The Personal Information Protection and Electronic Documents Act (the Act) and the Canadian Archival Community: A Guide and Commentary

May 1, 2001

By

David H. Flaherty, Ph.D.

David H. Flaherty Inc.
Privacy and Information Policy Consultants
1939 Mayfair Drive
Victoria, BC V8P 1R1
Tel: 250-595-8897
FAX: 250-595-8884

David@Flaherty.com

Table of Contents

Brief Summary

The full account that follows is somewhat complicated. The short version is that the **Personal Information Protection and Electronic Documents Act** (the Act) will have only modest application to most Canadian archives. However, its enactment does raise a number of issues about the relationship of privacy laws and archives, the most problematic of which are treated below in chapter 15 (including the threshold issues of jurisdiction and the risk of creating "privacy limbos" within archives).

The "authorized" interpretation of the Act set out by Industry Canada is that all archives are exempt from its requirements (especially if they are covered by federal, provincial, or territorial data protection legislation), and there are no constraints on the ability of archives to collect personal information.[1] If records from an organization covered by the Act are in an archive, the Act does not impose retroactive coverage over them, since it has no retroactive effect. If records from an organization covered by the Act are transferred to an archive, these records lose the privacy protections offered by the Act.

However, the core message of this guide and commentary is that all personal information held in archival settings should be handled in compliance with the fair information practices set out as a **national standard** in Schedule 1 of the Act. Archives, large and small, regulated and unregulated from a privacy perspective, need to figure out how to accomplish this goal in order to meet the legitimate expectations for privacy and confidentiality of those persons whose records are selected for archival retention.

Although official privacy protectors should remain vigilant about the practices of archives with respect to the collection and disclosure of records that include personal information, the known track record of major archives to date suggests that they have successfully incorporated fair information practices into their daily regime of archival work.

Readers should be aware that the author of this report wrote it under contract to the National Archives of Canada in response to its request for services. However, the end product is very much his own view of this particular world, which readers are welcome to disagree with from whatever perspective they bring to it. They should also be guided by the table of contents in terms of locating material that is of direct relevance to their interests.

[1] At this point in time, I am inclined to accept the interpretation of the Act offered by the specialists within the Department of Justice and Industry Canada, who have spent several years advancing and shaping the legislation and are certainly clear about their intentions as framers with respect to the coverage of archives. Within the body of this report, however, I have sometimes adopted a more skeptical approach to the scope of the Act, because, now that it has received royal assent, establishing the precise meaning and scope of its language is in the hands of the Privacy Commissioner of Canada and, ultimately, the Federal Court of Canada. I should add, further, that this is one person's view of the issues at stake in this arcane world.

1. Introduction: Archives and the Act

A series of introductory points attempt to set the stage for the analysis that follows in this guide and commentary, which focuses on the relationship between the Canadian archival community and privacy or data protection legislation.[2] They These preliminary observations, presented in a bullet format, are for the most part not controversial points:

- The House of Commons passed Bill C-6 in April 2000, after which it received royal assent as Statutes of Canada 2000, c. 5. Part 1, the privacy provisions, will go into effect on January 1, 2001. Parts 2 to four enter into force on May 1, 2000.

- Archivists, as individuals and as professionals, share with the public a demonstrated commitment to compliance with the fair information practices that are at the heart of privacy/data protection legislation in advanced industrial societies. Schedule 1 to the Act sets out such fair information practices in the form of a code or standard specifically developed for the private sector. As the Association of Canadian Archivists stated in its submission to the House of Commons on Bill C-54, "[a]rchivists are professionals governed by a formal Code of Ethics fully capable of self-policing on the disclosure and non-disclosure of personal information, as their past record has clearly shown."[3]

- The Code of Ethics for Archivists in Canada states in principle 3 (of 6) that "[a]rchivists encourage and promote the greatest possible use of the records in their care, giving due attention to personal privacy and confidentiality and the preservation of records." The application of these principles contains two additional statements that are also directly relevant to the concerns of this guide and commentary (and that are further discussed in the pages below):

    - A3…. Archivists discourage unreasonable restrictions on access or use, but may accept as a condition of acquisition clearly stated restrictions of limited duration and should suggest such restrictions to protect personal privacy. Archivists observe all agreements made at the time of transfer or acquisition.

    - C2. Archivists make every attempt possible to respect the privacy of the individuals who created or are the subject of records, especially those who had no voice in the disposition of the records….[4]

---

[2] None of what follows should be construed as offering legal advice to the archival community, since the author is not a lawyer. Although counsel acting on behalf of the author has reviewed this guide and commentary, an archive that believes that it requires legal advice on any matter raised by this presentation should obtain it through the usual channels. I am most grateful to Angela Westmacott of the firm of *Morley Ross Lovett & Westmacott* in Victoria for her invaluable assistance to me.

[3] See aca.archives.ca/official.com/c54/c54brief.htm. Although the issue of how to make sanctions effective is always a troublesome one, the reality is that this Code of Ethics only applies to members of the Association of Canadian Archivists, and membership in the ACA is not a prerequisite for employment as an archivist or in an archives. The reality of sanctions is that an archive is likely to discipline or fire an archivist who acted in breach of ethical standards.

[4] See http://aca.archives.ca/publicat/general/code.htm

- Archives that are clearly in the public sector are already subject to privacy legislation at national, provincial, and territorial levels for at least certain of their records. , since the introduction of the first federal data protection law was introduced in 1977.[5] It should be some comfort to the archival community (if not to historians and genealogists as users) that such legislation, long before the appearance of Bill C-54 (later Bill C-6) in 1998, has not posed insuperable burdens to the continued functioning of archives at the national, provincial, territorial, and municipal levels. The archival community has accepted the formalization of privacy rules required by such legislation, much as it will have to adapt to certain aspects of the Act when part 1 enters into force on January 1, 2001.

- An important qualification of the point in the previous bullet is that public sector privacy legislation tends to exclude from its scope "materials placed in the archives of a public body [e.g. Ministry, crown corporation, university, hospital, municipality] by or for a person or agency other than the public body."[6] The original intent of such provisions was to make life easier for archivists by removing the need to ensure full compliance with the rigours of such an Act for records that did not originate in the public sector. Now that data protection has finally developed for the private sector and quasi-public sector, one unintended consequence is in effect to create a "data haven" for private sector records that have been given, or will be given, to such an archive. At minimum, this will require self-regulation to ensure that fair information practices are in place for records.

- The other side of this coin is the Alberta *Freedom of Information and Protection of Privacy Act* which, uniquely in Canada, "does not affect access to records: (i) deposited in the Provincial Archives of Alberta; or (ii) deposited in the Archives of a public body that were unrestricted before the coming into force of this Act."[7] This is in effect a grandfather clause for personal information in all records for which access was **unrestricted** in the Alberta archives in 1995 (a province whose history spans the twentieth century).[8] However, and most importantly from a privacy perspective, the **restrictions** on access to records that existed on October 1, 1995 were kept in place. Thus access to such records, and those records acquired after the October date, now occurs in compliance with the Alberta *Freedom of Information and Protection of Privacy Act*.

---

[5] For a case study of the development and application of such federal laws, see David H. Flaherty, Protecting Privacy in Surveillance Societies (University of North Carolina Press, Chapel Hill, NC, 1989), part 4 and especially pp. 243-45.

[6] *B.C. Freedom of Information and Protection of Privacy Act*, RSBC 1996, chapter 165, s. 3(1)(g).

[7] Alberta *Freedom of Information and Protection of Privacy Act*, Statutes of Alberta, Statutes of Alberta, 1994, Chapter F-18.5 with amendments in force as of October 1, 1999, s. 3(b). This Act came into force on October 1, 1995.

[8] It makes practical sense that records in the Alberta Archives that were freely accessible on September 30, 1995 should not be closed to users the following day.

- The National Archives of Canada has recently made the following statement concerning the general issues addressed in this guide and commentary: "The impact of access to information and privacy legislation upon the access of Canadians to public records has been high. The archives' exemptions in the present acts have been an important help to ensure access under certain carefully governed situations. It is important to comment that there is a need to maintain a balance between allowing access on the one hand while still protecting privacy."[9]

- The general operations of archives already subject to existing data protection legislation (such as the National Archives of Canada, the Manitoba Archives, the British Columbia Archives, the City of Victoria Archives, or the Simon Fraser University Archives) are in principle not affected by the introduction of the Act. Similarly, all archives in the province of Quebec, perhaps without exception, are subject to the purview of the two data protection laws of that province that cover the public and private sectors.[10] However, it is possible that the Act will have an impact on certain records and, possibly, certain activities of such archives that involve the records of "organizations" subject to the Act, because these are not the records of public bodies as such.

- Privacy legislation continues to raise considerable anxieties among archivists, genealogists, and historians, since, at one level of understanding, these laws appear to threaten the continuance of their enterprises by restricting complete access to personal records, at least for a period of time. Full enforcement, for example, of the principles of data destruction and the right of an individual to be forgotten (le droit d'oubli) would substantially reduce the personal information available for archival and historical preservation, thus depriving the country of a central component of its historical memory.[11] As Danielle Lacasse, the president of the Association des archivistes du Quebec, stated to the Standing Committee on Industry, "archivists must constantly promote a fair balance between an individual's right to forget and the community's right to build its collective memory."[12] Seeking such a balance was also the theme of the submission by the Canadian Historical Association.

- Archival activities in Canada, even in public archives, are not adequately funded. Thus, a relevant reality is that most archives contain a large volume of records that have not been adequately catalogued and inventoried, meaning that their contents are unknown. This *is* a data protection problem of some consequence that will need to

---

[9] "Response to Dr. John English regarding his consultations on the future role of the National Archives of Canada and the National Library of Canada," quoted on the Web Site of the Canadian Council of Archives: **www.cdncouncilarchives.ca**.

[10] The ongoing debate in Quebec is whether its legislation can regulate the record keeping practices of federal entities, such as a bank, which is in part the rationale for The Act. The goal of the privacy advocate remains seamless coverage, which Quebec is already in a unique position to offer. See *Act respecting access to public documents and the protection of personal information* and the Act *respecting the protection of personal information in the private sector*. The Commission on Access to Information, which oversees these two laws, does not want The Act to apply to Quebec: Abridged Report 1998-1999 (Quebec, June, 1999), p. 17.

[11] See Flaherty, Protecting Privacy in Surveillance Societies, p. 8 for a listing of data protection principles and practices such as those mentioned in this sentence.

[12] House of Commons, Standing Committee on Industry, Hearings on Bill C-54, February 18, 1999.

continue to be addressed by archivists and official privacy protectors before access to personal information in such records can be granted (unless they are already quite old).

- Historians and archivists, who are appropriately twinned in defense of their important enterprises, made valiant efforts on February 18, 1999 to explain the importance of their professional work during the course of proceedings on Bill C-6 **(**formerly Bill C-54**)** in the House of Commons.[13] However, the reality of the exercise of political power in Canada today is that the proponents of the legislation, and their political masters at Industry Canada, regarded such submissions as of minor consequence in the overall scheme of trying to promote electronic commerce by ensuring the privacy rights of individuals. There were too many political problems in the offing for those public servants advancing the legislation to take scholarly and archival concerns too seriously, especially since they believed that Part 1 of the Act will, in fact, have only limited impact on archives in Canada. As noted further below Industry Canada officials regarded the existing framework of the law as appropriately handling archival concerns in particular. It is instructive, in this regard, to be reminded that, beyond some housekeeping and clarifying amendments, the House of Commons only made truly significant changes to the bills in response to law enforcement concerns (which is typical of the enactment of such data protection legislation in Canada during the past 25 years).[14]

- The goal of the archival community should now be to ensure that their own organizations implement the Act in a manner that is sensitive to the privacy interests of individuals and the broad goals of archives. This requires a process of ongoing education of official privacy protectors, privacy advocates,[15] archivists, and users of archives. Because this area of the law is in a state of flux, as are the personnel involved on both sides, this effort at mutual education about respective roles and obligations needs to be ongoing at federal, provincial, and territorial levels.[16]

- Official privacy protectors and privacy advocates are conditioned to react with alarm to the consolidation of significant amounts of identifiable personal information in one

---

[13] See, in particular, Association of Canadian Archivists, "Brief to Parliament on Bill C-54: Personal Information Protection and Electronic Documents Act (revised April 20, 1999), which is accessible from aca.archives.ca/official.com"; Canadian Historical Association, "Seeking a Balance: a response to Bill C-54," February 18, 1999 at http://www.yorku.ca/research/cha/html/english/c-54.html; see also Joanne Burgess, "The Right to Privacy in the Private Sector," at **www.yorku.ca/research/cha/html/english/burgess;**

[14] The Industry Committee of the House of Commons did amend Bill C-54 before presenting a revised version for 2nd reading in the House of Commons on April 13, 1999 to meet some concerns of archivists: it removed the requirement for archival institutions to be designed by order of the Governor-in-Council; it amended section 7(3)(h)(I) to reduce the period prohibiting disclosure from 110 to 100 years; and it agreed to regular five-year reviews of the legislation.

[15] Current leaders of the advocacy community include Pippa Lawson, Esq., of the Public Interest Advocacy Center in Ottawa; Valerie Steeves of the Department of Law, Carleton University; Professor Colin Bennett of the University of Victoria; Dr. Michael Yeo of the Canadian Medical Association; and Darrell Evans, the executive director of the B.C. Freedom of Information and Privacy Association.

[16] It is quite helpful in this regard that in places like Manitoba and the Yukon, the official Archives plays a central role in managing freedom of information and protection of privacy issues on behalf of the government.

location, such as at the National Archives of Canada.[17] In fact, and this is hardly surprising, privacy protectors are likely to have relatively modest knowledge of the archival process, because most Canadians know very little about archives. However, when various types of privacy protectors hear about the kinds of collections of personal information from administrative records that are held by any archive, they are likely to react with some alarm and surprise.[18] The archival community must deal with this fact on an ongoing basis. Official privacy protectors, in particular, must be encouraged, by a process of mutual education, to act in a pragmatic fashion with respect to the interests of archives and archivists, since they have the authority to cause significant problems.

- From the perspective of someone who is both a professional historian and a privacy advocate/official privacy protector/privacy consultant, the issues of privacy relating to the functioning of archives are quite manageable and in fact minimal, as I hope to demonstrate in the pages below.[19] In any league table of current privacy issues in Canada, the data protection problems posed by archives would be relegated to close to the bottom, compared, for example, to the health records of individuals. But archivists, in particular, in a manner very comparable to statisticians, need to be vigilant to protect their interests as professionals by promoting public understanding of their work, because they are both engaged in activities that are not intuitively regarded as privacy friendly, and since they involve the collection, use, and disclosure of so much personal data. Given the realities of overburdened professionals working in underfunded government archives for the most part, this duty is a serious challenge to the archival community.[20]

- In principle, if archivists comply with fair information practices on a statutory or self-regulatory basis, they can collect as much sensitive personal information as they can justify by archival standards and that public bodies and "organizations," as defined in the Act, will accept. In fact, an organization like the Ontario Archives has been collecting, and permitting the use of, sensitive personal information for most of the last century. These "government records" include psychiatric clinical case files, criminal investigation records of the provincial police, social service case files, and records of residential schools. In the hands of responsible custodians at the Archives, researchers have used these records for legitimate purposes without apparent

---

[17] A fine exception to this rule is Peter Bower, the executive director for access and privacy, Office of the Manitoba Ombudsman, since he is the former provincial archivist.

[18] The *Directory of Archival Repositories* on the web site of the Canadian Council of Archivists includes, for example, references to the following specific, or types of, archives: Canadian Lesbian and Gay Archives; Montreal Holocaust Memorial Center; Peterborough County, Ontario-City Health Unit; various hospitals; and many religious and ethnic organizations.

[19] Full disclosure and notice to readers includes the facts that I have worked on privacy issues since 1964, taught as an historian from 1965 to 1993, am a member of the Canadian Historical Association, served as the first Information and Privacy Commissioner for British Columbia from 1993 to 1999, and currently consult on privacy and information policy issues for a wide range of clients from the public and private sectors.

[20] The ongoing professional activities and aspirations of archivists can be followed in illuminating detail on the web site of the Canadian Council of Archives (CCA), founded in 1985: www.cdncouncilarchives.ca. The Bureau of Canadian Archivists comprises two separate associations based on language: the Association of Canadian Archivists, established in 1975, and the Association des archivistes du Quebec.

mishap.[21] At present, their collection and use is also subject to the oversight of the Ontario Information and Privacy Commissioner.[22]

- Archives subject to existing privacy legislation appear to be coping adequately with the burden it presents from a protection of privacy perspective, which is the focus of this guide and commentary. What is especially ironic is that some such archives appear to have somewhat more problems with "freedom of information" or "access to information" acts, which are intended to promote disclosure of government records. Government departments with records stored in a public archive can still try to deny access to them based on exemptions in such legislation, such as solicitor-client privilege and law enforcement.[23]

2. Some Facts about the Act

- The primary purpose of the Act is to extend fair information practices, over time, to the private sector in Canada, where it has been largely unregulated, except for innovative legislation in 1993 in the province of Quebec.[24]

- The Act largely responds to international pressures from the European Union to protect transborder flows of personal data, which have nothing to do with archives as such.

- The core problem posed by the Act, for purposes of this guide and commentary, concerns the collection, use, and disclosure by archives of records of personal information that originated with the private sector. Most people, including some privacy protectors and data subjects, are not adequately aware that some private sector records end up, by means of what is in fact a very sanitized and sanitizing process, in the hands of both small and large public and private archives. Disclosure of such archived records to researchers normally occurs several decades after the creation of the records. A typical exception would be persons seeking access to their own personnel records or military records held in an archive, such as the National Archives of Canada.

- The existence of different types of archives is completely irrelevant to the Act, which has as its primary concern protecting the privacy of individual residents of Canada in their current, contemporary relationships with the private sector and the quasi-private

---

[21] I owe this point to Ian Forsyth, the archivist of Simon Fraser University.

[22] Ann Cavoukian, the Ontario Commissioner, informed me that her Office has "had no problems with the Archives in terms of their handling of sensitive or confidential information." There have been no "complaints about the manner in which the Archives has handled this type of information." Her staff "could not recall any incident or allegation that personal information contained in archived records was misused or inappropriately disclosed by the Archives." (Personal communication, March 29, 2000)

[23] I am grateful for guidance on this issue to Mac Culham of the B.C. Archives.

[24] Quebec, *Act respecting the protection of personal information in the private sector*

sector.[25] The legislative concern is focussed on electronic commerce involving banks, telecommunication companies, and a multitude of service providers, not on archives. There is a risk, however, that archives could become accidental, or at least unintended, targets of such legislation.

- The Act incorporates the fundamental premise that individuals (as customers, clients, and employees) have reasonable expectations of confidentiality and security for their personal information, whether in the custody and control of a particular company or transferred to an archive. They wish to exercise informational self-determination. There is no question, in my view, that such individual expectations of confidentiality diminish over time, although they never entirely disappear.[26] Thus it would require considerable efforts to identify real privacy problems for nineteenth century records held in any Canadian archive, whereas personal information in records for the last twenty years that are already in archives are much more likely to be sensitive in some circumstances. That is why major archives and even privacy laws, such as in Manitoba, recognize that all records are completely open after one hundred years. However, I favour an access to information regime for archives that seeks to ensure fair information practices are followed for controlling access to all personal records, especially the most sensitive ones (juvenile delinquency, adoption, social work case files, psychiatric and mental health records, for example).

- Archivists and historians made their concerns and anxieties known during the process of legislative hearings on Bill C-6 (see below). Official data protectors and advocacy groups for privacy would be unwise to ignore that testimony, although it had limited impact on the contents of the Bill.

- The **consent** requirements in the Act may pose some practical problems for various kinds of archives, which need to be addressed. The issue is whether individuals who give their personal information to an organization now covered by the Act have any idea that their data may be transferred to an archive at some future time. The realities of archival purging, retention, and disposal practices are such that most personal information will not be archived in any event. However, employees, for example, are in a different situation from customers in most cases. In my idealistic opinion, each category of personal records held by an organization subject to the Act needs some kind of **notice** of the possibility of archival storage in lieu of the need for explicit consent. One problem with this idea is that the prospect of archival storage is remote for most individuals in contact with such organizations, because most personal records will be destroyed on the basis of retention schedules, on the grounds that they

[25] In practice, the old private sector/public sector distinctions have broken down, and there are considerable flows of personal data in all directions. Again, the privacy advocate and the citizen want seamless data protection with the force of law and an oversight mechanism, such as the Act will provide.

[26] As Information and Privacy Commissioner for British Columbia, I made several decisions that recognized the privacy rights of the deceased. See Order No. 27-1994, October 24, 1994 at www.oipcbc.org. All of us would be astonished, of course, to think that our passing might lead to the casual perusal of our medical or health records by simply curious persons and even by our heirs.

have no archival value.[27] Historians and archivists who testified on Bill C-6 before the House of Commons took the interesting position that archival retention is in fact consistent with the original purposes of data collection as a legitimate form of **secondary use**. As aptly stated by Joanne Burgess, president of the Institut d'histoire de l'Amerique francaise, "[t]he principle we want to have recognized is that secondary use for historical or other purposes, whether it's 10, 15, 20, 30, 40, 100, or 150 years later, is not the same thing as secondary use for other administrative or commercial purposes."[28] That plausible position is not one that the Act explicitly recognizes.

- Whether or not most archives in Canada can in fact be construed as falling under the ambit of the Act with respect at least to any of their activities that can be construed as commercial, **the reality is that this law is establishing the *de facto* national privacy standard, which any archive can only ignore at its peril for any personal information in its custody and control. All archives have to follow fair information practices, whether required by law or self-regulation.** The caveat, of course, is that most archives in Canada are not in fact "organizations" engaged in any significant way in commercial activities and thus, technically, are not covered by the Act for the most part. This topic is considered below in detail.

3. The Core Privacy Values in Schedule 1 of the Act

Part 1 of the Act, which addresses the protection of personal information in the private sector, is the heart of the legislation for purposes of this guide and commentary. Part 1 must be examined in the context of Schedule 1, which lays out a set of principles that organizations must generally follow in order to protect personal privacy.[29] These principles reflect the core privacy values, or **fair information practices**, that have been at the heart of national, state, provincial, and territorial legislation in advanced industrial societies since the early 1970s.[30] They are also in a direct line of intellectual inheritance from a similar set of principles developed by the Organization for Economic

---

[27] A financial institution, for example, will only retain, even for a long-term relationship with an individual customer, very basic information (e.g. account opening data) and not the details of regular transactions. The costs of storing paper and digital records and then trying to access them after the fact are thus promoting privacy protection for the individual.

[28] Standing Committee on Industry, Hearings on Bill C-54, February 18, 1999.

[29] Section 5 of the Act establishes the levels of obligation with respect to each principle (see below).

[30] Fair information practices represent the reasonable expectations of customers and employees of any organization as to how their personal information will be treated. The concept of fair information practices developed simultaneously in both the United Kingdom and the United States in the early 1970s. All of the privacy (meaning data protection) laws in the world (more than thirty countries have them) incorporate these practices. See Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, Ithaca, NY, 1992).

Cooperation and Development (OECD) around 1980.[31]

During the first half of the 1990s representatives of the public and private sectors in Canada met under the auspices of the Canadian Standards Association (CSA) to develop a model code for the protection of personal information in the private sector. The intention was to develop a self-regulatory code that would reduce the need for statutory solutions for data protection in this sector. Most privacy advocates wanted Canadians to have privacy rights, with an oversight mechanism in the form of a Privacy Commissioner, which would be enforceable by law as required. Simultaneously, the *European Directive on Data Protection* was mandating similar standards for non-European countries that wished to continue to trade in personal information with the European Union. In 1993, Quebec enacted private sector legislation of its own.

In the Act, Industry Canada adopted the highly innovative CSA Code and gave it the force of law. Schedule 1 (which incorporates the CSA Code into the Act) lays out ten principles, each one followed by a more complicated articulation of best practices. These have already served as the basis for self-regulatory codes by, among others, the Canadian Bankers Association and the telephone industry (the former Stentor). IMS Health Canada Ltd. went one step further and had its privacy code, based on the CSA **standard**, certified as such by the Quality Management Institute of the Canadian Standards Association.[32] I have summarized each of the ten principles below, with a brief commentary on what they mean, since the archival community should comply with them in the course of being sensitive to the protection of privacy in permitting access to personal records in their custody and control.

Although the principles establish a level of privacy protection that archives **should** aspire to achieve, Part 1 of the Act modifies the contents of these principles to some extent. Such modifications, especially with respect to the collection, use, and disclosure of personal information without the consent of the individual, will be discussed further below. However, in order to try to understand a very complex piece of legislation, one first has to understand the principles in Schedule 1.[33]

Principle 1 - Accountability: "An organization is responsible for the personal information under its control and **shall** designate an individual or individuals who are accountable for the organization's compliance with the following principles."

From an archival perspective, the requirements for compliance with this principle are laid out in a straightforward manner in 4.1.4:

- Implement procedures to protect personal information;
- Establish procedures to receive and respond to complaints and inquiries;
- Train staff and communicate to staff information about the organization's policies and practices;

---

[31] See Department of Justice, Canada, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Implications for Canada (Ottawa, 1985).

[32] See IMS Health, Our Commitment to the Protection of Personal Information (IMS Health, Canada, November, 1999, Pointe Claire, Quebec). Its code/management system applies to IMS's management of personal information respecting health professionals. QMI issues a certificate of registration to the standard with an expiry date.

[33] One explanation from Industry Canada for the peculiar structure of the Act is that the "management standard" had to be in an appendix to the law to avoid trade problems for Canada, with its major trading partners, before international trade tribunals.

- Develop information to explain the organization's policies and procedures.

The **accountability** principle requires both staff and clients of any archives to know what the rules are for collecting, using, and disclosing personal information. In my judgment, the head of any archive should be the "designated individual" for purposes of compliance with the rules, but with day-to-day responsibility delegated to other individuals (always including a Human Resources person who deals with staff information, which raises a different kind of privacy issue).

Principle 2 - Identifying Purposes: "The purposes for which personal information is collected **shall** be identified by the organization at or before the time the information is collected."

This should be a relatively uncomplicated issue for archives. The raison d'être of archives is to collect and use records, including personal information, for historical, genealogical, and other research purposes. Archives, even those located within a specific organization, such as a bank, are established for relatively precise purposes. They follow established principles to determine what records are worth preserving for archival purposes, which normally results in the elimination of routine, repetitive, and trivial information.[34] This requirement to identify purposes is much more complicated for private sector commercial concerns, which are constantly inventing new ways to use personal information for marketing purposes, such as the data warehouses developed during the 1990s. Explaining to donors what will be done with their gifts or transfers of records containing personal information to an established archive is a comparatively simple matter, not least because donors of sensitive records can easily continue to exercise some control over how their records are used through donation agreements.[35] At the same time, it is highly unlikely that corporate concerns with be transferring personal information on customers to an external archive, since such records are not kept very long in practice.

Principle 3: Consent: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."

For most data custodians, obtaining appropriate **consent** from individuals to collect and use their personal information is the most complex data protection issue, even though the CSA Code, and hence the Act, does not require **explicit** informed consent as such.

An archive that collects personal information from such diverse groups of individuals as employees, customers and clients, individual donors, and potential donors should obtain consent from these persons for specific uses of their information whenever possible. This is especially the case when archives collect personal information directly from individuals. Archives currently subject to data protection legislation (which would cover the major archives in the country) may have already

---

[34] I realize that this process is hardly unproblematic, given the range of records in existence today in various formats, and the difficulties of predicting what scholars of the future will find relevant. However, I leave ongoing discussions of such issues to the archival community and their funding masters.

[35] The Archives at Simon Fraser University acquired the records of the John Howard Society for the lower mainland of British Columbia, including case files of prisoners that the Society had worked with. The Society did not wish to be involved in access decisions. The Archives is subject to the B.C. data protection legislation, but these particular records would not be covered. Ian Forsyth, the archivist, agreed to administer the John Howard Society papers in compliance with the principles and spirit of the B.C. *Freedom of Information and Protection of Privacy Act*. I regard such a decision as exemplary from the perspective of ensuring fair information practices. The B.C. Archives takes a similar position with respect to sensitive records of hospitals, children's aid societies, and other organizations, whose records are technically not covered by the B.C. Act.

addressed these matters. An "unregulated" archive, such as that of a religious group (the United Church Archives in Toronto) or a specialized historical archive of a religious or ethnic group, should obtain as explicit consent as possible for future uses of personal data collected by them, even though the Act does not really require it.[36]

The much more serious issue for archives, in general, including those subject to existing privacy legislation, is whether they can assume that data subjects have consented to placing their personal information in an archive for consultation by scholars and other interested persons. For some archivists, this raises a significant fear that the strict enforcement of the consent principle would put them out of business in terms of collecting, storing, and allowing access to personal information already in their possession or custody.[37] A purist application of principle 3 would even have *ex-post facto* application to personal information held in archives from "organizations" subject to the Act (which has retroactive effect for an organization, but not for an archive that already holds records from such an organization), such as the Bank of Montreal or the Hudson's Bay Company.[38] In fact and in law, the responsibility of an organization is over when records are given to an archive, thus creating a "privacy limbo" to use the felicitous language of Heather Black, one of the framers of the Act from the Department of Justice. Some common sense is obviously required with respect to personal data that are already held by any kind of archive and that are already available to qualified users under controlled conditions. In an ideal world, a grandfather clause would be read into the Act for reputable archives (and no others are likely to continue in existence) with respect to personal data that are already held by the archive and made available to legitimate users.[39] However, it is highly unlikely that a court would read in such a qualification, let alone an entire grandfather clause. Fortunately, if archives do fall within the scope of Division 1 of Part 1, they could be covered by the language contained in section 7(2)(c), which indicates that knowledge or consent for use may not be possible or even necessary, where the use is for scholarly study or research purposes. (See below)

Archivists and historians raised the issue of "informed consent" in their appearance before the House

---

[36] In the course of the next four years, the largest provinces are likely to produce their own versions of the Act for areas subject to provincial jurisdiction, which will mostly likely extend The Act's standards officially to the entire private sector in Ontario, British Columbia, and Alberta, for example, so any archive should self-regulate to the standards of Schedule 1. I am using the term *unregulated archive* to mean one that is not subject to existing data protection legislation and that the Act will not cover. A regulated archive, however, can still hold *unregulated records* if, as is typically the case, such legislation does not cover records stored in an archive by a person or agency other than a public body.

[37] In its submission on Bill C-54, the Association of Canadian Archivists pointed out that the requirement for knowledge and consent of the individual involved "is unduly cumbersome. It will drain already scarce archival resources away from critical archival preservation tasks to the administration of this act, and it will seriously delay, inconvenience, and discourage researchers." Furthermore, the requirement to inform the Privacy Commissioner of Canada "where it is impracticable to obtain consent," will impose "a major burden on archives" and "will be a cause for long delays for researchers." See **aca.archives.ca/official.com/c54/c54brief.htm** at p. 4. This perspective is, in fact, a misreading of what the Act actually requires.

[38] After their appearance before the House of Commons on Bill C-54, a trio of archivist and historians' groups complained about the broad scope of the legislation: "It will impose retroactive controls on a host of manual or paper-based records containing personal information. In effect, within the private sector as defined in Clause 4, Bill C-54 will regulate all surviving personal information created during the 20th century!" (Letter to Ms. Susan Whelan, Chair, Standing Committee on Industry, April 20, 1999, at **www.archives**.ca/aca/official.com/c-54/index.htm

[39] Again, it is problematic that the House of Commons and Industry Canada did not accept the proposal of the Association of Canadian Archivists "that there shall be no retroactive application of the legislation to any private-sector records already under the custody and control of an archival institution. It is unacceptable that records that have been 'open' for decades in some cases, and used by many researchers, should now be closed to other researchers." See **aca.archives.ca/official.com/c54/c54brief.htm** at p. 4.

of Commons, emphasizing the exceptions to the general rule in existing legislation, such as in Quebec and in the federal **Privacy Act**, which recognize consistent uses of information, "without the consent of the individual, where this is consistent or compatible with the original purpose [of data collection]." The groups "emphasized that even when informed consent is not required for the use or disclosure of personal information, stringent protocols exist to ensure that the privacy rights of individuals are safeguarded." Strict enforcement of informed consent requirements would "make it extremely difficult for companies to maintain and develop an active institutional memory."[40] The scholars and archivists further warned:

The most significant and detrimental consequences of any such measure would be to Canada's archival heritage and history. It would of course be possible to ask for explicit consent for future processing of data for historical or archival purposes. But given that historical inquiry is constantly changing in terms of subject, focus, and method, it would be virtually impossible to provide the kind of detailed information required for truly informed consent with respect to potential future scholarly, archival or historical research, and to the range of potential safeguards for privacy. Core archival practices, for example, currently run to several pages. In the absence of such nuance and complex consent forms, it is likely that such measures would result in a high refusal rate and the corresponding destruction of large numbers of records. Any widespread destruction would undermine the scientific validity of many future research endeavours and have perhaps unintended, but unfortunate consequences. It would impoverish our archival heritage. It would undermine our ability to know and understand our past. It would remove the rights of citizens to seek redress for injustices.[41]

The archivists and historians offered three recent examples in support of this last assertion: (i) the Japanese-Canadian wartime removal compensation package; (ii) all Aboriginal and treaty claims, including those relating to residential schools; and (iii) the relocation of Inuit communities in the North during the 1950s. The argument of the submission on this point is so compelling that I quote it in full:

Imagine these three scenarios again. If a Japanese-Canadian being relocated in World War Two from the West coast, or an Aboriginal parent losing a child to a residential school, or an Inuit survivor from the High Arctic relocations, if these three had been asked, on forms then being filled out that were designed to accomplish these unpleasant transactions, to consent to these forms containing their personal information eventually being transferred to an archives for later historical use, the vast majority would have checked "No" in a little box on the form. They would have done so because they are uninformed about the nature of archival activity or historical research, and the nuances of long retention periods before release, archival appraisal and sampling methodologies, descriptive practices to shield names, severing of personal identifiers from documents before release, codes of research ethics, etc. They would check "No" simply because they don't want people or perhaps Big Brother government snooping in their lives. Such fears are legitimate, but they are uninformed about the nature of and regulations governing archival work and historical research. Yet by checking "No" --unless archival retention, as recommended above, is seen as being consistent with the original purpose, thus not requiring consent-- these people would have destroyed the very records upon which later redress settlements for themselves and their children have been based. Moreover, the point of history is that no one at the time could have predicted such future uses for these records. In all three cases, and many more like them, the destruction of these records would have been a national tragedy, and an international scandal.

---

[40] Letter to Ms. Sue Whelan, Chair, Standing Committee on Industry, April 20, 1999, **aca.archives.ca/c-54/index.htm** at pp. 4-5.

[41] Ibid., p. 5.

This submission fully reflects what this guide and commentary has termed the realities of life for archivists and historians. No country in the world, to the best of my knowledge, requires informed consent, as such, for archival storage of information. These archivists and scholars make a plausible argument that "archival retention and, after a reasonable passage of time, historical research is consistent with the original uses for which personal information was gathered."[42]

The note to principle 3 provides only limited guidance for archives with respect to obtaining consent, although it acknowledges, in a very important way for archives, that "organizations that do not have a direct relationship with the individual may not always be able to seek consent."[43] This particular principle is in fact modified, considerably, by section 7 of the Act. These are such important modifications for the continued functioning of archives that they must be addressed here (as well as below).

Section 7 sets out criteria that must be met if an organization is going to **collect, use, or disclose** personal information without the knowledge or consent of the individual concerned. The most relevant one for Archives is that **"the collection is solely for journalistic, artistic or literary purposes."** Although it would have been preferable if the drafters had added the words "scientific" and "scholarly" to this list, the language is broad enough to cover the traditional activities of archives and their patrons in terms of collecting personal information for archival purposes, especially with the reference to literary purposes.[44] A secondary defence for an archive might be that it is not in fact "collecting" personal information when it accepts a set of records, in whatever format, for inclusion in an archive. It is also regrettable that the legitimacy of collecting personal information for journalistic, artistic, or literary purposes was not repeated, exactly, concerning the use and disclosure of the same information. For some reason, as noted in a subsequent paragraph, the drafters changed the language from section 4(2)(c).[45]

The Concise Oxford Dictionary (7th edition, 1982) defines "literary" as "of, constituting, occupied with, literature or books and written composition esp. of the kind valued for quality of form." The relevance of such a definition is the fact that courts will look to dictionary definitions in interpreting the plain meaning of the language used by legislative drafters.[46] The federal *Privacy Act*, however, explicitly sets out specific conditions in which the use or disclosure of personal information for statistical or scholarly purposes is permitted. [Section 8.2.j actually says research or statistical purposes]

---

[42] Ibid., pp. 5, 6.

[43] Although I am aware that section 2(2) removes the two notes in Schedule 1 from the Act, I encourage those seeking to comply with the national statutory standard that it creates to look to the notes for guidance on best practices.

[44] The framers and drafters of Bill C-6 worked in complete secrecy and were largely unable to share drafts with anyone outside of government, including the various Privacy Commissioners across the country. One result is that certain desirable minor changes were not made in advance, and Industry Canada was very reluctant to make any changes during the legislative process for fear of opening the floodgates. The Canadian Historical Association recommended adding the words "scholarly and statistical purposes" to Bill C-6. See Canadian Historical Association, "Seeking a Balance," **http://www.yorku.ca/research/cha/html/english/c-54.html** at p. 2.

[45] There is apparently no technical reason why the language of section 4(2)(c) had to be repeated.

[46] While the statutory language of "literary purposes" would tend to cover the traditional activities of archives, there may be situations, such as empirical studies by epidemiologist and social scientists, for example, which may not fall squarely within these terms. It is indeed unfortunate that the drafters did not include the words "scientific" and "scholarly" to this list of appropriate collection, uses, or disclosures.

It is also helpful to note that the *European Directive on Data Protection*, which sets minimum standards for national data protection within the European Union and which inspired and pushed Canada to enact the Act, makes the following supportive statements about the kinds of uses of personal records addressed in this guide and commentary:

([Recital] 20) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected[,] provided that Member States [of the European Union] furnish suitable safeguards; ….

Article 6 1. Member States shall provide that personal data must be: …
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for **historical, statistical or scientific purposes** shall not be considered as incompatible provided that Member States provide appropriate safeguards; [emphasis added]

Article 9 Processing of personal data and freedom of expression
Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression[,] only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. [This language likely explains the indirect inspiration for the language used by the drafters of Bill C-6 in section 7.]

Sections 7(2) and 7(3) introduce similar modifications to the requirement of principle 3 for consent for the use or disclosure of personal information from an archive, without the knowledge or consent of the individual, only if it is *used* "**for statistical, or study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable[47] to obtain consent[,] and the organization informs the [Privacy] Commissioner [of Canada] of the use before the information is used."** There are at least two problems with this set of five statutory controls on uses of personal information held by an archive subject to the Act or that acts as if it is. The first is somehow ensuring that identifiable personal information is used in a way that ensures its confidentiality (which does not appear in 7[3]). While a researcher using the records of employment in the shops of a particular company sixty years ago will likely have no interest in using the names of employees other than for record linkages, for example, a writer using personal information for the purposes of a biography for inclusion in the Dictionary of Canadian Biography is in quite a different situation with respect to the publication of names (and it can hardly be assumed that the Parliamentary framers of the Act intended to make it impossible for archival sources to be used by their future biographers). The issue of biography is especially sensitive with respect to living individuals, such as Pierre Eliot Trudeau or Brian Mulroney, about whom considerable amounts of personal information will be held by archives (although they are also "public figures" or celebrities, with fewer reasonable expectations of confidentiality, in a way that most Canadians are not). It is thus necessary to read the qualification in the phrase in section 7 about 'using information in such a way as to ensure its confidentiality,' in a manner that will not prevent the identification of biographical topics in particular. This is a good example of where the drafters of the Act paid no attention to important forms of legitimate scholarship, because they had so many "larger"

[47] The French version refers to "practically impossible," or "impossible in practice," which are more meaningful terms than "impracticable."

issues to cope with in the exercise of their mandate.[48]

The second problem is that archives acting in accordance with the Act should inform the Privacy Commissioner in advance of granting access to identifiable personal information held in their collections. This could happen by one major notice of ongoing activities. Again, there is a significant risk of scholars and genealogists, in particular, feeling that this is a kind of censorship clause that appears to require validation by the Privacy Commissioner (meaning his staff) before a research project involving the use of identifiable personal information can go forward.[49] One can document the Privacy Commissioner's raising relatively purist positions on comparable matters in his relations with the health and statistical communities in particular (which is admittedly part of the privacy watchdog role).[50] In an ideal world, various types of archives subject to the Act, or acting in compliance with its principles, will have a consultation process with the Privacy Commissioner's office (and its provincial and territorial equivalents) in order to establish, well in advance, the legitimacy of how they collect, use, and disclose identifiable personal information for "journalistic, artistic or literary purposes." This should even be true for the National Archives of Canada, which is explicitly exempt from Part 1 of the Act. (See section 4(2)(a))

Section 7(3) of the Act addresses issues of *disclosure* of identifiable personal information without the knowledge or consent of the data subject. This may only occur if the disclosure is "for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent[,] and the organization informs the Commissioner of the disclosure before the information is disclosed." Note that these criteria must be met in their entirety. Section 7(3) at least omits the qualification, "the information is used in a manner that will ensure its confidentiality," which is highly problematic concerning section 7(2), as discussed above. The potential remedy of discussing standard disclosures with the Privacy Commissioner, as part of an initial consultation process, as discussed in the previous paragraph, has similar application here.

The treatment of **consent** in principle 3 in Schedule 1 contains many additional qualifications about the process of obtaining consent for collection, use, or disclosure of personal information that are not directly relevant to the traditional work of archives in promoting uses of archival materials, although they are appropriate to the much simpler process of collecting, using, and disclosing personal information from staff and clients. In terms of 4.3.4 and 4.3.6, it seems unlikely to me that most archives will be collecting **sensitive** personal information in the normal course of interactions with

---

[48] Although I am thinking about traditional forms of scholarship as I write, I readily agree with the suggestions of the Association des archivistes du Quebec that the term "scholarly" should not "limit the use of personal information to academics only. This would exclude popular study and research, such as genealogical publications, popular history books or historical studies done by amateur historians." (Standing Committee on Industry, Hearings on Bill C-54, April 18, 1999) In fact, the French version of section 7(3)(f) refers to disclosure of personal information "for statistical purposes or for the purposes of study or of learned research," which language is more supportive of popular uses of personal information than the English translation. Both the French and English versions of the Act have equal weight.

[49] The Canadian Historical Association informed the Standing Committee on Industry that sections 7(2)(c) and 7(3)(f) were potentially cumbersome and time consuming, raising the risk that access to information "will get bogged down in the bureaucracy and seriously restrict what scholars are effectively able to research." It recommended a clause like section 8(3) of the Privacy Act that gives the National Archives of Canada the discretion to release records containing personal information that are non-sensitive and will not cause injury. It added: "During the National Archives of Canada's administration of this permissive 'archives clause,' there has not been a complaint regarding the release of personal information or a privacy violation in over fifteen years." See Canadian Historical Association, "Seeking a Balance," **http://www.yorku.ca/research/cha/html/english/c-54.html** at pp. 2-3.

[50] See Privacy Commissioner of Canada, Annual Report 1998-1999 (Ottawa, 1999), pp. 13-16, 27-30 at www.privcom.gc.ca

their employees and patrons, who will likely be filling out standard forms that can easily include consent notices. If archives exchange mailing lists with one another, they will have to be quite careful about getting consent from such persons in advance of doing so (see 4.3.7[b]).

Principle 4 - Limiting Collection: "The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means."

A strict application of such a fair information practice as "limiting collection" to existing archives could have a disastrous impact on their traditional activities (which the drafters cannot have intended). While it would be appealing to interpret principle 4 narrowly as applying to the present-day collection of personal information from staff and patrons, not the traditional collection activities of any archive, it is unlikely that the language of principle 4 supports this narrow interpretation. Thus it would be safer for archives to set out their broad purposes in their mission statements or statements of goals to the effect that they do not collect personal information **indiscriminately,** that the amount and type of information collected is **limited** to that which is **necessary** to fulfil archival purposes (4.4.1), and that this process occurs by **fair and lawful means**. Archives may find it burdensome to have to address such matters, but it appears to be necessary to avoid undesired contact with the "privacy police." Sensitivity to privacy always requires good housekeeping practices with respect to the handling of personal information.

Principle 5: Limiting Use, Disclosure, and Retention: "Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes."

As previously noted, the CSA Code was not drafted with the needs of archives or scholarship in mind; it was intended to apply to the current needs of companies doing business with customers. It is only in that sense that principle 5 has relevance to the work of archives in dealing with its current patrons and clients. The archivists and historians who testified on Bill C-6 before the House of Commons wanted an amendment to principle 5 itself, stating that the "use and disclosure of personal information for historical, statistical, scholarly or archival purposes shall not be deemed to be incompatible with the purposes for which it was collected."[51] In fact, it was impossible to make changes to the CSA Code during the legislative process and, again, archivists, scholars, and statisticians were not present during the development of the code itself.[52]

Archivists will have particular reason to fear the second sentence of principle 5, since it incorporates the principle of anonymization, or even destruction, of identifiable data over time, including guidelines on retention that include "minimum and maximum retention periods." (4.5.2) In particular:

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to

---

[51] Letter to Ms. Susan Whelan, Chair, Standing Committee on Industry, House of Commons, April 20, 1999, **aca.archives.ca/c54/index.htm** at p. 5.

[52] The Canadian Standards Association's Technical Committee on Privacy, which negotiated and drafted the code in the early 1990s, was made up of corporate, industry, and consumer representatives, public servants, and some privacy officials. See Canadian Standards Association, Model Code for the Protection of Personal Information (Canadian Standards Association, Etobicoke, Ontario, March 1996), pp. iv-vi. The one academic on the committee represented the Consumers Association of Canada.

govern the destruction of personal information. (4.5.3)

However, sections 4.5.2 and 4.5.3 of the Schedule both use the word "should" indicating that the principle is directory rather than mandatory.

Successive Privacy Commissioners of Canada have made positive noises about such practices as the destruction or anonymization of personal records, again without adequate regard to the interests of the archival community in the long-term retention in identifiable form, for legitimate secondary purposes, of at least some personal information. The judgment of what is transitory information, as opposed to information of archival quality, should be the domain of archivists and record managers in consultation with the official privacy protectors.[53] This process normally occurs through the implementation of record retention schedules and donation agreements in cooperation among record managers, archives staff, and government institutions.[54]

The National Archives and the Association des archivistes du Quebec wanted an amendment to schedule 4.5.3 to the effect that "[o]rganizations shall develop guidelines and implement procedures to govern the destruction of personal information *not of historical or archival value.* The response from Industry Canada is that the first part of the sentences says that information does not have to be destroyed, so such an amendment was unnecessary. As noted elsewhere, it was in fact impossible (or at the very least difficult) to amend the CSA Code during the legislative process on Bill C-6, since it had evolved as a national standard (although in fact Parliament could have done so and could do so in future); it is now unlikely that the Canadian Standards Association will exercise custody rights on behalf of its offspring, since it has seemingly lost interest in the Code. It would be appealing to argue that, in practice, the proposed amendment to Bill C-6 will have to be "read into it" during its implementation phase, since no one intends to stop the functioning of archives in this country. Again, the problem is that a court would be unlikely to read in such language. Faced with this question of interpretation, there is a reasonable prospect that a court would simply conclude that time limits cannot be imposed on archives for destruction of personal information, because of the nature of the functions that they perform. In fact, a court will likely never have a chance to interpret the destruction clause in Schedule 4.5.3, since it is not on the specified list of what the Federal Court can review in section 14 of the Act. In addition, the clear purpose of archives is to preserve records that they choose to archive, not destroy them.

After their appearance before the Standing Committee on Industry of the House of Commons, the Canadian Historical Association, the Institute d'histoire de l'Amerique francaise, and the Association of Canadian Archivists commented as follows about the risk of more frequent destruction of records:

---

[53] I continue to refer in this guide and commentary to the relationship between archivists and the official privacy community, but the Act has also spawned a national advocacy community (including this writer), which tends to promote very strict application of fair information practices, especially in the health field. The introduction of list. serves on the Internet has made possible the maintenance of such coalitions in the face of the spatial and time zone differences facing Canadians on a daily basis. Representative leaders of this coalition are Pippa Lawson of the Public Interest Advocacy Centre in Ottawa, Darrell Evans, the director of the BC Freedom of Information and Privacy Association, and John Westwood and Murray Mollard of the BC Civil Liberties Association. See John Westwood, "Life in the privacy trenches: Experiences of the BC Civil Liberties Association," in
Colin J. Bennett and Rebecca Grant, eds., Visions of Privacy: Policy Choices for the Digital Age (University of Toronto Press, 1999), 231-43.

[54] Thus the access to information directory of the Manitoba government not only lists the categories of records available from government departments, but also the retention or destruction schedules and the dates when at least some information is transferred to the Manitoba Archives. My casual perusal of this directory reminded me of how much personal information is destroyed on a regular basis, because it is not of archival value, or the cost of long-term storage is prohibitive in terms of competing archival priorities.

We would insist that there is a legitimate public interest in the preservation of historical records and the study of the past. We strongly oppose any measures that would result in collective amnesia. Personal information should be protected by the reasonable passage of time, until it can no longer be used against the person, not by destruction, which is final and removes other protections and rights to which citizens are entitled.[55]
The power of this statement speaks for itself.

Principle 6 – Accuracy: "Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."

Again, this is a principle that only applies to archives to the extent that they collect information from employees and clients/patrons on a one-time or an ongoing basis. Secondly, archives have no interest in collecting, using, and disclosing inaccurate information for archival purposes, but they are dependent on the quality of such data that the original collectors entrusted to them.

Principle 7 – Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."

This is at least one fair information practice set out in Schedule 1 in which the interests of archivists and official data protectors fully coalesce, that is with respect to the importance of ensuring **security** for personal information held in various types of records. One would expect an archives to use the full range of methods of protection outlined in 4.7.3, including physical measures (locking filing cabinets), organizational methods (training staff), and technological measures (the use of passwords and audit trails). Even the concept of **sensitive** information in the Schedule has considerable relevance here, since any archive should be more careful about the security of health information or personal diaries, for example, than a list of members of an ordinary group or a list of customers of a company. The National Archives segregates some records physically from the main holdings; these records are often stored in special vaults, have restricted finding aids, and are put into archival containers that are marked in some way or other for special treatment. The practical difficulties of defining "sensitive" information should encourage archives to follow strong security practices for all of the personal information in their custody and control.

Principle 8 – Openness: "An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."

Again, compliance with this principle should be a simple matter for a well-established archive in Canada. The National Archives, for example, already publishes a substantial booklet (discussed below) on how it controls access to personal information held in its archival collections, but it pertains only to public and not private archival records. Section 4.8.2 of the Schedule outlines the following requirements:

> The information made available shall include

[55] Letter to Ms. Susan Whelan, Chair, Standing Committee on Industry, April 20, 1999 at **aca.archives.ca/official.com/c-54/index.htm** at p. 2.

(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

(b) the means of gaining access to personal information held by the organization;

(c) a description of the type of personal information held by the organization, including a general account of its use;

(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

(e) what personal information is made available to related organizations (e.g. subsidiaries).

In preparing standard responses to these categories for their privacy codes, archives need to remember that they hold personal information in their collections, but they also collect personal information from those who work for the organization and from patrons and users of the archives. The brochures that most archives have available for users and visitors should address such issues as concisely as possible.

Principle 9 - Individual Access: "Upon request, an individual **shall** be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate." The attached note is directly relevant to archives: "In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide…."[56]

Compliance with principle 9 could be literally impossible for most archives, if it were construed to mean that they were somehow responsible for informing a requester whether any information about him or her was held in the entire archive, as opposed to records of employees, donors, users, and the like. The National Archives, for example, would have no practical way of knowing whether an applicant's name appeared in the employment records of the local operations of a particular company without doing research on behalf of the applicant, which would lie beyond the normal duty of a data custodian for this type of archival information. Fortunately, the note to principle 9 does acknowledge that "[i]n certain situations, an organization may not be able to provide access to all the personal information it holds about an individual," although, typically for Schedule 1 and the CSA Code, the drafters wrote as if they have never reflected on an archive as a normal place for storing substantial amounts of personal information.[57] This note lists a number of "limited and specific" reasons why an organization may need to deny access, including a number of considerations applicable to archives as well:

---

[56] Although I am aware that section 2(2) removes the two notes in Schedule 1 from the Act, I encourage those seeking to comply with the national statutory standard that it creates to look to the notes for guidance on best practices.

[57] I acknowledge that this notes has no legal force in the Act and is simply an example.

- Information that is prohibitively costly to provide,
- Information that contains references to other individuals [third-party information],
- Information that cannot be disclosed for legal, security, or commercial proprietary reasons,
- Information that is subject to solicitor-client or litigation privilege.

A standard response from an archive, for its archival holdings, could be that applicants for access would have to do **their own** research in the archives to learn what information exists about them in relevant archival holdings.[58]

Section 4.9.3 would require an archive to inform requesters to whom it discloses personal information collected from them for administrative purposes, such as the membership in the friends and supporters of a specific archive. For the latter information, a data subject has rights of correction of inaccurate information held about them. Neither consideration appears to be relevant to the normal work of an archive.

Principle 10 - Challenging Compliance: "An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance."

This is a reference to those accountable under principle one. Principle 10 essentially requires an archive to have a complaint-handling mechanism, which should already be the case for well-established archives. In practice, complaints against archives for breach of fair information practices will be necessarily limited to complaints that the routine handling of administrative information about specific persons is somehow not in compliance with Schedule 1. It is barely conceivable, although not unimaginable, that a person could actually discover that an archive held information about him or her without knowledge or consent and want the information excised. Finally, there is an obligation on an archive to investigate complaints received.

4. The Realities of Archives in Canada

[58] It would be extremely hostile to the privacy enterprise to require an archive to somehow index its holdings so as to be able to indicate to an applicant what personal information it held about him or her on a global basis. The enactment of the Swedish *Data Act* in 1973 led to the ridiculous situation whereby, in order to fulfill such access requests, the record holdings of Statistics Sweden had to be made searchable on the basis of individual names, which had not been previously possible. See David H. Flaherty, Privacy and Government Data Banks: an international perspective (Mansell, London, 1979), p. 118.

There are several separate issues here: the first is the wide variety of archives in this country, the second is the kinds of personal data that they archive on a permanent basis, and the third is the question of accessibility and how that information is shared or made publicly available.[59] They require brief attention here, as a reminder to the archival community to keep its house in good order from a privacy and data protection perspective (which means complying with fair information practices, an issue to which I return below).

Archives in Canada, it should perhaps be said, will collect any significant historical records of the Canadian past, including the records of corporations, companies, law firms, and banks and trust companies.[60] The National Archives of Canada, for example, houses records from Air Canada, Massey Ferguson, the Bank of Montreal, the Canadian Pacific Railway, an Ottawa law firm (1808-1973), Dominion Textiles Inc. (1860-1997), and the Molson family and business records (1619-1992), including diaries. The National Archives has a mandate to acquire private sector records of national significance. Provincial, municipal, local, and specialized archives have similar obligations. In fact, it would normally be considered a great coup for any archive to acquire the records of a major company, such as the Hudson's Bay Company's voluminous and ongoing records held at the Manitoba Archives. It would be hard for anyone, including official privacy protectors, to argue against such collection activities from any perspective, although the current initiative of the Privacy Commissioner of Canada in seeking to limit access to the original records of early 20th century censuses should make any commentator cautious in this regard.[61]

A number of major Canadian companies maintain their own archives, such as Hydro-Quebec, Ontario Hydro, Manulife, SunLife, and Scotiabank, all of which are listed in the Directory of Archival Repositories.[62] A major forest products company like McMillan Bloedel sent its own archives to the University of British Columbia Archives after completion of a history of the company. The relevant moral may simply be that there is no predicting which records of the past, including personal information, will survive in an archive or in what kind of archive.[63] The purpose of an "archive" is to protect and disclose records of archival value.

Companies for the most part do not retain considerable amounts of personal information on employees and customers over time. They have developed record retention schedules that follow largely legal and consumer protection requirements for how long such records need to be retained (and to meet all of the business and operational requirements of the firm) and then they are destroyed. During a recent

---

[59] See the *Directory of Archival Repositories* on the web site of the Canadian Council of Archivists: **www.cdncouncilarchives.ca**. A 1989 survey included 700 Canadian archives. A 1996 Directory of Archives is 442 pages in length and evidently described 520 institutions, which can be categorized by jurisdiction (federal, provincial, and territorial), theme, and type.

[60] A helpful definition of an archives includes the following: (1) "The non-current records of an organization or institution preserved because of their continuing value; also referred to, in this sense, as archival materials or archival holdings." (2) "The agency responsible for selecting, preserving, and making available archival materials; also referred to as an archival agency." Frank Evans, et al., A Brief Glossary for Archivists, Manuscript Curators, and Records Managers (July, 1974).

[61] See Privacy Commissioner of Canada, Annual Report 1998-99 (Ottawa, 1999), pp. 26-27 at **www.privcom.gc.ca;** and Canadian Historical Association, Brief to the Expert Panel on Access to Historical Census Records, February 9, 2000, at http://www.yorku.ca/research/cha/html/english/census/censusbr_e.htm#top

[62] See www.cdncouncilarchives.ca

[63] A commentator on an earlier draft informed me that there are some few medical files, securely protected, in the holdings of private records at the National Archives, as well as legal files of law firms there and in other archival institutions as well.

privacy assessment that I undertook for a Canadian bank, I reviewed its record retention schedule, which revealed that banking information on individual customers is not stored for long periods, even if one remains a customer of a financial institution for ten or twenty years. To put it simply, such companies have no financial incentive to store such personal records for more than five to ten years, at most, from the date of a transaction. Even the value of personal information on customers used in data warehouses for marketing purposes does not have a very long shelf life, because such companies need the most current information possible in order to profile, categorize, and then target their customers, or prospective customers, with solicitations for particular products and services. Institutions that do information-based marketing (and all commercial organizations do so) want a profile of their customers in the immediate past and the present. Thus records about individuals stored in hard copy (paper and fiche) and digital information are destroyed on a regular basis. Since the advent of large-scale automation in the early 1960s, it would be very surprising if companies had lists of individual customers that were available ten years after the fact, whereas it is possible that the records of a particular store or financial institution from earlier times might still have ledgers and registers in existence covering personal information. Historians naturally fear that the ease of destroying digital records today, their transitory character, and the lack of incentives for a company to spend money on internal archives, will make it increasingly difficult to write in an informed manner about the Canadian past. Thus, I argue that the privacy issues posed by archival records are *de minimis* from any kind of broad perspective, because they contain so little personal information. Even such public institutions as hospitals do not, in fact, keep patient records much beyond a ten-year period, unless an individual continues to be treated regularly by that hospital.[64] Similarly, it appears to be unheard of in Canada for the patient records of an individual physician, or a group medical practice, to be archived.

