IC

THE EUROPEAN UNION DATA PROTECTION DIRECTIVE: LESSONS FOR THE PROTECTION OF PRIVACY IN CANADA

Colin Bennett
Associate Professor
Department of Political Science
University of Victoria
P.O. Box 3500
Victoria, BC. V8W 3P5

(604) 721-7495 (voice)
(604) 721-7485 (fax)
CJB@UVVM.UVic.Ca

Address to the Industry Canada workshop, August 31, 1995

THE EUROPEAN UNION DATA PROTECTION DIRECTIVE: LESSONS FOR THE PROTECTION OF PRIVACY IN CANADA

Colin Bennett
Associate Professor
Department of Political Science
University of Victoria
P.O. Box 3500
Victoria, BC. V8W 3P5

(604) 721-7495 (voice)
(604) 721-7485 (fax)
CJB@UVVM.UVic.Ca

Address to the Industry Canada workshop, August 31, 1995

INTRODUCTION

On July 24, 1995, the Council of Ministers of the European Union formally and finally adopted a "Directive on the Protection of Personal Data with Regard to the Processing of Personal data and on the Free Movement of such Data."[1] This approval was the culmination of five years of drafting and redrafting as the document passed through the complicated and lengthy EU decision-making process. The formal adoption puts to rest speculation about whether or not this Directive would actually emerge. It gives the world's privacy advocates and experts a sense of relief that they no longer have to try to follow the intricate twists and turns of the European policy process. It gives data users (in both public and private) sectors a clearer sense of what personal data processing practices will be impermissible in the years ahead. And it gives European governments three years to bring their laws up to the new European standard.

For third parties such as Canada, however, the adoption of this long-awaited Directive raises more questions than it answers. The implications of a harmonized European data protection regime for third countries have always seemed somewhat hypothetical while the Directive was still in draft form. Now begins a period of speculation about what the provisions in the Directive actually mean for other countries, and about whether those provisions will be, or can be, enforced.

The purpose of this paper is to review and critique the final text of the EU Data Protection Directive and to analyse in more detail those provisions that may relate to the practices of third countries such as Canada. I then contrast this initiative with the state of the debate in Canada about privacy on the information highway.

I. THE EU DATA PROTECTION DIRECTIVE: WHAT IS IT?

When news spread around the close community of privacy experts and officials in 1990 that the European Commission had proposed a Directive to harmonize Europe's data protection laws, most (including myself) were vague about the implications, unclear about the legal status of such an instrument, and puzzled by the labyrinthine political process through which it has to pass.

---

[1] References are to the Common Position text of the Directive that was approved by the Council of Ministers in February 1995. European Union, *Common Position No. 1/95 Adopted by the Council on February 20 1995 with a View to Adopting a Council and European Parliament Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.* Brussels: OJC 93, 13 April 1995 (hereafter the "EU Data Protection Directive").

"Directives" are one of three forms of rule-making in the EU.[2] In the declarations that accompanied the formal adoption of the "Single European Act", it was provided that the European Commission shall give precedence to the use of Directives in the harmonization of public policy throughout the community. The goals expressed in directives are supposed to be binding. But member states are granted some latitude in deciding the actual form of implementation and the more detailed content of the legislation. This gives member governments an opportunity for delay, for bargaining with the Commission, and for the satisfaction of domestic interests.[3]

The aim of the Data Protection Directive is to "ensure a high level of protection for the privacy of individuals in all member states...and also to help ensure the free flow of information society services in the Single Market by fostering consumer confidence and minimising differences between the Member States' rules."[4] This reflects the underlying assumption that harmonized data protection legislation and the free flow of information are complementary rather than conflicting values. It reflects a belief that the single European market relies not only on the free flow of capital, goods and labour, but also of information. The hope is that "any person whose data are processed in the Community will be afforded an equivalent level of protection of his (sic) rights, in particular his right to privacy, irrespective of the Member State where the processing is carried out."[5]

Member states have three years (from July 1995) to enact the required new legislation. Each member country will be affected by this Directive and will need to amend their existing laws. Two countries (Greece and Italy) have the dubious luxury of a blank sheet, and can tailor their legislation directly to the provisions of the Data Protection Directive. Over and above this three year delay, countries can apply a further delay of up to three years with respect to personal data whose processing is already underway at the time the legislation comes

---

[2] The others are *regulations*, which are directly binding on national governments and other actors and pass into law without further action; and *decisions*, which are more specifically targeted to individual governments, groups, or individuals. Directives are by far the most important and least common type of rule.

[3] See, B. Guy Peters, "Bureaucratic Politics and the Institutions of the European Community," in Albert M. Sbragia ed. *Euro-Politics: Institutions and Policymaking in the "New" European Community*. Washington DC: Brookings, 1992

[4] Mario Monti (Single Market Commissioner), *Council Definitively Adopts Directive on Protection of Personal Data,* European Commission Press Release, IP/95/822, July 25, 1995.

[5] Ibid

into force. In addition, once legislation is enacted, they can apply a nine year delay to the application of three provisions to personal data already held in manual filing systems.[6]

The EU Data Protection Directive is a complicated instrument. The text has been subject to much drafting and redrafting as compromises have been struck and restruck within the Commission, the Parliament and the Council. It is not a "user-friendly" document that individuals/consumers can use to ascertain and exercise their data protection right. Nowhere do we find a clear list of "fair information principles", as in most legislation and in the recent model code from the Canadian Standards Association (CSA).[7] The reader is initially confronted with a series of legalistic "whereas" statements before the body of the Directive that state intentions, place this Directive in the context of other values and policies, and pay lip service to the variety of present even though they take some unearthing and interpretation.[8]

Thus, the Directive implements the principle of openness by requiring the data controller to "notify the supervisory authority...before carrying out any wholly or partly automatic processing operation or set of such operations."[9] "Notification" seems to contemplate a form of registration similar to that within the UK Data Protection Act of 1984, with exemptions for more routine personal data[10] and optional registration for manual records.[11] A"register of processing operations" should be maintained by the supervisory authority and be openly available.[12]

In addition, the data controller must provide the data subject with information about the identity of the controller, the purposes of the processing, the recipients of such data, whether

---

6 Chris Pounder and Freddy Kosten, *Data Protection News*, Issue No. 21, Spring 1995. pp. 36-37.

7 Canadian Standards Association, *Model Code for the Protection of Personal Information,* CAN/CSA-Q830-1994. Rexdale: CSA. (Working Draft of December 1994)

8 I have argued elsewhere that data protection laws have converged around this common set of principles. See, Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press, 1992.

9 EU Data Protection Directive, Article 18 (1)

10 Article 18 (2)

11 Article 18 (5)

12 Article 21

replies to questions are obligatory or voluntary, and the existence of a right of access and rectification.[13] These stipulations apply whether data are collected directly from the data subject, or from a third party.[14]

The *principle of access and correction* appears in Article 12. Access should be granted "without constraint"[15] and without excessive delay or expense. Individuals also have the right to know the nature of the data that are processed and the recipients of their data. They should be allowed to rectify inaccurate data and to erase or block data the processing of which does not comply with the provisions of the Directive.[16] Any rectification should also be communicated to third parties to whom the data may have been disclosed.[17]

The *principle of collection limitation* is probably the linchpin of any data protection regime. Article 6 declares that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[18] This clearly establishes what has come to be known as the *finality principle*. It differentiates then between the purposes at the time of collection and any new purpose that may be used to justify further processing. With few exceptions, the purpose for "further processing" must be compatible with the purpose for collection.[19] The data should also be "accurate, adequate, relevant and not excessive in relation to the purposes for which they are collected."[20]

Many laws and codes make a clear distinction between the *limitations on collection*, the *limitations on use*, and the *limitations on disclosure*. They appear as separate principles, for example, in the 1981 Guidelines from the OECD.[21] The EU Directive speaks more generally

---

[13] Article 10.

[14] Article 11.

[15] Article 12 (1) (i.e. no enforced subject access)

[16] Article 12 (2)

[17] Article 12 (3)

[18] Article 6 (b)

[19] See, Pounder and Kosten, *Data Protection News*, Issue no. 21. pp. 12-13.

[20] Article 6 ©

[21] Organization for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*. Paris: OECD, 1981.

about data processing, making little distinction between the stages of data collection, use and disclosure or between processing that occurs within or outside the controlling organization. This perhaps reflects the more fluid and decentralised "information highway" environment of the 1990s.

Thus, Member States shall provide that personal data must be "processed fairly and lawfully."[22] The six legal grounds specified are: if the data subject has given unambiguous consent; if the processing is necessary for the performance of a contract; if the processing is necessary to comply with a legal obligation; if the processing is needed to protect the vital interest of the data subject; if the processing contributes to a task carried out in the public interest; and if the processing is in the "legitimate interests" of the data controller or third parties.[23] At least with regard to the last two contingencies, data subjects are given an explicit "right to object" to the processing if there are "compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[24] The right to object to direct marketing is made more explicit, although the mechanism (whether to opt out or opt in) is left to the discretion of the Member states.[25]

The Directive reflects the continental law approach to regulation by giving the green light to certain specified activities. This approach is also reflected in Article 8 that specifies the conditions under which personal data within certain especially sensitive categories may be processed[26] -- data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health and sex life.

The final principle is that of security. Controllers must implement "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access."[27] The measures shall be appropriate to the level of risk. These obligations apply to data controllers themselves, as well as to organizations that process personal data by contract on their behalf.

---

[22] Article 6 (1) (a)

[23] Article 7 (a-f)

[24] Article 14 (a)

[25] Article 14 (b). This provision was the object of heavy lobbying by the direct-marketing industry.

[26] Article 8 (1) prohibits the processing of "personal data revealing racial or ethic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

[27] Article 17

The Directive is probably most forceful in specifying the nature and function of a member state's "supervisory authority." Each member shall provide that one or more public authorities are responsible for monitoring the application of the national provisions adopted pursuant to the Directive.[28] These authorities shall act with "complete independence" and shall be endowed with: investigative powers; effective powers of intervention (especially before processing operations begin);[29] powers to engage in legal proceedings; and powers to "hear claims" concerning the protection of rights and freedoms and regarding the "lawfulness of data processing" under the Directive. In addition, member states shall provide that the supervisory authorities are consulted when developing administrative measures with privacy implications.[30] In total, these provisions add up to a greater range of powers and responsibilities than exist within most European data protection regimes.

Article 29 establishes a Working Party composed of a representative from the data protection authority in each member state, joined by representatives of the European Commission, and of other Community institutions. The Working Party is expected to give the Commission advice on divergences between national legislation, on the level of protection in third countries, on codes of conduct, and on proposed amendments to the Directive. It shall also draw up an annual report.[31]

The Working Party has only advisory status. Executive decision-making power over the Directive is granted to a mysterious body simply called "The Committee."[32] This is comprised of representatives from the member states, and chaired by someone from the Commission. This appears to be a mechanism by which the Commission can adopt decisions and regulations pursuant to the Directive, and in particular in regard to the determination of the "adequacy of protection" within third countries. Thus, the Working Party will report opinions to the Commission, which are referred to the Committee which then report back to the Commission on the "measures to be taken." If the Commission adopts the measures, then they should be implemented by Member States.

---

[28] Article 28 (1). The use of the plural permits countries with a federal structure to have authorities for national and local units (e.g. Germany). It does not envisage "sectoral" oversight authorities such as exist in Canada.

[29] Article 28 (3). In addition Article 20 contemplates a form of "risk analysis" through prior checking by the supervisory authority of new processing operations that might be especially harmful.

[30] Article 28 (2)

[31] Article 29

[32] Article 31

II. THE EUROPEAN DATA PROTECTION DIRECTIVE: A CRITIQUE

I have highlighted only a selection of the most important aspects of this Directive and glossed over many of the details.[33] The overview should serve as a basis for an initial critique of its provisions, and for an analysis of its likely effects.

First, it is important to recognise that this is a major achievement. Most proposed Directives do not make it through the process; the Data Protection Directive was declared dead on more than one occasion. For all its faults, it undoubtedly represents progress for the cause of personal privacy protection in Europe.

Second, the Directive should not be seen in isolation but as a culmination of a set of processes that were set in motion in the 1970s. I argued in Regulating Privacy how various technological, political and international forces had produced an inexorable process of policy convergence. In the 1970s and 1980s, that convergence was confined to the statutory principles upon which national legislation was grounded; but different states still relied on very different policy instruments for the implementation of those principles. The Data Protection Directive contemplates convergence, not only of policy, but also of the enforcement and oversight mechanisms within Europe.

Thus, countries (such as Germany) that have not yet developed procedures for the registration of data processing operations will be forced to do so. Countries (such as Britain) whose data protection authority does not have extensive powers of investigation and supervision, will be forced to grant the Data Protection Registrar more powers than are currently available under the 1984 Data Protection Act. Countries (such as France) that have not yet made use of industry codes of practice will have to give thought to how these instruments might be integrated into their laws.[34]

Third, there are some real innovations in data protection within this Directive. Most notably, this final draft has abandoned what I regard to be certain artificial and outdated distinctions. For instance, there is now little distinction made between public and private sector data processing; previous drafts differentiated between the sectors in regard to the fair

---

[33] For a more thorough analysis, see Pounder and Kosten, *Data Protection News*, Issue No. 21 (Spring 1995).

[34] Article 27 encourages "the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States." See, Colin J. Bennett, Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association. Rexdale: CSA, 1995.

obtaining and legitimacy of processing of personal data.[35] Some laws only cover "automated" data processing. The Directive applies to "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis."[36] Thus "structured" manual files are also covered, a provision that will cause major headaches for countries (such as Britain) whose law only regulates computerised files. As mentioned above, the Directive also avoids artificial distinctions between collection, use and disclosure, preferring the all-encompassing term "data processing."

However, the Data Protection Directive also suffers from some major drawbacks. First, it is very complicated. This will detract from its value as an instrument that individuals might cite and use. It is exactly the kind of document that one would expect if a large and fluctuating number of European bureaucrats tried to cobble together the German and the French law, add on a few provisions from the British, spend five years taking it through the European legislative process, and subject it to analysis and lobbying from almost every conceivable interest. The complexity and vagaries of the process have produced a complicated and legalistic document with many derogations and qualifications, a number of "lowest common denominator" provisions and much incoherence.

Perhaps the greatest incoherence is provided by the different time limits allowed for implementation of the various provisions. Pounder and Kosten comment that this "mish mash of derogations is a recipe for chaos." They have worked out the meaning of Article 32. I quote their analysis:

> Once legislation is passed, any processing of new personal data is immediately subject to the Directive, irrespective of whether the processing is automated or not. If advantage is taken of the maximum delay, all remaining **automatically processed** personal data will become subject to **all Articles** within six years of adoption of this Directive..., whilst existing manual filing systems, at the end of this period, will become subject to **all relevant Articles** (notably all Data Subject Rights, judicial remedies and the power of the Data Protection Authority) except Articles 6-8 (but only if Member states so choose).[37]

---

[35] See the first draft: Commission of the European Communities, *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data*, (COM[90] 314 Final - SYN 287, Brussels, September 1990).

[36] Article 2 ©

[37] *Data Protection News*, Issue No. 21, Spring 1995, p. 37.

Thus some personal data held by a multi-national company could be subject to different time limits and derogations, depending on when the processing began, on whether it is manually or automatically stored, and on the country in which the data are processed.

The more specific provisions of earlier drafts have not only given way to derogations, but also to some vague generalisations. Take for instance the issue of "informed consent." The first draft contained some strong language about the need for "informed consent" for secondary uses of personal data. Now it seems that any data processing is permissible, unless the data subject "objects." It is not clear whether this means a right to "opt-out" or merely a right to complain. The greater flexibility within the final version is a reflection of the wider move towards "subsidiarity" in the light of conflicts over the Maastricht Treaty.

The initial purpose of the Directive was to harmonize European policies at a "high and common level of protection." It is difficult to judge whether this has been achieved as so much will be left to subsequent interpretation and implementation by Member States. But it is also difficult to evaluate because nowhere do we find a conceptually precise discussion of what this means. The "level of protection" around the world is often judged according to anecdote and conventional wisdom. Thus Germany is said to have "strong" data protection; the United States weak. But often these judgements are based on crude and binary indicators. To ascertain the "level of protection" is a complex task that obviously requires empirical evaluation of practice, rather than a simple reading of the "black letter" of the law.[38]

III. THE EUROPEAN DATA PROTECTION DIRECTIVE: THE IMPLICATIONS FOR THIRD COUNTRIES

Since 1990, when it was first introduced, this Directive has worried certain governmental and private sector interests in third countries. It is worth stressing at the outset that the purpose of this Directive was not to force third countries to "come up to standard." The principal motivation is to harmonize European law. The provision relating to outside countries, while of central significance to Canada, should be placed in the perspective of the entire Directive. For the Europeans, there are far more significant data protection problems than the implications of transborder data flows. On the other hand, European policy makers are serious enough about privacy to want to prevent their efforts being undermined by

---

[38] For a discussion of the limitations of harmonization, see, Charles D. Raab and Colin J. Bennett, "Protecting Privacy Across Borders: European Policies and Prospects, " *Public Administration*, Vol. 72 (Spring 1994): 95-112. In a more recent paper, we have attempted to assess the extent to which data protection can be evaluated according to clear and common criteria. See, Charles D. Raab and Colin J. Bennett, "Taking the Measure of Privacy: Can Data Protection be Evaluated?" Paper presented to the PICT conference, Westminster, May 1995.

data processing offshore. Five years of effort is not something that data protectors in Europe are going to waste. So it is reasonable to assume that the provisions relating to the processing of personal data by "third countries" will be taken seriously.

Article 25 stipulates that "Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if...the third country in question ensures an adequate level of protection." The "adequacy" of protection shall be assessed "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations." Particular consideration is to be given to the nature and purpose of the data and the "rules of law, both general and sectoral" and the "professional rules and security measures that are complied with." This obviously suggests that something less than a comprehensive data protection statute might be considered "adequate."

Article 26 lists a number of derogations from this provision. Personal data may be transferred to a country with "inadequate" protection when: the data subject has given his consent "unambiguously"; the transfer is necessary to fulfil a contract between the data subject and the controller, or between the controller and a third party; the transfer is necessary on "important public interest grounds, or for the establishment, exercise or defence of legal claims"; the transfer is necessary to protect the "vital interests of the data subject"; and the transfer is of data that are already in a public register.[39]

Member states can also authorize transfer to a country with "inadequate" protection if the data controller enters into a contract that "adduces sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals."[40] In such cases, the country concerned shall inform the Commission and the other Member States of such authorizations, to allow for objections. The Commission may also decide, through its "Committee" (Article 31) that certain "standard contractual clauses offer sufficient guarantees."[41]

Where the Commission decides (again according to Article 31) that a third country does not ensure adequate protection, Member States are "to take the measures necessary to prevent

---

[39] Article 26 (1)

[40] Article 26 (2)

[41] Article 26 (4)

the transfer of data of the same type to the third country in question."[42] The Commission "shall then enter into negotiations with a view to remedying the situation."[43]

The initial wording of this provision spoke of an "equivalent level of protection" which was generally taken to mean the existence of a comprehensive data protection law on the European model. Since "equivalent" gave way to "adequate" the standard has been lowered and made impossible to define. Thus nobody knows what constitutes "adequate protection." Nobody can even say for sure that "adequate protection" is provided even in those countries that have supposedly "strong" laws. The implementation of this provision is, therefore, likely to be unpredictable and politicized.

The determination of "adequacy" rests not with data protection agencies (who only have an informal advisory role through the Working Party) but with the Commission itself. The implementation of Articles 25 and 26 will therefore be susceptible to the vagaries of the European policy process and are likely to be confused with the resolution of issues that have nothing to do with data protection. Logrolling may therefore override the more predictable and rational pursuit of a data protection standard.[44] The weakening of the standard means unpredictability, and that is something about which Canadian interests should be concerned.

The other major problem with the regulation of transborder data flows is that neither the supervisory authority nor the data controller has the power to scrutinize the processing of personal data in another jurisdiction nor be satisfied that data subjects can exercise their privacy rights. The Directive establishes a more coherent and institutionalized process to make judgements about "adequacy." Yet those determinations will continue to be made on the assumption that the wordings of contracts, laws and professional codes are reflected in practice. The Directive does not get around the central dilemma inherent in the former attempts to regulate international data transmissions by the Council of Europe Convention,[45] or through the "model contract" by the International Chamber of Commerce.[46]

---

[42] Article 25 (4)

[43] Article 25 (5)

[44] As Pounder and Kosten put it: "if you support out tomato initiative, we shall in turn support you in defining the Republic of Munchkin land as offering an adequate level of protection." *Data Protection News*, Issue No. 25, p. 33.

[45] Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg: Council of Europe, 1991.

[46] See, "Model Clauses for Inclusion in a Model TBDF Contract," *Privacy Laws and Business*, December 1992.

One suggested way to tackle the problem of enforcement is to make the "data exporter" directly, continually and completely liable under domestic law for the processing of data overseas. Contracts would establish the exporter's right to enforce and supervise the importer's data protection obligations. [47] Then, and only then, can the interests of the exporter and those of the data subject be coincident. One possible mechanism to achieve this supervision would be to require the data exporter to oblige the recipient of the data to undertake regular and independent privacy audits of its operations.[48] The development of the Canadian Standards Association's Mode Privacy Code offers some hope that certain independent verification procedures may be established in Canada, and used (among other things) to satisfy European standards.

IV. THE IMPLICATIONS FOR CANADA

It is very difficult to predict whether the European Directive will presage the blockage of data flows to Canada. European data protection authorities will clearly not be willing to tolerate the deliberate and continuous flouting of the Directive through the establishment of "data havens." European data users will be justifiably aggrieved if they have to abide by strong data protection measures in Europe, whilst overseas competitors can act with impunity. European citizens, and the public interest and consumer groups that represent them, will also not look kindly on the continual flouting of their privacy rights by overseas interests. On the implementation of Articles 25 and 26, at least, the interests of European data users, data subjects and regulators may be coincident.

Perhaps the most important implication of this Directive, however, is not economic but psychological. An embarrassing aspect of this initiative is that some countries (such as Spain and Greece) that in recent memory were governed by dictatorships now have, or will get, better privacy standards than Canada. Even some of the former states of Eastern Europe (especially Hungary and the Czech and Slovak Republics) have legislation. Canada is, therefore, only one of a handful of democratic countries that has not developed a comprehensive privacy protection policy. The motivation to emulate legislation elsewhere in order to "keep up with the Joneses" has always been a significant force within this policy domain.[49]

---

[47] See, Joel R. Reidenberg, "Setting Standards for Fair Information Practice in the U.S. Private Sector," *Iowa Law Review* Vol. 80 (Spring 1995).

[48] See, Bennett *Implementing Privacy Codes of Practice*, p. 108.

[49] See, Bennett, *Regulating Privacy*, pp. 123-7.

There are, however, far more important domestic reasons why Canada needs to establish a general policy framework for privacy protection in its private sector, and why the hodgepodge of federal and provincial laws and voluntary codes of practice will not suffice in the years ahead.[50] For a number of historical, cultural and political reasons, our federal and provincial policy-makers have assumed that the privacy threat from government is more severe than that from the private sector. Consequently, our public sector institutions are now almost completely regulated. Yet only Quebec has passed a comprehensive data protection statute on the European model. Bill 68, the Act Respecting the protection of personal information in the private sector, embodiment to the information privacy rights incorporated into the new Civil Code and came in to effect in 1994. Canada thus became the only country in which the scope of privacy protection in one of its jurisdictions exceeds that of the central government.

Clearly this incoherence in untenable for four Canadian reasons. First, the volume of personal information that will be transmitted across the highway will increase exponentially in the years ahead. Consumers will become increasingly remote from the organizations that process their data. The information highway technologies will hold enormous potential for the compilation of profiles of an individual's lifestyle habits and purchasing choices, facilitating more sophisticated direct-marketing and affecting the conditions under which individuals may access a variety of products, services and opportunities. The much-vaunted "set-top" box will control the communication of voice, text, video and graphic data to and from the Canadian household. It will also be a valuable repository of data about our private lives -- our entertainment preferences, our financial transactions, our shopping habits, our private communications and so on.[51]

A second and related reason will be shifting institutional responsibilities and especially the erosion of the distinction between the public and the private sectors. Where the "public" sector ends and the "private" sector begins is becoming increasingly difficult to determine. The distinction is being eroded by efforts to privatize or hive- off government functions. Thus "private" organizations are increasingly performing "public" functions, and often require the use of "public" data to fulfill those obligations. Illustrations include: the use of smart cards and ATM machines for the dispensing of government benefits; the matching of data on welfare recipients with bank or financial records to ascertain eligibility; the trading of government information to enhance revenue; the use of consumer credit reports for security checks; and so on.

---

[50] Reviews of current privacy regulation can be found in: Bennett, *Implementing Privacy Codes of Practice*; and Ian Lawson, *Privacy and the Information Highway: Regulatory Options for Canada.* Ottawa: Industry Canada, 1995.

[51] See, Industry Canada, *Privacy and the Canadian Information Highway*, Ottawa: Industry Canada, 1994.

The pervasiveness and flexibility of the new technologies will make it increasingly difficult to determine which "data" are "in" the public sector, and which "in" the private, producing a range of new regulatory dilemmas.

