving the Lotus Marketplace product, the "P-Trak" database from Lexis-Nexis, the Pentium III chip, and more recently the "Doubleclick" software will continue to raise the profile of privacy and temporarily force those data users whose practices have been criticized to restore their reputations. Adoption of a privacy standard can save time and energy otherwise spent on a contentious process of claim and counterclaim, the end of which typically leaves nobody the wiser about where the truth lies and what reforms are necessary.

Second, implementing privacy protection policy is not generally a complicated process. It would certainly be a more straightforward standard than those within the ISO 9000 series of management standards. Privacy protection could be a component of "total quality management" and indeed there are some interesting parallels between the fair information principles and the requirements of quality assurance. But more likely the standard would stand separately. Simply because ISO 9000 registration can be expensive, this is no argument for opposing a privacy standard. Moreover, any conformity assessment should offer a gradation of procedures, which would allow self-declaration and other less onerous verification processes where appropriate.

Third, many organizations are probably already complying with a good number of the privacy principles without knowing it. In some (but not all) cases, privacy principles are commonsense and implemented as part of the responsible corporation's obligations to its customers. Most, however, have

not thought about the privacy principles systematically. The introduction of a credible international standard within the marketplace would provide a far more effective measurement tool.

Objection 6: One standard cannot "fit all."

This is true, but it is hardly an obstacle. Any set of data protection rules will need to be adapted to the specific circumstances of different sectors. Many legislative schemes enable the negotiation of codes of practice in order to translate the language of the law into practical advice for banks, direct marketers, health-care providers, telecommunications companies and so on. In some jurisdictions, the privacy commissioner is responsible for negotiating these codes and giving them his "stamp of approval."

The CSA *Model Code* also allows organizations to "tailor" the wording to their own needs. Of course, where "tailoring" ends and "dilution" begins can be a tricky question. Nevertheless, I would assume that an international standard could operate on the same premise. The privacy principles are sacrosanct, but in tailoring them to their needs and problems, different organizations might develop codes of practice that explain how the principles will be implemented. Any conformity assessment process would then be based on this declaration.

Objection 7: It would never work in the United States

It is disappointing but unsurprising that the initial American reaction to this initiative should have been so negative. The idea has been greeted (in the American standards community and elsewhere) by a litany of spurious arguments and red-herrings most of which rely on a mistaken assumption that the United States is somehow "different", that it already possesses sufficient mechanisms for privacy protection and it should not therefore be made to follow the more interventionist approaches of countries elsewhere.

The United States is "different." But should the difference be allowed to make a difference? Whatever the cultural, constitutional and institutional differences, the reality remains that American multi-nationals in every service sector, and many manufacturing sectors, will need to convince European authorities that when they process personal data on European citizens that they comply with fair information practices. In the absence of comprehensive data protection law, and given the inherent weakness of contractual solutions, I would have thought that such a management standard would be in the interests of the American service sector.

Moreover, there is nothing inherently "un-American" about a privacy protection standard. The code of "fair information principles" that underpins most law and international agreement was initially developed in the United States. The principles negotiated through the CSA are very similar to those that appear in numerous voluntary codes of practice published by the more progressive American companies. A standard would be a natural extension of these codes of practice. The difference is that "adoption" of the standard would mean something. It would not be just a symbolic statement issued from top management, but a claim verified through an accepted conformity assessment methodology.

Furthermore, the current "Safe Harbour" negotiations between the EU and the US Department of Commerce indicate that one principal European concern is that many American companies might hide a number of privacy-invasive practices behind the Safe Harbour label.[10] The adherence to the Safe Harbour principles by organizations will hopefully entail a commitment to implement those principles. So we might be seeing the initial phase of the negotiation of an instrument that in the final analysis may look little different from the CSA's *Model Code of Practice*.

Conclusion

In conclusion, a separate international privacy standard is in the interests of all nations and stakeholders. The internationalization of personal data communications within the global information infrastructure will require a concomitant internationalization of privacy standards. Moreover, we must face the reality that only a minority of countries will be motivated to follow the European model of a general data protection law overseen by an independent supervisory authority. A full ISO privacy standard, certifiable by national standards bodies, will therefore be a crucial instrument for data protection within the fluid, networked and distributed computing and communications environment of the 21st century. It would provide a ready instrument for any data user whose practices have been questioned to indeed prove that they "say what they do, and do what they say."

[1] For presentation at CFP'2000 (Workshop on "Freedom and Privacy by Design") An earlier draft of this article was published in December 1997 in the Open Standards Tracking Report at: www.digital.com/info/osstr/tr1297.htm#A3

The objections are still being raised. The objections to the objections are still relevant.

[2] Available at: http://www.cous.uvic.ca/poli/bennett/research/ISO.htm

[3] Opinion 1/97 on Canadian initiatives relating to the standardisation in the field of privacy at: http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm

[4] Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information*. CAN/CSA-Q830-96 (Rexdale: CSA, 1996) is at http://www.csa.ca. (Referred to as *CSA Model Code)*

[5] Canadian Standards Association, Making the CSA Privacy Code Work for You: A Workbook on applying the CSA Model Code for the Protection of Personal Information to your organization. PLUS 8808 (Rexdale: CSA, 1997).

[6] Colin J. Bennett, *Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association*(Rexdale: CSA, 1995).

[7] *First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy,* at:

http:// europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp4en.htm

[8] For some empirical evidence of the nature of international data transfers and the complexities of determining "adequacy" see: *Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method of several categories of transfer-final report*: (Luxembourg: Office for Official Publications of the European Communities, 1999 (ISBN 92-828-5638-0)) or www.europa.eu.int/comm/dg15/en/media/dataprot/studies/adequat.htm

[9] See, Electronic Privacy information Center, "Surfer Beware" at: http://www.epic.org/reports/surfer-beware3.html

[10] See the latest opinion by the Article 29 Working Group: Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles at: http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm