What Government Should Know about Privacy: A Foundation Paper

Colin J. Bennett
Department of Political Science
University of Victoria
Victoria, B.C. V8W 3P5

CJB@UVIC.Ca
http://web/uvic.ca/polisci/bennett

Paper prepared for the Information Technology Executive Leadership Council's Privacy Conference, June 19, 2001
(Revised August 1, 2001)

Introduction

This paper has been commissioned to: "promote and establish a base level understanding regarding privacy concepts, key definitions of privacy terms and privacy management tools that will facilitate a shared/common point of reference for OPS staff." The research is to focus on "the historical development of fair information practices arising out of the concerns of governmental and non-governmental organizations regarding the computerization of personal data." The paper is also to "provide a cross-jurisdictional analysis of privacy policy management tools that have been developed by governmental and non-governmental organizations, including tools that Ontario has developed."

The paper therefore adopts a very broad comparative and historical perspective in order to promote a base level understanding of the essential approach to privacy protection adopted by governments over the last thirty years. This issue has come a very long way since the 1960s when it first appeared on policy agendas. This paper attempts to explain why the privacy issue has developed in the way it has, and to draw certain lessons for Ontario policy-makers.

No commonly agreed definition of the word "privacy" exists. There is even considerable doubt as to whether this is the most appropriate concept to frame the set of issues raised by the collection, use and dissemination of personal information by modern complex organizations. The first section of the paper, therefore, tries to review some of the key conceptual issues, not with a view to providing an inevitably flawed definition of privacy, but in order to demonstrate how the policy debates in different countries have tended to be informed by a particular definition over others, which centers on the notion of "information privacy" or "data protection." The second section of the paper discusses these more focussed concepts and reviews their historical development in Canada and overseas.

In the early 1970s when governments were first trying to tackle this question as a policy problem, certain assumptions were made about how one can, and cannot, provide a workable set of information privacy rights for citizens. These assumptions have underpinned most of the policy activity in Western societies throughout the succeeding decades, and have led to a general acceptance and convergence around a set of procedural information privacy principles, often referred to as "fair information principles" (FIPs). The third section analyzes the FIPs doctrine, how it became the basis for privacy as a public policy problem, how it has been represented in different legal regimes, and how it has been adapted and critiqued in recent years.

The fourth section reviews how the implementation of FIPs has varied from jurisdiction to jurisdiction and how a number of more specific privacy

management tools have arisen to counter the challenges of privacy protection in a more decentralized and networked computing environment. This section discusses these policy instruments in more general and comparative perspective. The paper therefore moves from the abstract discussion of ethical principles, to the analysis of privacy as a policy problem, to the development of different privacy policy instruments including those used in Ontario.

The concluding part of the paper addresses how governments can and should try to strike the appropriate "balance" between privacy and organizational demands for personal information for program management and service delivery. Historical experiences in Canada, and elsewhere, suggest that there is no necessary incompatibility between privacy protection and other policy goals which require the processing of personally identifiable personal information.

What is Privacy?

Although there is no consensus on how to define privacy, even in English-speaking nations, there is common agreement that privacy is something that every human being needs at some level and in some degree. This point is substantiated by a wealth of social psychological and anthropological evidence which has suggested that every society, even the most primitive, adopts mechanisms and structures (even as simple as the building of walls) that allow individuals to resist encroachment from other individuals or groups.[1] Moreover, Dystopian visions of a world without any privacy have had a profound and symbolic effect on public consciousness in most societies. We may not know what privacy is, but we can all agree that something precious is lost when it goes away.

A further central, and more controversial, assumption in the privacy debate is that privacy is something that "we" once had, but now it is something that public and private organizations employing the latest information and communications technologies are denying us. This theme is represented in a large corpus of polemical literature in which Orwellian metaphors and imagery are prolific, even though '1984' came and went without any palpable change in the attention paid to privacy questions. Continually over the last thirty years publishers in North America[2], Britain[3] and elsewhere have been attracted by this more polemical

---

[1] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

[2] An incomplete list would include: Jerry Rosenberg, *The Death of Privacy (1969);* Arthur Miller, *The Assault on Privacy (1971);* John Curtis Raines, *Attack on Privacy (1974);* Alan Lemond and Ron Fry, *No Place to Hide (1975);* Lester Sobel ed. *War on Privacy (1976);* Robert Ellis Smith, *Privacy: How to Protect What's Left of It (1979);* William C. Bier, *Privacy: A Vanishing Value (1980);* David Linowes, *Privacy in America: Is your Private Life in the Public eye? (1989);* Jeff Rothfeder, *Privacy for Sale ,(1992)*Deckle Maclean, *Privacy and Its Invasion (1995);* Ann Cavoukian and Don

genre. The contexts may change, the technologies may evolve, but the message is essentially the same: Privacy is eroding, dying, vanishing, receding, and so on. Despite privacy laws, conventions, codes, oversight agencies and international agreements, some have argued that privacy is something of the past, to the extent that one prominent business leader could proclaim, in a much-quoted statement, "you have zero privacy anyway; get over it!" [4]

Clearly privacy is a controversial and subjective term whose meaning changes over time and space. Some authors have approached the definitional problem simply by providing a list of the interests individuals might have in the information about themselves.[5] Let us make two sets of distinctions to help focus the analysis and summarize a very complicated and sprawling literature. The first distinction relates to how one might draw the boundary between the public and the private; the second relates to the reasons or motives behind the privacy value, or why one might want to draw that boundary in the first place.

The classic definition of privacy offered at the end of the last century by Samuel Warren and Louis Brandeis ("the right to be let alone") shields some subtle and important distinctions concerning what aspects of personal life should, in fact, be "let alone."[6] Let us first make a distinction between the privacy of space, the privacy of behavior, the privacy of decisions and the privacy of information.

Many formulations and discussions of privacy adopt an explicit or implicit spatial dimension, and rest on the assumption that there is "zone" or a "realm" into which other individuals or organizations may not encroach. The term "an Englishman's home is his castle" or the principle that the "state has no business in the bedrooms of the nation" (attributed to Pierre Trudeau, among others) are

---

Tapscott, *Who Knows? Safeguarding your Privacy in a Networked World (1997);* Whitfield Diffie and Susan Landau, *Privacy on the Line (1998);* Charles Sykes, *The End* of Privacy (1999); Reg Whitaker, *The End of Privacy* (1999); Simson Garfinkel, *DataBase Nation: The Death of Privacy in the 21st Century* (2000).

[3] Donald Madgwick, Privacy under Attack (1968); Malcolm Warner & Michael Stone, The Data Bank Society (1970); Anthony A. Thompson, Big Brother in Britain Today (1970); Donald Madgwick & Tony Smythe, The Invasion of Privacy (1974); Patricia Hewitt, Privacy: The Information Gatherers (1977); Ian Will, *The Big Brother Society (1983);* Duncan Campbell & Steve Connor, *On the Record: Surveillance, Computers and Privacy (1986);* Simon Davies, *Big Brother: Britain's Web of Surveillance (1996);* Stuart Goldsmith, *How to Live a private Life free from Big Brother's Interference (1997).*

[4] Scott MacNealy of Sun Micro Systems allegedly made this statement in 1999, although the original source and context seem to have been forgotten in the frenzied rush by privacy advocates to hold this up as an extreme and ill-considered position.

[5] Thus, David Flaherty listed the following: the right to individual autonomy, the right to be left alone, the right to a private life, the right to control information about oneself, the right to limit accessibility, the right to exclusive control over access to private realms, the right to minimize intrusiveness, the right to expect confidentiality, the right to enjoy solitude, the right to enjoy intimacy, the right to enjoy anonymity, the right to enjoy reserve, the right to secrecy. *Protecting Privacy in Surveillance Societies,* (Chapel Hill: University of North Carolina Press, 1989), p. 8.

[6] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890): 193.

based on a conception of a spatial distinction, or a physical boundary between what is public and what is private. Contemporary concerns about the privacy of the physical person and its protection from various biometric devices are also centered on a notion of a physical or spatial boundary.[7]

For others, the boundary is more properly drawn in terms of the specific behaviors, matters or actions that should be shielded from intrusion. Take this justification by Charles Fried: "to respect, love, trust, feel affection for others, and to regard ourselves as the objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion."[8] Privacy is, therefore, essential for intimate behavior.