Thirdly, the Canadian public has hardly been oblivious to the technological and institutional forces that threaten their privacy. The 1992 national Canadian public opinion survey Privacy Revealed from Ekos Research Associates demonstrated unequivocal support for stronger public policies to protect privacy. Fifty-two percent of Canadians are "extremely" concerned about privacy, with 92 percent at least moderately concerned. Seventy-one percent totally agree that privacy rules should apply to both government and business. Sixty-six percent believe that government should be working with business to come up with guidelines on privacy protection for the private sector.[52]

A more recent 1995 poll from Equifax Canada Inc. reports that privacy concerns are rising; that those viewing privacy as a fundamental right have increased; that there is a greater number of consumers who feel that they have lost all control over how personal information about them is circulated; and that those believing that the protection of privacy will get worse by the year 2000 has also increased.[53] Polls such as this, together with a greater number of stories in the print and TV media, are slowly increasing the salience and visibility of the issue.

The final factor, and perhaps the most important for business interests, is the economic implications of inconsistent privacy standards. The Quebec legislation permits the *Commission d'accès à l'information* to prevent the flow of personal data to parties outside Quebec if that information will be used "for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned."[54] If used, these powers could constitute a non-tariff trade barrier within Canada. Besides, the cost of having to abide by one set of rules in Quebec and a different set in the rest of the country could prove an enormous inconvenience for many businesses within the service sector that rely on unimpeded inter-provincial communications.

---

[52] Ekos Research Associates, *Privacy Revealed: The Canadian Privacy Survey,* Ottawa: Ekos, 1992.

[53] Louis Harris and Alan F. Westin, *The Equifax Canada Report on Consumers and Privacy in the Information Age,* Ville d'Anjou: Equifax Canada, 1995.

[54] Bill 68, *An Act Respecting the Protection of Personal Information in the private sector,* Section 17 (1).

V. THE STATE OF THE CANADIAN DEBATE ABOUT PRIVACY PROTECTION

Policy debate about the future of personal privacy protection in Canada's private sector is currently being conducted in two separate arenas, both of which span the federal/provincial divide.

The first is the Canadian Standards Association (CSA). Since 1992, representatives from government, industry and consumer groups have been negotiating a "Model Code for the Protection of Personal Information." The committee has been updating and revising the OECD Guidelines, with reference to the Quebec legislation and the emerging EU Directive. This is intended to establish common safeguards to protect personal information throughout the entire private sector. The code would then be adopted by different sectors, adapted to their specific circumstances, and used as a way to promote "privacy friendly" practices.

The code is due to be issued at the end of 1995, after appropriate public consultation and redrafting. It has not yet been determined, however, what role the CSA might play in certifying or registering industry codes and practices. There is potential to register data users (in both private and public sectors) to the standard and thus to oblige them to implement the privacy principles. The scrutiny of operational manuals and/or on-site auditing could be a prerequisite for maintaining a registration to the CSA privacy standard.[55]

The CSA Model Code can provide a greater consistency of policy, more consumer awareness of privacy rights, a better yardstick for the measurement of the adoption of data protection, and a greater level of responsibility for the collection, storage and disclosure of personal data. However, adoption of the code would still be voluntary, even though pressures can be exerted by government, international data protection authorities, and by consumers and clients. The process of building a system of data protection in Canada would still be incremental and piecemeal.

Perhaps for these reasons, the Advisory Council on the Information Highway has recently passed a set of recommendations to "ensure privacy protection on the Information Highway." In addition to encouraging the adoption of voluntary standards based on the model CSA code and the analysis of a range of technological solutions (mainly encryption techniques), the Advisory Council recommended that the federal government:

> create a level playing field for the protection of personal information on the information highway by developing and implementing flexible framework legislation for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA model code, while allowing the flexibility to determine how they will refine their own codes.

---

[55] See, Bennett, *Implementing Privacy Codes of Practice*.

They have recommended that a federal/provincial/territorial working group should be established to implement the CSA principles in all jurisdictions.

What seems to be envisaged here is the passage of "framework" or "shell" legislation at the federal level (consistent with moves in other areas towards "regulatory flexibility"). The legislation would oblige companies to abide by the CSA principles and develop their own codes based on the CSA model.[56] More recently, in his 1994-95 Annual Report, the Federal Privacy Commissioner has suggested that the CSA privacy code be added to the federal Privacy Act, meaning that "observance of the CSA standards would become a legal obligation and would be supported by a system of independent oversight."[57]

VI. CONCLUSION: HOW CANADA CAN EXCEED THE EUROPEAN STANDARD

There is a tendency to regard the Europeans as way ahead of Canada in responding to the privacy protection problem. Indeed, for some countries the passage of the European directive signals the advent of "fifth generation" data protection before we have developed our first comprehensive privacy policy. The lateness of Canada's response, however, may be an advantage. We do have the opportunity to learn from other countries and to fashion a policy response that is perhaps more sensitive to the challenges of the information highway than the overly bureaucratic and legalistic approach of the EU Directive. I conclude with some random thoughts about the "state of the debate" which suggest that we may be in a better position to resolve these problems than some think.

First, the European approach to data protection is dominated by the drafting of legal rules; the EU Directive is a lawyer's document. The debate in Canada has so far recognised the need to apply the full range of available policy instruments to the problem: self-regulatory codes, legislation, and privacy-protecting technologies (especially public-key encryption). Of course, no policy can succeed without greater consumer awareness and involvement. All are necessary conditions for the protection of personal data on the information highway; none is a sufficient condition.[58]

---

[56] This is one model discussed by Ian Lawson, *Privacy and the information Highway*, pp. 43-4.

[57] Privacy Commissioner of Canada, *Annual Report* 1994-95, p. 7.

[58] These options are laid out in the Industry Canada paper, *Privacy and the Information Highway.*

Second, there has been a greater number of self-regulatory initiatives in Canada (in the form of voluntary codes) than in any other country.[59] Any personal data protection policy inevitably relies on a significant measure of self-regulation; major responsibilities will continue to reside with individual companies and their trade associations for consumer and employee education. Canada has been creating a data protection regime from the "bottom-up" and we can build upon this experience.

Third, the CSA Model Code offers a novel solution that can raise the level of consistency, increase consumer awareness of their rights, monitor and measure the adoption and implementation of the privacy standards in different sectors and raise the general level of organizational responsibility for the personal information that is collected, stored and communicated over the networks. This code has been openly negotiated by industry, consumer representatives and government. It reflects a typically Canadian approach to consensus building.

Fourthly, if the CSA decides to offer registration or certification to this code, a crucial auditing mechanism is established when that will oblige certain businesses to develop codes of practice, demonstrate how those codes are implemented, and force regular and independent auditing through an accredited registrar such as the Quality Management Institute (QMI). Registration to the code would occur under pressures from consumers, clients and domestic and foreign governments. It may promote a more effective system of privacy auditing than currently occurs anywhere in Europe.

Fifth, however, the CSA initiative alone is insufficient. It may fill in some of the gaps in the patchwork but can never produce a comprehensive system of personal data protection that is required. Only legislation can really force adoption of the CSA code, focus the attention of the data users, produce a true consistency of rules, define a line beyond which organizations may not be permitted to step and provide genuine redress for the aggrieved. I suspect, also, that in the long run only legislation can avoid a series of case-by-case battles in the European Commission about the "adequacy" of personal data protection in Canada.

Finally, only legislation can involve the agencies that have developed the most expertise and experience in balancing the privacy rights of individuals with the needs of organizations -- the federal and provincial offices of the Information and Privacy Commissioners. The CSA cannot act as a clearinghouse for complaints. Any "sectoral"

---

[59] The most important codes are those that have been devised through the trade associations such as Stentor, the Canadian Direct Marketing Association, the Canadian Bankers Association, the Canadian Life and Health Insurance Association, and the Insurance Bureau of Canada.

approach to the problem would involve oversight by regulatory bodies (such as the CRTC and OSFI) which have neither the time, resources nor expertise to oversee the processing of personal data in any continuous manner.

A comprehensive legislative solution to privacy protection in Canada would then integrate the existing mechanisms of industry and company codes, the CSA standard, and the Offices of the federal and provincial privacy commissioners. A combination of registration and auditing to the CSA standard, and complaints resolution through the privacy commissioners could constitute an effective national policy that meets the needs of consumers, satisfies international standards, and is sensitive to emerging technological advances and business interests in the increasingly interconnected and competitive global economy. Such a framework would not only meet the privacy standards of the European Directive; it might even exceed them.