A third way to draw the line is in terms of individual decisions and choices. Privacy is essential for preventing coercive interference with decision-making affecting intimate and personal affairs. This concept of decisional privacy has been relied upon, especially in American constitutional law, to protect decision-making surrounding abortion, contraception, "lifestyle" choices, the right to choose one's spouse and the right to rear one's children in accordance with one's own religious convictions.[9]

And finally, the boundary can be drawn in terms of information. Here the important point is not that certain information is inherently private, but that we should have a right to control its circulation. A number of definitions have centered on this informational aspect of the privacy question: "the control we have over information about ourselves"[10]; "the individual's ability to control the circulation of information relating to him"[11]; the "claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others"[12]; and the "interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves."[13] Definitions surrounding the concept of information tend therefore to emphasize the importance of "control."

These distinctions are neither mutually exclusive nor jointly exhaustive. Most have been developed by American commentators in the context of attempting to sort out tricky doctrinal questions in relation to the development of American

---

[7] See Roger Clarke's companion paper, "ID Authentication and Privacy." Clarke makes a similar set of distinctions between the privacy of the physical person, the privacy of personal behavior, the privacy of personal communications and the privacy of personal data.
[8] Charles Fried, "Privacy," *Yale Law Journal* 77 (1968): 477.
[9] See Anita L. Allen, "Taking Liberties: Privacy, Private Choice and Social Contract Theory," *Cincinatti Law Review* 56 (1987): 463.
[10] Charles Fried, *An Anatomy of Values* (1970), p. 140.
[11] Arthur Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (Ann Arbor: University of Michigan Press, 1971), p. 25.
[12] Alan F. Westin, *Privacy and Freedom*, p. 7.
[13] http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

constitutional and tort law. Moreover, none of these spatial, behavioral, decisional or informational distinctions can be absolute. Police can, under certain circumstances, enter one's "private" space. Certain behaviors are typically private, depending on where they take place, or with whom. Thus the state should have no interest in sexual relations between consenting adults in the privacy of one's home, but it may have a significant interest in regulating such behavior in a public place. Decision-making on intimate issues can never be wholly private. Neither can the control of personal information. Whether drawn in spatial, behavioral, decisional or informational terms, each of these boundaries is inherently flexible and contestable. Privacy has to be "balanced" against correlative rights and responsibilities to the community.

It is also useful to reflect on the purposes for the assertion of privacy claims. Here we can distinguish between three overlapping dimensions of the problem: *humanistic, political and instrumental*.[14] Fundamentally privacy claims are made for humanistic reasons. Here the essential concern is to protect the dignity, individuality, integrity or private personality of each and every one of us, regardless of wider implications or consequences. This notion corresponds broadly to what James Rule means by an "aesthetic" conception of privacy or "the restriction of personal information as an end in itself."[15] The fundamental issue is the loss of human dignity, respect and autonomy that results when one loses control over the circumstances under which one's space, behavior, decisions or personal information is intruded upon. These conceptions are at the heart of the privacy movement in virtually every democratic state.

A second dimension, however, is explicitly political. Privacy plays an important role within liberal democratic theory, and is a prerequisite for liberal democratic societies. Alan Westin demonstrates that privacy performs several functions within this general role: it prevents the total politicizing of life; it promotes the freedom of association; it shields scholarship and science from unnecessary interference by government; it permits the use of a secret ballot and protects the voting process by forbidding government surveillance of a citizen's past voting record; it restrains improper police conduct such as physical brutality, compulsory self-incrimination and unreasonable searches and seizures; and it serves also to shield those institutions, such as the press, that operate to keep government accountable.[16] More recently, Paul Schwartz has advanced a similar theory of "constitutive privacy" to protect participation in public life on the Internet.[17]

A third, a somewhat different, purpose is an instrumental or strategic one. The promotion of privacy may also serve to ensure that, in Paul Sieghart's terms, "the

---

[14] Colin J. Bennett, *Regulating Privacy: Data Protection in the United States and Europe* (Cornell: University Press, 1992), pp. 22-37.
[15] James Rule et al. *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980), p. 22.
[16] Alan F. Westin, *Privacy and Freedom,* p. 25.
[17] Paul M. Schwartz, "Privacy and Democracy in Cyberspace. *Vanderbilt Law Review* 52 (6) (1999): 1610-1702.

right people use the right data for the right purposes."[18] When anyone of those conditions is absent, critical rights, interests and services might be jeopardized. This is an explicit concern about information, but it expresses a fundamental assumption that if you can protect the information on which decisions are made about individuals, you can also protect the fairness, integrity and effectiveness of that decision-making process. In contrast to the first two concerns, this aspect of the problem stems not so much from the collection of personal data as from its use and dissemination. In this view, organizations can collect as much personal information as they like, provided there are adequate procedures in place to make sure that the "right people use it for the right purposes."

Thus, privacy has an aesthetic appeal to individual autonomy and dignity. It can be justified in political terms in order to promote the institutions of liberal democracy, and it has a number of instrumental values. Whether justified in philosophical, political or utilitarian terms, privacy is almost always seen as a claim, right of interest of individuals that is threatened by a pervasive set of social and technological forces.

Privacy concerns go back centuries. And specific problems about how certain types of personal information in certain contexts, particularly medical contexts, have been the subject of claim and counterclaim, and regulatory and judicial decision-making for a very long time. Privacy protection as a *public policy question,* however, is of more recent vintage. The issue came to the agenda of advanced industrial states in the late 1960s because of two main characteristics of post-industrialism – bureaucratization and information technology. When those forces reached a critical point in the 1960s and 1970s with the expansion of the state and the computerization of state functions, many Western societies attempted to develop a coordinated public policy approach.

As a public policy question, however, governments tended to define the problem in informational, rather than in spatial, decisional or behavioral terms. Even though some laws (such as in Canada and the US) are entitled "Privacy Acts", statutory protections have historically focussed on the informational dimension of the problem, on the assumption that other aspects of the privacy question can be dealt with by the courts, or can be redefined in informational terms. And in general, policy makers have been more influenced by arguments of instrumental damage, than aesthetic appeal. The position that we all deserve privacy on a humanistic level is abstract. The position that individual interests can be harmed when personal information is processed inappropriately, especially if that position is supported by well-chosen horror stories, can have a more direct political appeal. The history of privacy, as a public policy (rather than a legal or ethical) issue has been dominated by a quite particular understanding of how the issue should be framed. Since the 1960s and 1970s, for better or worse, this informational and instrumental conception of privacy has tended to drive policy

[18] Paul Sieghart, *Privacy and Computers* (London: Latimer, 1976), p. 76.

debate and has set national and international policy choices on a particular trajectory.

The Nature of Information Privacy

The concept of informational privacy arose in the 1960s and 1970s at about the same time that "data protection" (derived from the German, *Datenschutz*) entered the vocabulary of European experts. It is inextricably connected to the information processing capabilities of computers, and to the need to build protective safeguards at a time when large national data integration projects were being contemplated in different European, North American and Australasian states. These projects raised the fears of an omniscient "Big Brother" government with unprecedented surveillance power. Experts in different countries then turned their attention to what should be done. Study commissions were established, such as in Britain, the United States, Canada, Sweden, Australia and elsewhere. These analytical efforts led to the world's first "data protection" or "information privacy" statutes, which have spread around the world in a number of stages. Appendix One presents an up-to-date chronology of the diffusion of these statutes around the different regions of the world.

Concerns differed among these states. However, a closely-knit group of experts in different countries coalesced, shared ideas, and generated a general consensus about the best way to solve the problem. The overall policy goal in every country was to give individuals greater control of the information that is collected, stored, processed and disseminated about them by public, and in some cases, private organizations. This goal was prominent in English-speaking countries, as well as in continental Europe. The concept of *Informationsselbstbestimmung (informational self-determination)* was later developed and given constitutional status in Germany. By the 1980s, therefore, it is possible to discern the set of key assumptions upon which information privacy policy development had rested. Those assumptions are as follows.

First, it is generally impossible to define a priori those data that are inherently worthy of greater protection (sensitive data), because it is the context rather than the properties of the data that lead to privacy risks. The same information can take on very different sensitivity levels in different contexts. My name in the telephone directory may be insensitive; my name on a list of bad credit risks or sex offenders may be very sensitive. For the most part, therefore, law cannot delineate between those types of data that are worthy of protection and those that are not. Public policy, therefore, cannot draw a line between those types of

information that should remain private, and those that may be in the public domain.[19]

Second, privacy is a highly subjective value. Concerns about the protection of personal information vary over time, over jurisdiction, by different ethnic subgroups, by gender and so on. For instance, a name and address in a telephone directory may be insensitive for most people, but may be very sensitive for vulnerable persons who do not want to be monitored and tracked down. Examples of such people would be battered wives, doctors who perform abortions, celebrities, child protection staff, police officers, and so on.

Consequently, public policy cannot second-guess the kinds of personal information about which a given population will be concerned at a given time. The most privacy protection policy can achieve is to give individuals the procedural rights to control their personal information, should they be so motivated. Thus, the content of privacy rights and interests have to be subjectively defined by individuals themselves according to context. Information privacy policy is based inevitably therefore on *procedural*, rather than *substantive*, tenets. It can only put in place the mechanisms by which individuals can assert their own privacy interests and claims, *if they so wish*.

A third conclusion stemmed from the observation that personal information cannot easily be regarded as a property right. Classic economic theorizing would contend that an imperfect marketplace can be rectified in one of two ways. First, one can give a value to personal information so that the costs and benefits of transactions are allocated more appropriately. But is very difficult to establish personal information as property in law, and then to define rights of action over its illegitimate processing. Consumers may have some bargaining power with a direct marketing firm that wants to trade lists; citizens, however, have no bargaining power when faced with a warrant or any other potentially privacy-invasive technique backed up by the sanctions of the state. And at the outset of the privacy debate, it was the power of government agencies that posed the most significant challenges.

It was therefore hard to resist the conclusion that only regulatory intervention might redress the imbalance. Consequently information privacy was generally defined as a problem for public policy, rather than an issue for private choice. More recently, as critiques of the dominant approach have surfaced, the personal data processing practices of the private sector have arisen as equally significant concerns. Moreover, as Internet communications and e-commerce have risen to prominence, so a variety of market-based solutions have been proposed, all of which have been based on the premise that personal information can be given a property value, to be traded and exchanged within the personal information

[19] To some extent this assumption has been challenged by the requirements in the 1995 European Data Protection Directive concerning “sensitive data.”

market.[20] These kinds of arguments had, however, very little influence on the experts and legislators that grappled with the information privacy problem in the 1970s.

A fourth assumption concerns the relationship between information privacy and information security. These and related concepts (data protection, data security, confidentiality etc.) cause considerable confusion. Roger Clarke notes that

> the term 'privacy' is used by some people, particularly security specialists and computer scientists, and especially in the United States, to refer to the security of data against various risks, such as the risks of data being accessed or modified by unauthorised persons. In some cases, it is used even more restrictively, to refer only to the security of data during transmission. These aspects are only a small fraction of the considerations within the field of 'information privacy'. More appropriate terms to use for those concepts are 'data security' and 'data transmission security'. [21]

In other words, data security is a necessary but not a sufficient condition for information privacy. An organization might keep the personal information it collects highly secure, but if that information is highly sensitive and the organization should not be collecting that information in the first place then the individual's information privacy rights are clearly violated. Over time, it became clear that the European concept of "data protection" was being used in much the same way as the term "information privacy." Some, however, see this term as overly technical and concentrating on the "data" rather than the person as the object of "protection."[22]

Finally, there is common consensus that the focus of protection should be the individual, or the "natural person" rather than some other entity. Therefore, organizations and corporations cannot have privacy rights. Some societies (in Scandinavia for example) have attempted to embrace the rights of natural and legal persons in their data protection legislation. Essentially, however, the common consensus is that the goal of information privacy policy – to give individuals greater control over information relating to them – necessitated making a distinction between the subject of the information (the data subject) and the controller of that information (the data controller). This distinction is by no means unambiguous; there are plenty of instances where an individual might where both hats at any one time. Nevertheless, information privacy policy did develop (domestically and internationally) on the assumption that the interests of

---

[20] See, Rule James and Lawrence Hunter. "Towards a Property Right in Personal Data," in Colin J. Bennett and Rebecca Grant (eds.) *Visions of Privacy: Policy Choices for the Digital Age.* (Toronto: University of Toronto Press, 1999). Kenneth Laudon , "Markets and Privacy." Communications of the ACM 39 (1996): 92-104; Lawrence Lessig, *Code and Other Laws of Cyberspace. (*New York: Basic Books, 1999).

[21] http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

[22] See Roger Clarke's discussion, ibid.

groups, corporations and other organizations in the information about them can and should be dealt with through other legal instruments.

These five assumptions would not be accepted by every scholar and commentator. They were and are deeply contested. The basic point at this juncture in the analysis is that privacy protection policy was placed on a particular trajectory as a result of some common assumptions about the nature of the information privacy problem. The policy responses that developed (data protection or information privacy statutes) for the most part were driven by a shared understanding among elites about the nature of the problem they were facing. Those shared assumptions, based on fundamental liberal principles, have had some profound and widespread policy implications in every advanced industrial state. Assuming, then, that we each have information privacy rights, claims or interests, how can one frame a public policy to protect those rights?

The Fair Information Principles Doctrine

Once these, and other, assumptions are accepted about how one can and cannot develop public policy on privacy, a logic is set in motion that leads inevitably to a basic set of procedural rights. Hence a set of "fair information principles" evolved that logically had to converge around a set of key and basic principles. The historical origins of fair information practices can be briefly traced to policy analysis in Europe and the United States in the late 1960s and early 1970s.[23] Those experts who were attempting to resolve this issue in national arenas shared a strong desire to draw lessons from their counterparts overseas. This intense process of lesson-drawing produced an international consensus on how best to resolve the privacy problem through public policy.

While the codification of the principles may vary, they essentially boil down to the following tenets.[24] An organization (public or private):

- must be *accountable* for all the personal information in its possession
- should *identify the purposes* for which the information is processed at or before the time of collection
- should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances)
- should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes

[23] Colin J. Bennett, *Regulating Privacy,* pp. 95-115.
[24] Colin J. Bennett and Rebecca Grant (eds). *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999), p. 6.

- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (*the finality principle)*
- should *retain* information only as long as necessary
- should ensure that personal information is kept *accurate, complete and up-to-date*
- should protect personal information with appropriate *security safeguards*
- should be *open* about its policies and practices and maintain no secret information system
- should allow data subjects *access* to their personal information, with an ability to amend it is inaccurate, incomplete or obsolete.

These principles are, however, relative. However conceptualized, privacy is not an absolute right; it must be balanced against correlative rights and obligations to the community. Privacy protection, therefore, is the "process of finding appropriate balances between privacy and multiple competing interests."[25]

The fair information principles appear either explicitly or implicitly within all national data protection laws, including those in the US, Australia, New Zealand and Canada that are called 'Privacy' Acts. They appear in self-regulatory codes and standards, such as that published by the Canadian Standards Association which forms the basis of Canada's new private sector data protection law.[26] But they have principally spread as a result of international agreements. Early in the debates, it was recognized that information privacy couldn't simply be regarded as a domestic policy problem. The increasing ease with which personal data might be transmitted outside the borders of the country of origin has produced an interesting history of international harmonization efforts, and a concomitant effort to regulate transborder data flows. In the 1980s, these harmonization efforts were reflected in two international agreements, the 1981 *Guidelines from the Organization for Economic Cooperation and Development*,[27] and the 1981 *Convention* from the Council of Europe.[28] In the 1990s, these efforts were extended through the 1995 *Directive on Data Protection* from the European Union which tries to harmonize European data protection law according to a higher standard of protection, and to impose that standard on any country within which personal data on European citizens might be processed.[29]

---

[25] http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

[26] Canadian Standards Association, *Model Code for the Protection of Personal Information - Q830* (Rexdale: CSA, 1996)

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

[28] Council of Europe. *Convention for the Protection of Individuals with Regard toAutomatic Processing of Personal Data.* Strasbourg: Council of Europe, 1981.

[29] Articles 25 and 26 of the Directive stipulate that personal data on Europeans should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection." European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.* Brussels: OJ No. L281.24 October 1995. (The EU Data Protection Directive).

Appendix One contains a comprehensive overview of the state of personal data protection legislation in 2001. It demonstrates how rapidly data protection law has diffused around the advanced industrial world in the 1980s and 1990s, and how societies more commonly characterized as "developing" are now beginning to pass similar laws.

Despite this harmonization there are, of course, continuing debates about how the FIPS doctrine should be translated into statutory language. There are disputes for example: about how to regulate the secondary uses of personal data -- through a standard of relevance, or through specific provisions about legitimate custodians; about the limitation on collection principle and to what extent the organization should be obliged to justify the relevance of the data for specific purposes; about the circumstances under which "express" rather than "implied" consent should be required; and about the distinction between collection, use and disclosure of information, and whether indeed these distinctions make sense and should not be subsumed under the overarching concept of "processing." How these and other statutory issues are dealt with will, of course, have profound implications for the implementation of privacy protection standards within any one jurisdiction.

The laws have also differed on the extent of organizational coverage -- those in North America and Australia have historically mainly regulated public sector agencies, whereas those elsewhere (especially in Europe) encompass all organizations. This distinction is rapidly changing, however, as countries like Canada, Australia and Japan have moved to regulate private sector practices. Laws have also differed on the extent to which they regulate non-computerized files (i.e. the manila folder in the filing cabinet). This distinction is also eroding.

Most notably they have differed with regard to the policy instruments established for oversight and regulation. Most countries (with the notable exception of the United States) have set up small privacy or data protection agencies with varying oversight, advisory or regulatory powers. Some of these agencies have strong enforcement and regulatory powers; others act as more advisory "ombudsman-like" bodies. Some are headed by a collective commission (such as in France), others by a single "Privacy Commissioner" or "Data Protection Commissioner." In some regulatory regimes, instruments of "self-regulation" (such as company codes of practice) play a more important role than in others.

Any regulatory privacy protection scheme therefore needs to ascertain the correct mix of the following seven functions and ensure that the mix is compatible with existing constitutional and administrative legal requirements:

- The Receipt, Investigation and Resolution of Complaints
- Audit Powers

- Enforcement Powers
- The Receipt, Verification and Approval of Privacy Codes
- Advice on the Privacy Implications of New Technologies
- Public Education and Research
- Sanctions and Remedies

One of the effects of the 1995 European Data Protection Directive has been to extend the process of policy convergence beyond the level of basic statutory principles. This Directive also pushes for greater conformity in the ways in which these principles are enforced through a "supervisory authority." Moreover, the principle of independent oversight is also regarded as a test of the "adequacy" of data protection in non-European countries. The process of convergence of data protection norms is extending geographically and deepening in meaning and content.[30] We now see a convergence on principles, on the scope, and on the implementation mechanisms.

It can be finally noted that this deep and extending consensus surrounding the FIPs doctrine has occurred against a backdrop of some profound skepticism as to whether it can actually protect personal privacy and stem the inexorable tide of surveillance. Authors who have examined the issue from a broader sociological perspective have continuously raised the concern that contemporary information privacy legislation is designed to manage the processing of personal data, rather than to limit it. Thus, David Lyon has contended that "the concept of privacy is inadequate to cover what is at stake in the debate over contemporary surveillance."[31] From the perspective of those interested in understanding and curtailing excessive surveillance, the formulation of the privacy problem in terms of trying to strike the right "balance" between privacy and organizational demands for personal information hardly addresses the deeper issue. They cannot halt surveillance, or the more precise process of "dataveillance," to use a term coined by Roger Clarke.[32] Information privacy policies may produce a fairer and more efficient use and management of personal data, but they cannot control the voracious and inherent appetite of modern organizations for more and more increasingly refined personal information. And this information is increasingly extracted through intrusive biometric technologies that are altering the very boundaries between the self and the outside world. [33]

---

[30] See, Colin J. Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" In P. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* (Cambridge: MIT Press, 1997).

[31] David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994), p. 196.

[32] Roger Clarke, "Information Technology and Dataveillance" *Communications of the ACM* 31 (5): 498-512.

[33] See Roger Clarke's critique at : http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html#OECDD

The Implementation of Fair Information Principles in Canada

The forces that brought the privacy issue to the agenda in Canada were generally the same as those in other countries: the computerization of personal information systems (especially in the public sector), the development of a universal identifier (the Social Insurance Number) and a growing sense of alienation from the agencies of government. In the 1970s, there followed a quiet but wide-ranging debate about the privacy issue.[34]

The first privacy legislation at the federal level was actually contained in Part IV of the 1977 Canadian Human Rights Act, which established the office of the Privacy Commissioner, a member of the Canadian Human Rights Commission, whose main task was to receive complaints from the general public, conduct investigations and make recommendations to Parliament. While Part IV succeeded in codifying fair information principles in legislation for the first time, privacy probably sat uneasily within a statute devoted to the question of discrimination, a related but obviously more controversial issue that tended to overshadow the importance of privacy protection.

Parallel debates over a federal access to information act in the early 1980s raised immediate questions about the compatibility between such legislation and the privacy standards within Part IV. The current 1982 Privacy Act, therefore, flows from a belief that data protection should be a corollary to freedom of information, and that the various exemptions in both pieces of legislation should be internally consistent. Bill C-43, incorporating an Access to Information Act and a revised Privacy Act, thus institutionalized the Canadian innovation of legislating access to information and privacy protection within the same statutory framework.

This model was later copied by some of the provinces: by Quebec in 1982, by Ontario in 1988, by British Columbia in 1993, by Alberta in 1995 and by Manitoba in 1997. By the end of 2001, every Canadian province and territory will have in place a legislated privacy protection policy for the personal information held by public agencies. Appendix Two presents the current profile of privacy protection legislation in Canada, as applied to the public sector.

The passage in 1993 of Quebec's Bill 68, *An Act Respecting the protection of personal information in the private sector*, gave effect to the information privacy rights incorporated in the new Civil Code, and made Quebec the first jurisdiction in North America to produce comprehensive data protection rules for the *private* sector. Bill 68 applies the fair information principles to all pieces of personal information collected, held, used or distributed by enterprises engaged in an "organized economic activity." The Commission d'Accès à l'Information du Québec, the body established under the 1982 public sector access and privacy

[34] Colin J. Bennett, "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing" *Canadian Public Administration* 33 (1990): 551-570.

law, oversees its implementation, hears complaints and renders binding decisions.

After Quebec's action, Canada became the only country in which the scope of privacy protection in one of its member jurisdictions exceeded that of the federal government. In the rest of the country, there were only a few isolated statutes relating to specific sectors, such as consumer credit industry, and a sprinkling of common law remedies and constitutional provisions of potential relevance. In the 1990s, with the exception of Quebec, privacy protection in the private sector was largely dependent on the implementation of a set of voluntary and sectoral codes of practice developed according to the framework of the 1981 *OECD Guidelines.*[35] Throughout the decade, a number of political, international, technological and legislative developments convinced federal policy makers that this incoherent policy could not be allowed to continue.

First, the passage of a *Data Protection Directive* from the European Union meant that no jurisdiction in Canada (save Quebec) could plausibly claim an "adequate level of protection" and therefore safely process personal data transmitted from EU countries; data protection has some significant trade implications. Second, the passage of the Quebec legislation created an "unlevel playing field" within the Canadian federation, creating uncertainties and transaction costs for businesses that operate in different provinces. Third, the publication of a series of public opinion surveys demonstrated that the general public regards privacy protection as a matter of major concern.[36] Fourth, the commercialization of some governmental functions had undermined the implementation of public sector data protection law and the ability of Canada's privacy commissioners to ensure the protection of personal data when it is transferred to a private contractor. Finally, the debates over the development and character of the Canadian "information highway" exposed the need for a common set of "rules of the road" for the networked and distributed computing and communications environment of the 21st century.[37]

The result of the subsequent government commitments, policy analysis and legislative process was the *Protection of Personal Information and Electronic Documents Act* (Bill C-6) which came into force on January 1, 2001.[38] With this legislation, Canada then took a significant step towards providing a more complete set of privacy rights for its citizens. It is based on the CSA's privacy standard, which contains Canada's own version of the fair information principles. While this law fills in some very important gaps in the existing patchwork of

---

[35] See, Colin J. Bennett, *Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association* (Rexdale: CSA, PLUS 8830, 1995).
[36] Principally, Ekos and Associates, *Privacy Revealed: The Canadian Privacy Survey* (Ottawa: Ekos, 1993).
[37] Information Highway Advisory Council, *Communication, Community, Content: The Challenge of the Information Highway* (Ottawa: Minister of Supply and Services Canada, 1995).
[38] See http://e-com.ic.gc.ca for a copy of the legislation and related official documents and news releases.

federal and provincial statutes that have been passed over the last thirty years or so, it does not, and cannot, regulate the entire Canadian private sector. On January 1, 2001 only the following businesses will be obliged to comply: banks, telecommunications, broadcasting, airlines, and transportation companies, as well as any company that sells personal information across provincial or international borders.

After 3 years, the law will apply to all commercial activities by the private sector, including companies under provincial or territorial jurisdiction, unless they are covered by "substantially similar" provincial or territorial law; the federal government has already declared the 1993 private sector legislation in Quebec as meeting this standard. So, if the provinces and territories fail to pass "substantially similar" legislation in the next three years, *PIPEDA* will apply by default to the retail sector, the manufacturing sector, some financial institutions, video-rental outlets, and indeed to most businesses that have face-to-face relations with consumers. Thus the provincial governments are now deciding whether they want to pass their own statutes (either generally, or for specific sectors such as health) or to do nothing and surrender an important constitutional power to the federal government, a decision that would possibly have implications for federal/provincial relations beyond that of privacy. Appendices Three and Four contain an overview of the current progress at the provincial level for general private sector legislation and specific health information legislation, respectively.

Two broad conclusions are relevant about the historical progress of information privacy legislation in Canada. First, the relative lateness of Canadian efforts to regulate the private sector has meant that federal and provincial legislation has been forced to comply with already established international standards, even though the FIPs doctrine has been shaped by some distinctively Canadian concerns and interests. Second, although the rest of this paper will focus on public sector issues, it is readily apparent that the distinction between the sectors has been rapidly eroding, to the extent that there will need to be renewed attention to the compatibility of existing public sector privacy provisions with emerging private sector rules.

Privacy Policy Management Tools

Information privacy law is, therefore, based on some very similar assumptions and basic principles. Increasingly it is being overseen by independent oversight agencies which have been forced to operate in increasingly similar ways and with similar powers. Twenty years ago, however, the consensus about the issue extended merely to the basic requirements of a data protection, or information privacy, law. The enactment in a general statute of the fair information principles, and their enforcement and oversight through an independent data

protection agency, were generally regarded as both necessary and sufficient to deal with the problem.

Over the last twenty years, a number of factors have necessitated a range of more specific policy instruments for the protection of privacy that might be applied within both private and public sectors. First, the move from the "databank" to the more decentralized networked information systems has provided a range of new data processing and manipulation techniques. Second, the distinction between public and private sectors have eroded as a result of outsourcing and privatization initiatives. Third, the staggering variety of intrusive surveillance techniques has subtly different privacy implications necessitating more finely tuned privacy solutions. There is now a complicated "privacy tool kit" comprising different privacy-enhancing technologies and self-regulatory approaches.[39]

Many of these tools have been developed to encourage private sector compliance with data protection norms. But all have some relevance to government agencies, particularly those involved with electronic service delivery and other "e-government" applications. But there is a confusion over the way these various instruments have been described. The following attempts to distinguish between these various instruments in terms of functions they are designed to perform within an overall privacy protection framework. I distinguish between five different instruments:

- Privacy Commitments
- Privacy Codes of Practice
- Privacy Standards
- Privacy Seals
- Privacy Impact Assessments

Privacy Commitments

Often called "codes", "guidelines" or some other title that would indicate a more thorough self-regulatory function, privacy commitments perform no other function than to indicate to clients, consumers and regulators that the organization has considered privacy protection at some level, and believed that it would be good policy to state a set of commitments. Privacy commitments do no more than place on the record what the organization believes it does with a consumer's or client's personal data. Many examples can be found in the privacy statements to be found on contemporary public and private sector websites.

[39] See, Bennett and Grant (eds.) *Visions of Privacy.* See the companion paper. "ID Authentication and Privacy" by Roger Clarke for a complete discussion of privacy-enhancing technologies.

Privacy commitments tend to be relatively brief pledges, and are often designed for external consumption rather than to affect internal organizational functioning. They also have sometimes not been produced as a result of a careful and thorough analysis of an organization's personal information holdings. They tend to be statements of what top management believes is happening (and ought to happen) rather than comprehensive instruments of self-regulation that bind employees and reflect a deep organizational culture that respects privacy. Privacy commitments may inform data subjects about certain rights to access and correction, about how to opt-out of disclosures and so on. But they may sometimes finesse crucial questions about how those rights might be exercised.

Privacy commitments need not be symbolic. Frequently it is quite useful for an organization to state its policies in a brief, open and "user-friendly" manner. Privacy commitments can supplement more detailed and thorough codes of practice, that are based on a realistic and comprehensive analysis of how an organization collects, uses, stores and processes personal information. In the context of electronic government, the content and wording of privacy commitments by government agencies will take on an increasing importance.

Privacy Codes of Practice

The term "code of practice" should be reserved for codified policies that not only state commitments to the outside world, but also bind employees to these obligations. There are probably more instruments that can be called "privacy codes" in Canada than in any other society.[40] I have concluded that "almost by default, Canada has become the only country in the advanced industrial world that has begun seriously the process of promoting privacy protection from the bottom up."[41] Most were developed in the absence of a regulatory framework, in order to avoid or anticipate further regulatory intervention. Codes of practice are, and will continue to be, a feature of privacy protection policy in Canada. The question is, what role should they play under a legislated regime?

Peter Hustinx, the President of the Netherlands *Registratiekamer* (the Dutch Data Protection Authority), has concluded that codes of practice do offer some clear advantages even within a legislated data protection regime. The procedure of negotiating codes enhances the understanding of the privacy problem within different sectors. It also allows the data protection authority to gain a better appreciation of the relevant privacy issues and directly to influence the self-regulatory mechanisms. Codes are quite flexible instruments and once negotiated can be adapted to changing economic and technological developments. Codes also allow organizations to publicize their privacy policies and to remove suspicions about the improper collection, processing and dissemination of personal data. They allow an "enhanced measure of

[40] Bennett, *Implementing Privacy Codes of Practice,* pp. 119-20.
[41] Ibid., p. 56.

understanding on both sides."[42] Similar advantages have been noted by Canadian analyses of the subject.[43]

Privacy codes may also perform crucial functions within the framework of statutory data protection regimes, such as those of the Netherlands, New Zealand, Ireland and the UK. Article 27 of the European Directive requires the European Commission and Member States to "encourage the drawing up of codes of conduct intended to contribute to the proper implementation of...national provisions...taking account of the specific features of various sectors." Terminology is again confusing, but we can make a distinction between five kinds of privacy code according to the scope of application: the organizational code, the sectoral code, the functional code, the professional code and the technological code.

The simplest instrument is the *organizational code* that applies to one agency that is bounded by a clear organizational structure. Typically these codes have been developed by large, high profile organizations whose practices have come under scrutiny from the media or privacy advocates, or who may have received a volume of consumer complaints.[44]

A second, a perhaps more important category is that of the *sectoral code.* The major defining feature of the sectoral code is that there is a broad consonance of economic interest and function, and by extension a similarity in the kinds of personal information collected and processed. Sectoral codes permit, therefore, a more refined set of rules tailored to the issues within each sector. Sectors also tend to operate within an already defined set of regulatory institutions and rules, which in turn have established a relatively cohesive policy community that is engaged in an ongoing basis in the negotiation of new rules for the sector and the implementation of existing rules. The model codes of industries, such as banking, life insurance, cable television and so on, provide the most obvious examples to date in Canada. Sectoral codes have begun to emerge within public and private industries that operate on a global scale, such as those of the International Air Traffic Association (IATA). They have also emerged in some public, and quasi-public sectors.[45]

The final three types of code, clearly span these more traditional sectoral boundaries. What we call *functional codes* are defined less by economic sector

---

[42] Peter Hustinx, "The Use and Impact of Codes of Conduct in the Netherlands," (paper presented to the 16th International Conference on Data Protection, the Hague, 6-8 September 1994), p. 3.

[43] Bennett, *Implementing Privacy Codes of Practice,* p. 51; Lola Fabowale, *Voluntary Codes: A Viable Alternative to Government Legislation* (Ottawa: Public Interest Advocacy Centre, May 1994).

[44] See www.privacyexchange.org for examples of company codes of practice, as well as for evidence of the variety of instruments that fall within this broad classification.

[45] The New Zealand Privacy Commissioner, for example, has negotiated codes of practice in the health and educational sectors. See: http://www.privacy.org.nz

and more by the practice in which the organization is engaged. The most obvious example is direct-mail and telemarketing. The direct-marketing associations in the United States, Canada and many other countries represent businesses in a wide and growing number of sectors. Both have responded to long-standing concerns about direct marketing by developing privacy codes of practice that have tried to regulate members and keep up-to-date with evolving technologies, including the Internet. The Canadian Marketing Association states that its code is "compulsory" because members are expected to sign a commitment to its provisions and may be expelled from the association if found in violation of its provisions.[46]

There is really no functional difference between technological codes of practice and the "guidelines" developed by government to apply privacy principles to new practices. For example, several jurisdictions, including Ontario, have published guidelines for the conduct of "data matching" programs.[47] Data-matching involves the comparison of discrete systems of records in order to identify individuals who might be of interest to an agency for some reason, and has been a matter of serious concern for data protection agencies throughout the 1980s and 1990s. These and other computer matching guidelines at the federal level and in other countries require prospective computer matches to go through a careful assessment process to ensure compliance with information privacy principles. The assessment will cover issues of notification, data retention, and security. In addition the business case has to be thoroughly investigated and justified. In some jurisdictions, a formal cost-benefit analysis should be conducted.[48]

A fourth category of privacy codes includes those that have been developed by professional societies. Typically, these codes apply to those directly engaged in information-processing activities. *Professional codes* have been developed for information processing professionals, for survey researchers, for market researchers, and for a range of health and welfare-related professionals.[49] They are created by professional, rather than trade, associations and can be reinforced by some significant disciplinary measures entailing a loss of professional reputation. They may also be incorporated into larger sets of ethical guidelines and codes of conduct.

A final set of codes can be defined not by function, but by *technological practice.* As new potentially intrusive technologies have entered society, so codes have developed to deal with the specific privacy problems associated with their application and distribution. *Technological codes* typically apply to very new

---

[46] www.cdma.org

[47] Ontario Corporate Freedom of Information and Privacy Office, *Enhancing Privacy: Computer Matching of Personal Information Guideline,* May 1994.

[48] For a review of data matching policies see, Colin J. Bennett, "The Public Surveillance of Personal Data," in D. Lyon and E. Zureik (eds), *Surveillance, Computers and Privacy* (Minneapolis: University of Minnesota Press, 1996).

[49] An example is the privacy code of the Canadian Medical Association at: www.cma.ca

applications. They may be developed outside a regulatory framework. In 1992, the Canadian banks developed a code for the governance of electronic funds transfers (EFT). Smart card technology is also amenable to specific regulation through privacy codes of practice.[50]

Increasingly we see such codes within societies that already have statutory data protection. The British Data Protection Registrar has developed a code of practice on Closed Circuit Television cameras (CCTV). Another example of a governmental code of practice is the "Electronic Service Delivery Privacy Standard" developed in order to protect the privacy of Ontarians when the provision of government services is redesigned to involve private sector partners and new service delivery technologies. The project envisages the use of one or more service channels to provide simultaneous single-window access to services such as license registrations, updating of personal registration data, the collection of fees and so on. This instrument reads exactly the same as a "privacy code of practice." It is mandatory for participating ministries, and developed within the legislative framework of the Ontario Freedom of Information and Protection of Privacy Act. But it is also based on the 10 principles within the Canadian Standards Association's *Model Code for the Protection of Personal Information.* Those principles are then elaborated and interpreted to apply to the electronic service delivery function.[51]

In conclusion, there are now many instruments (called codes, guidelines, standards), all of which perform a similar role, to apply a given set of privacy protection norms to a particular organization, sector, function, profession or technology. These instruments differ from privacy commitments in the simple fact that they may embody a set of rules for employees, members or member organizations to follow. They state more than a simple claim; they also provide important guidance about correct procedure and behavior based on a version of the information privacy principles. But privacy codes of all kinds have been developed for different motivations and have no consistent format, and have been formulated with varying amounts of care and analysis. Absent a statutory framework, procedures for implementation, complaint resolution and communication vary substantially.[52] Experience also suggests that codes of each sort can play an important role within the context of an existing data protection legal regime. They can assist in the application of basic data protection norms to increasingly complicated and fluid organizational and technological environments.

[50] The Association of Card Technologies in Canada is an example. See www.actcanada.com
[51] http://www.gov.on.ca/mbs/english/fip/pub/esd1.html
[52] See, Bennett, *Implementing Privacy Codes of Practice.*

Privacy Standards

The phenomenon of a privacy standard extends the self-regulatory code of practice in some important ways. Standards imply not only a common yardstick of measurement, but also a process through which organizational claims about adherence to a set of norms can be more objectively tested. Standardization means a common code, but also a conformity assessment procedure that might more effectively determine that an organization "says what it does, and does what it says."

Technical standards have played an important role in computer security for some time. One example would be the certification system established under the British Standard, BS7799. This standard comprises a code of practice for computer security, as well as a standard specification for security management systems, which includes a risk analysis for the different categories of information stored by the organization. There is also a certification scheme, called 'c:cure' that can operate in conjunction with the ISO 9000 range of generic quality management standards.[53]

The idea of a more general privacy standard, however, that could incorporate the entire range of privacy protection principles is a more recent innovation. The first comprehensive privacy standard was negotiated in Canada. In 1992, representatives of the major trade associations joined with key government officials and consumer representatives ostensibly to harmonize the codes of practice that had already been developed and also in recognition that the process of code development under the *OECD Guidelines* had not been successful. Later that year, it was decided to formalize the process by using the more institutionalized process of standard development under the Canadian Standards Association (CSA) which then acted as facilitator and secretariat. The *Model Code for the Protection of Personal Information* was finally passed by the Technical Committee without dissent on September 20, 1995, and was subsequently approved as a "National Standard of Canada" by the Standards Council of Canada, and was published in March 1996.

For some, it was envisaged that the code should operate as a *standard.* Within CSA, the Quality Management Institute (QMI) registers companies to the series of "quality assurance" standards, principally those within the increasingly popular ISO 9000 series. There are some interesting parallels between the goals of "total quality management" and the implementation of fair information principles. The QMI announced in September 1996 a three-tier recognition program. Soon, however, the federal government announced its intentions to introduce federal legislation based on the standard, so there was never a pure test of whether a market mechanism alone would encourage registrations.

[53] See http://www.c-cure.org/bsframes.htm

Even though few organizations have so far demonstrated an interest in this program, there might in fact be several incentives to adopt a privacy standard. Moral suasion, the desire to avoid adverse publicity and the possible use of privacy protection for competitive advantage are the kinds of incentives that operate at the moment. But 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. For instance, if a private contractor processed personal data under government contract, a simple way for the government agency to ensure the adherence to the same data protection standards as apply in government would be to require the contractor to register to the standard. The same would apply to international contracts and the transborder flow of data. It is possible that European data protection agencies could also enforce Article 25 of the new *EU Data Protection Directive* by requiring any recipient of European data in Canada to be registered to the *CSA Model Code.*

In Canada, the CSA standard was also used to broker a *de facto* agreement between the federal government and the provinces over some basic legislative principles, something that would have been exceedingly difficult within a formal federal-provincial law making exercise. There are some similar patterns in other countries. General standards, similar to that of the CSA, have more recently been negotiated in Australia and Japan. In 1999 the Japanese Standards Association released JIS Q 15001, which adapts the environmental management standard, ISO 14001 to personal data protection.[54] In Australia, a set of National Privacy Principles, similar to those of the CSA, were issued in February 1998 by the Privacy Commissioner. Although there was no explicit certification scheme offered, the overall aim was to get Australian business to adopt these National Principles in a formal manner. As in Canada, this initiative has been overtaken by a more general legislative approach.[55]

A further attempted extension of the standard has occurred at the international level. 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.[56] The expected resolution, however, did not materialize mainly as a result of some very intensive lobbying by certain US multinational interests. The AHAG was

[54] See, Jos Dumortier and Caroline Goemans, "Data Privacy and Standardization" Discussion paper prepared for the CEN/ISSS Open Seminar on Data Protection, Brussels 23/24 March, 2000. http://www.law.kuleuven.ac.be.icri

[55] http://www.privacy.gov.au/private/index.html#4.1

[56] The arguments for such as standard were provided in: Colin J. Bennett, *Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada* (1997) at: http://www.cous.uvic.ca/poli/bennett/research/ISO.htm

maintained for another year in order to study the issue further, but was disbanded in June 1999.

Since then, the initiative has moved to Europe. The Centre Européanne de Normalisations (CEN), responsible for the negotiation of standards within Europe, has begun to study the feasibility of an international privacy standard, supported by the Article 29 Working Party which is responsible for overseeing the implementation of the European Data Protection Directive.[57] In March 2000, it was proposed to begin standardization activities along three paths: a general data protection standard which would set out practical operational steps to taken by an organization in order to comply with relevant data protection legislation, principally the EU Directive; a series of sector-specific initiatives in key areas such as health information and human resources management; and task specific initiatives mainly related to the online environment.[58] A working group of the CEN's Committee on Standardization has been working throughout 2001 on this initiative.

Proponents contend that an international standard would hold a number of advantages over national models. It would carry far greater weight and credibility in both Europe and the United States. It would attract attention and international certification efforts from different national standards bodies. It would also provide a more reliable mechanism for the implementation of Article 25 of the European data protection directive. The scrutiny of laws and contracts provides no assurances to European data protection agencies that data protection rules are complied with in the receiving jurisdiction. Required registration to a standard, which would oblige independent and regular auditing, would provide a greater certainty that "adequate" data protection is being practiced by the receiving organization (public or private), wherever it is located. This does, of course, require concomitant efforts to harmonize systems of conformity assessment and auditor certification. At the end of the day, bilateral and multilateral mutual recognition agreements need also to be negotiated to ensure that domestic conformity assessment programs are commonly respected.[59]

Privacy Seals

One logical corollary of any standard is a commonly understood mark, symbol or cachet that can be awarded to any organization that is successfully certified or registered. The Canadian Standards Association's "mark" is generally regarded as a symbol of quality within the Canadian marketplace, and its use is jealously

---

[57] 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

[58] See, Dumortier and Goemans, "Data Privacy and Standardization."

[59] See. Colin J. Bennett, "An International Standard for the Protection of Personal Data" Objections to the Objections." Paper give at CFP 2000, Toronto, April 2000 at: http://www.cfp2000.org/program/

guarded and restricted to those companies that have followed an appropriate registration or certification process. The "claim" that an organization might make about its compliance is also carefully monitored.

The development of a specific "mark" or "seal" for privacy protection has, however, proliferated on the Internet. Several schemes can be mentioned. The most notable have been developed by the TRUSTe organization and by the Better Business Bureau (BBB) Online. These programs are built on the premise that consumers should be able to have consistent disclosure of privacy practices from all sites with which they interact. To build this consistency, these licensing programs require participating Web sites to post a privacy policy disclosing their online information-gathering and dissemination practices. A cornerstone of these programs is an online branded seal displayed by member Web sites and which is awarded only to sites that adhere to established privacy principles and agree to comply with ongoing oversight and dispute resolution procedures.[60]

Another example of a seal program is the "Privacy Protection (PPM) Mark" system that was devised in Japan in 1998.[61] This system was conceived to apply to any organization, not just those operating on the Internet or in the private sector. The Japan Information Processing Development Center (JIPDEC) serves as the granting organization, and is responsible for examining private enterprises' applications for the privacy mark, certifying them, and operating this system appropriately. The system also allows for a designated organization, such as a trade association, to oversee the application of the PPM within its own sphere of competence. Besides the above requirement, an enterprise must have a compliance program complying with MITI's "Guidelines for Protection of Personal Information Related to Computer Processing in the Private Sector"[62] (or the industry guidelines established based on the Guidelines by the business group to which the enterprise belongs). It must also demonstrate that personal information is appropriately managed based on the compliance program or that a feasible structure has been established. The certification is then in existence for two years.

Privacy protection marks or seals certainly represent an extension of the code or practice and the standard. Ideally, privacy seals should operate to distinguish the compliant from the non-compliant and present consumers and clients with clear statement by which to make informed choices in the marketplace, and particularly in the online marketplace. This raises the question of whether they have any relevance for government organizations. In theory, there is no reason why the relevant privacy protection authority within a jurisdiction could not use existing seal programs in order to encourage compliance with legislation. Privacy and data protection commissioners do not have the resources to monitor compliance on an ongoing basis. In the context of electronic service delivery,

[60] www.truste.org; www.bbbonline.org
[61] http://www.jipdec.or.jp/security/privacy/pamph-e.html
[62] MITI Notification No.98 on March 4, 1997: *Personal Information Protection Guidelines*

the use of seal programs may bolster client confidence, even though a market mechanism is rarely in play. Current seal programs, however, have not inspired great confidence. Furthermore, the more privacy seal programs in existence, the more the consumer will be confused, and the more difficult will it be for any one system to achieve a reputation as the methodology by which privacy-protective practices can be claimed and assured.

Ideally these four instruments (commitments, codes, standards, seals) should be cumulative. The self-regulatory process should involve: 1) An agreement and statement of organizational policy; 2) a codification of that policy throughout the organization or sector; 3) a verification of those practices through some external and independent conformity assessment process; and 4) the assignment of a "seal of good house-keeping." More often than not, however, public claims are made without adequate internal analysis, or external auditing. And privacy seals are invariably awarded without a proper codification and verification of organizational practices. Therefore, the number of organizations that have engaged in privacy self-regulation in this cumulative and logical manner are very few.

Privacy Impact Assessments

The final instrument has been more clearly developed with public sector personal data processing applications in mind. Privacy Impact Assessments (PIAs) have received a great deal of attention in data protection circles as useful ways to anticipate privacy problems before systems are developed. PIAs therefore have an anticipatory function, and should be used to alert organizations (public and private) of the potential legislative implications and public reactions to proposed schemes. According to David Flaherty, "the idea is to require the preparation of privacy impact assessments for new products, practices, databases and delivery systems involving personal information…..Ultimately, a privacy impact assessment is a risk-assessment tool for decision-makers to address not only the legal, but the moral and ethical, issues posed by whatever is being proposed."[63]

The country with perhaps the most experience of PIAs is New Zealand. Blair Steward of the New Zealand Privacy Commissioner's Office has found that PIAs may be desirable in assessing risks:

- Arising from a new technology or the convergence of existing technologies (for instance, electronic road pricing or other intelligent transportation system applications, person-location or person-tracking using a cellphone or GPS technologies);

[63] David H. Flaherty, "Privacy Impact Assessments: An Essential Tool for Data Protection," in S. Perrin, H. Black, D. H. Flaherty and T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001).

- Where a known privacy-intrusive technology is to be used in new circumstances (for instance, expanding data matching or drug testing, installation of CCTV in public places); and

- In a major endeavor or changing practice having significant privacy effects (for instance, a proposal to merge major public registries into a "super registry", to adopt a national ID card, to confer state powers to access computer systems).[64]

For PIA's to be effectively and consistently applied, however, guidelines need to be followed concerning the type of analysis necessary. This may include: the personal information in which the proposed scheme deals; the sources from which this information is to be obtained; the circumstances in which collection is to take place; the processing (including collection or inter-connection) of that information; the intended uses of the information held or thus produced; the proposed recipients and their intended use of it; the circumstances in which processing, use and disclosure is to take place; and the safeguards which will be operated against unauthorized access, use, disclosure, modification or loss.

The PIA guidelines issued by Management Board Secretariat in Ontario are some of the most comprehensive in the world. They are quite innovative in that they require a PIA wherever there are "proposals that entail major increases in the scope of collection, use and disclosure of personal information, through program integration, broadening of target populations, a significant shift toward indirect collection of personal information, or the expansion of data collection for new eligibility criteria or program administration functions."[65] Unlike some other formulations, where the PIA is completed before any system design, for Ontario policy, "the privacy impact assessment is best approached as an evolving document which will grow increasingly detailed over time."[66]

The value of PIAs for managers is that they can significantly reduce "risk." The risks associated with failing to consider the privacy implications of a given proposal can take many forms:

- Failure to comply with either the letter or the spirit of the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Privacy Act*, or fair information principles more generally, resulting in criticism from the Information and Privacy Commissioner.
- Stimulating public outcry as a result of a perceived loss of privacy or a failure to meet expectations with regard to the protection of personal information;

[64] http://www.privacy.org.nz/privword/pwtop.html
[65] http://www.gov.on.ca/MBS/english/fip/pia/PIA.doc
[66] Ibid.

- Loss of credibility or public confidence where the public feels that a proposed program or project has not adequately considered or addressed privacy concerns;
- Underestimating privacy requirements such that systems need to be redesigned or retrofitted late in the development stage at considerable expense.[67]

Non-compliance with a given set of information privacy norms can be quite objectively evaluated. But privacy protection is not, generally, as measurable as environmental protection. PIAs inevitably, therefore, entail a good deal of quite subjective and speculative analysis. Public reaction to privacy invasions is often very difficult to gauge and predict.

Conclusion: Balancing Privacy with Agency Goals

From the preceding historical and comparative overview we can draw some useful lessons about the reasons why privacy has become such a salient question in jurisdictions such as Ontario, and about how this important value might be reconciled with the contemporary goals of government agencies employing the latest technologies for electronic service delivery.

The sketch presented above demonstrates an extraordinary progress for privacy protection policy over the last thirty years. From modest beginnings when it was often regarded as a "fringe" and elitist issue that rarely engaged the interest of the general public and the politicians they elected, it is now high on the political agendas of most industrialized (and some industrializing) states. It is a subject on which political candidates often develop positions. It is debated in many international organizations. It reaches the agendas of corporate boardrooms. The annual conference of the world's privacy and data commissioners is a focal event attended by representatives from over thirty countries. The relatively confined elite of mainly legal experts that pushed the privacy agenda in the 1970s has given way to a large and sprawling coalition of different interests. Privacy is an "issue whose time has come."

In this context, the debate about privacy solutions has been intense, and the cross-fertilization of ideas regular. Consequently we have seen a progressive harmonization of solutions. The divergences of the 1970s have given way to a continuing process of convergence to the extent that it now makes great sense to speak of a global approach to privacy protection, fostered through instruments such as the European Data Protection Directive. At the same time, the range of possible privacy policy instruments has expanded. There is now a range of

[67] Ibid.

different tools within the "toolbox" all of which are necessary, and none sufficient. It is necessary to gain a better understanding of the function that each tool can, and cannot, perform. Within this comparative and historical context, the following lessons can be drawn about how governments should approach the privacy issue in the years ahead.

LEARN from experience elsewhere. In the world of privacy protection, no government is an island. Decisions made anywhere in the world about system architecture, about standards, about international regulatory rules constrain, and will continue to constrain, how governments can and cannot process personal information to achieve programmatic goals. Moreover, the toolbox of privacy instruments is increasingly a global toolbox, containing instruments for privacy protection that any jurisdiction can apply should they so wish.

BEWARE the perception of "Big Brother." Some of the most controversial privacy scandals have arisen as a result of large-scale governmental plans to integrate personal data systems. Indeed, it was those very plans that initially forced the issue to the agendas in many Western societies.[68] Even though several generations of information technology have come and gone since these initial projects were first proposed, governments still need to be cautious about large-scale data integration plans. The specter of the "Big Brother" omniscient state is still a real fear among Western publics.

RESIST the temptation to identify citizens just for the sake of it. Governments need to reflect on the extent to which they actually need to identify its citizens. There is often an assumption that government has a core and unique function to identify citizens. That may be part of the political culture of several continental European countries, but it is less so in common law countries, where the verification of identity is an important function for specific purposes, but not generally. Debates over proposals to develop national identification cards in the UK and Australia, for example, were characterized by strong opposition from all sides of the political spectrum. One of the lessons from these highly politicized disputes is that establishing identity simply for the sake of establishing identity if *not* part of government's role. It is especially ironic that this role should be asserted at a time when the historic role of the state is being redefined and scaled back.

ANTICIPATE, rather than react to, privacy events. History suggests that organizations get caught out when they fail to appreciate, or they underestimate the degree of citizen concern over the collection and use of personal information. The recent uproar over the Longitudinal Labour Force File in Canada demonstrates the highly subjective and volatile quality of privacy concerns.

[68] For instance, the "Project Safari" in France; the "Federal Data Center" in the United States; the "Project Metropolitan" in Sweden. See David H. Flaherty, *Protecting Privacy in Surveillance Societies,* for a discussion of these cases.

Likely citizen reaction always needs to be anticipated when projects with potential privacy implications are being conceptualized and designed. The development of PIAs should play an increasingly important role in Ontario, and elsewhere.

BE TRANSPARENT. There is an obvious need for transparency, and widespread consultation. Historical examples suggest that organizations (public and private) get into trouble when they are less than honest about their personal data processing practices. Privacy scandals emerge when outsiders' suspicions are raised about the hypothetical ways in which systems developed for legitimate purposes can change into more intrusive surveillance devices. Government agencies should give closer attention to how they might use instruments such as the CSA privacy standard as a mechanism to force them to "say what they do, and do what they say."

ENHANCE TRUST. There is no necessary incompatibility between privacy protection and other policy goals, which require the collection of personal information. Any government service requires a degree of trust from clients. Good privacy protection can help enhance that trust. But quite often privacy is often seen as a barrier to the realization of programmatic goals. It is regarded as an obstruction which one can fix *post facto* through legislative rules that constrain the collection, use and disclosure of personal information by the agency in question. But there is always a bias to keep the options open, and to craft legal constraints in the most mutable language. And there are always pressures for "function creep" -- the processes whereby new applications are developed after the systems are put in place.

DESIGN PRIVACY IN. Finally, therefore, a shift in attitude is necessary about privacy within government. The number and complexity of privacy questions that are, and will continue, to tax the minds and resources of regulators will mean that post facto consideration of privacy questions will not only relegate privacy to a secondary status, it will also prove very inefficient. Conversely, if privacy becomes a design principle. If it is part and parcel of decision-making from the very early conceptualization of a project, then more profound questions might be asked about whether the same programmatic goals could be achieved without the collection and processing of identifiable personal information. The basic architecture of information systems can be designed to be privacy invasive or privacy friendly. The most significant challenge for the privacy movement today is less a legal and regulatory one, but more one that ensures that those who build information systems, and negotiate the standards upon which they are developed, are sufficiently conscious of the privacy implications of what they are doing. [69]

[69] See, Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

APPENDIX ONE

THE DIFFUSION OF INFORMATION PRIVACY LEGISLATION BY REGION[70]

	1970s	1980s	1990s
W. Europe	Sweden (1973) W. Germany (1978) Denmark (1978) Austria (1978) France (1978) Norway (1978) Luxembourg (1978)	Iceland (1981) UK (1984) Finland (1987) Ireland (1988) Netherlands (1988)	Portugal (1991) Spain (1992) Switzerland (1992) Belgium (1992) Italy (1996) Greece (1997)
E. Europe			Slovenia (1990) Hungary (1992) Czech (1992) Estonia (1996) Lithuania (1996) Poland (1997) Slovakia (1998) Latvia (2000)
N. America	United States (1974)	Canada (1982)	
S. America			Chile (1999)
Australasia		New Zealand (1982) Australia (1988)	
East Asia		Japan (1988)	South Korea (1994) Hong Kong (1995) Taiwan (1995)

[70] This table establishes the first date that information privacy legislation was enacted in each country either for the public sector, or for both private and public sectors. It does not incorporate legislative actions at the sub-national levels. It does not include FOI (access to information) laws. It does not include legislation that only regulates private sector enterprises. It does not include subsequent amendments.

APPENDIX TWO

STATUS OF PUBLIC SECTOR PRIVACY LEGISLATION IN CANADA

JURISDICTION	NAME OF ACT	DATE PROCLAIMED	INDEPENDENT OVERSIGHT
Federal	*Privacy Act*	1982	Privacy Commissioner of Canada
Alberta	*Freedom of Information and Protection of Privacy Act*	1995	Office of the Information and Privacy Commissioner
British Columbia	*Freedom of Information and Protection of Privacy Act*	1993	Office of the Information and Privacy Commissioner
Manitoba	*Freedom of Information and Protection of Privacy Act*	1997	Office of the Manitoba Ombudsman
New Brunswick	*Protection of Personal Information Act*	2000	Office of the Ombudsman
Newfoundland	*Freedom of Information and Privacy Act*	1982	Department of Justice
Nova Scotia	*Freedom of Information and Protection of Privacy Act*	1994	FOI and Protection of Privacy Review Officer
Ontario	*Freedom of Information and Protection of Privacy Act*	1988	Information and Privacy Commissioner/ Ontario
Prince Edward Island	*Freedom of Information and Protection of Privacy Act*	Pending proclamation	Information and Privacy Commissioner, PEI
Quebec	*An act respecting access to documents held by public bodies and the protection of personal information*	1982 (currently under review)	Commission d'acces a l'information du Quebec
Saskatchewan	*Freedom of Information and Protection of Privacy Act*	1992	Information, Privacy and Conflict of Interest Commissioner
N.W.T. and Nunavut	*Access to Information and Protection of Privacy Act*	1996	Information and Privacy Commissioner
Yukon Territory	*Access to Information and Protection of Privacy Act*	1996	Office of the Ombudsman

APPENDIX THREE

Status of General Privacy Protection Law and for the Private Sector in Canada

Federal	Bill C-6	In force Jan. 2001
Alberta	No known action	
B.C.	Parliamentary Report Published (2000)	
Manitoba	Discussion document published (1999)	
New Brunswick	Discussion document published (1998)	
Newfoundland	No known action	
Nova Scotia	No known action	
Ontario	Discussion document published (2000)	
P.E.I	No known action	
Quebec	Bill C-68 (An Act respecting The Protection of Personal Information in the Private Sector)	1993 (currently under review)
Saskatchewan	No known action	
NWT	No known action	
Yukon	No known action	

APPENDIX FOUR

Status of Canadian Health Information Privacy Protection Law

Federal	No known action	
Alberta	Health Information Act (Bill 40)	2001
B.C.	No action (1998 report to Ministry of Health concluded no action necessary at this time)	
Manitoba	Personal Health Information Act	1997
New Brunswick	No known action	
Newfoundland	Discussion paper (2001)	
Nova Scotia	No known action	
Ontario	Personal Health Information Bill (introduction, 2000)	
P.E.I.	No known action	
Quebec	Personal health information covered by general public and private sector legislation	1982 (public) 1993 (private)
Saskatchewan	Health Information Protection Act	1999
N.W.T	No known action	
Yukon	No known action	