The likely main source of **sensitive** personal information in corporate records would be employee or human resource records. Again, the realities are, especially for the past forty years, that most companies keep only skeletal records of a person's employment over time. Good practices among Human Resource professionals is to cull files on an annual basis to remove irrelevant information or data that are no longer timely. Most union contracts require the destruction or removal of disciplinary or grievance records after relatively brief periods. My experience in British Columbia was that institutions of higher education were less likely to clean out faculty files over time. For universities created in the 1960s or thereafter, the file of a particular faculty member contained unnecessary personal information from the past that proper archival procedures should address. In the private sector, when an employee retires, is terminated, or leaves for another position, the likelihood is that his or her records will be scheduled for destruction after a relatively short period of time. Moreover, the modern corporation does not itself store very much sensitive information on employees. Disability records are in the keeping of insurance companies. Companies that offer counselling services to employees usually employ specialized companies for that purpose and pay only for blocks of time, not the receipt of individualized records. An exception to the rule of companies not collecting and storing of personal information would be files on senior executives, such as a president and chief executive officer.

Despite all of these qualifications, official data protectors will require assurances from various types

---

[64] When I located a church-related hospital in northern British Columbia that had a full set of patient records dating back to the 1920s, my interest, even as the Privacy Commissioner for British Columbia, was to ensure their survival and eventual location in an archive under **controlled conditions** for access to them, since they should prove to be so useful for illuminating the history of a particular region that contains many indigenous persons. The reality is that the lack of an established archive for northern British Columbia makes the survival of such records problematic. I had a similar reaction to the actual survival of the patient records of a famous mental institution in the lower mainland. Placing such records in an approved archives can meet the twin goals of preserving the Canadian past and being sensitive to the privacy rights of those persons whose lives are chronicled in part in such extremely-sensitive records.

of archives under their jurisdiction that there are procedures in place for ensuring and preserving the privacy interests of personal information about individuals in their custody and control. Such issues do not arise so directly, if a company maintains its own archives, as leading corporations do. However, what happens to the records of a company like Eaton's when it goes out of business completely? One would hope that a major archive would acquire its records for preservation, but how does that happen? From a privacy perspective, the placement of personal records in any archive must occur in compliance with fair information practices, whether based on law or self-regulation (for which the Act sets the **national standard** in a manner more precisely than public sector privacy laws). This is especially the case as it has become possible for archives to store all kinds of personal records in an electronic format that is compact and does not require the shelf space of paper records; such digital records are also more readily searchable and linkable to other data bases that are in an electronic format. Electronic records are thus very much of a two-edged sword for the archival community: they are thought to be easier to destroy and to store.

In general, and at the present time, a properly-functioning archives receives major and minor collections of records on the basis of an acquisitions agreement with the donor that is likely to set some restrictions on access to them. Thus, for example, the National Archives' recent acquisition of the records of a particular company includes films, video, artwork, plans, technical drawings, slides, photographs, and textual records, including corporate minute books, correspondence of company executives, cancelled share certificates, public relations records, price lists, legal records, financial records, and labour relations records. Based on a listing provided to me by the National Archives, none of this material appears to be sensitive from a privacy perspective, yet restrictions on access appear to exist.[65] I was informed that corporate records of this particular company that were more than 75 years old would likely be open for consultation without restrictions, whereas records less than 15 years old would likely be restricted at the request of the donor company. However "files containing personal information on individuals will be restricted to protect the privacy of the individual," including payroll records and union grievance files. The Manuscript Division of the National Archives has guidelines for that purpose.

Under sections 7 and 8 of the *Privacy Act* and its Regulation 6, the National Archives has a twenty-five-page publication entitled Guidelines for the Disclosure of Personal Information for Historical Research at the National Archives of Canada (1995). The most significant rules include the following, which I quote here to illustrate the kinds of rules that archivists are most likely to follow, or perhaps should follow, with respect to the disclosure of at least certain personal information in their custody and control:

- The code applies only to personal information from government records about a living individual or to persons who have been deceased twenty years or less. [a good principle]

- Government personal information held for archival or historical purposes may be disclosed in accordance with the regulations for research or statistical purposes. (Section 8[3] of the *Privacy Act*) [The majority of researchers obtain access to personal information in archival records through this provision. The invasion-of-privacy test under it ensures that extremely sensitive information remains protected.]

---

[65] With the advent of the Act, it would be highly desirable for such access restrictions for corporate records to be fully spelled out at the time of a donation. Template agreements for such purposes should not be difficult to fashion that could include the requirements of the Act.

- Information disclosed for such purposes must be of such a nature that disclosure would not constitute an unwarranted invasion of the privacy of the individual to whom the information relates (Regulation 6).
- Identifiable personal information may be disclosed for research and statistical purposes, if this is reasonably necessary for the purpose for disclosure (Section 8(2)(j) of the *Privacy Act*). [this is comparable to s. 7(3)(f) in the Act] [Researchers rely on this provision [8(2)(j)] infrequently for access to personal information arranged in case files, which would include personnel, immigration, and unemployment insurance records.]

- Obtains a written undertaking from the researcher that "no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates.""[a useful clause for everything except biographical and genealogical research]

Acting in accordance with Treasury Board policy, the National Archives has developed an **invasion-of-privacy test** to determine whether disclosure of sensitive information "would clearly result in harm or injury to the individual to whom it pertains." The four interrelated factors in the test are as follows:

- Expectations of the individual: For example, was the information compiled or obtained under guarantees which preclude some or all types of disclosures?

- Degree of sensitivity of the information: highly sensitive (medical, criminal activity, law enforcement, security, and finances) versus innocuous? Current information versus information for which the passage of time has reduced the sensitivity?

- Probability of causing measurable injury to the individual in the form of "any harm or embarrassment which will have direct negative effects on an individual's career, reputation, financial position, health or well-being."

- Context of the personal information in a file must be assessed in relation to the entire file in order to ensure that disclosure "does not form part of a crucial segment of a larger picture that could reasonably be expected to be injurious to the individual."

The National Archives thus has detailed rules in place for certain kinds of records requiring a clear and detailed research proposal, an outline of the specific records requested, a statement of the methodology to be used to protect the privacy of individual subjects, and a statement of the accountability of the applicant.[66] Finally, Treasury Board policy requires that "[w]hen a government institution is transferring personal information for archival or historical purposes, the National Archives should consult that organization for advice on records containing information which, is disclosed, could constitute an unwarranted invasion of privacy."[67] Again, this is a sound policy for any archive to

---

[66] National Archives of Canada, Guidelines for the Disclosure of Personal Information for Historical Research at the National Archives of Canada (1995), pp. 6-7.

[67] Ibid., p. 21.

emulate when it is accessioning personal records (and the reality is that few records do not contain any personal information in them). Once such departmental records are at the National Archives, it has the sole discretion, under section 8(3) of the *Privacy Act*, to disclose personal information to researchers.

The Manitoba Archives has developed some novel practices in the sense that all applications for access to recent government records in its custody and control have to be processed by the departments concerned, including those that involve considerable amounts of personal information.[68] This fifteen-year old practice is partly the result of the costs involved, and the expectation that individual departments will have greater understanding of the sensitivity of personal information in their own records. All government records are also scheduled for destruction or retention based on information in the Access and Privacy Directory for the province.[69] The Manitoba Archives also collects records extensively in the private sector from businesses, labour groups, and churches. Access to such records is controlled by means of a donation agreement, a set of restrictions on access, and research agreements with researchers for access to *restricted* records, which are obviously essential for any sensible archival arrangements.[70] The Archives discusses privacy considerations with potential donors and expects to come to terms with them about any conditions, such as periods of time before records are fully open. The Manitoba *Freedom of Information and Protection of Privacy Act* has a 100-year rule applicable to all records being open. This means in practice that privacy rights cease to exist one hundred years after the creation of the record. The Hudson's Bay Company continues to give its records to the Manitoba Archives but the company is careful about the transfer of, or access to, records covering the last fifty years of its history. Personal records are available after 50 years, general records after 30 years, and minutes after 15 years.

The Manitoba Archives has a standard agreement with the Law Society of Manitoba to collect records of law firms and legal practices. It houses the records as well of the Children's Home of Winnipeg, which was a private sector organization. It also houses records collected since the 1930s under the *Juvenile Delinquents Act* and the *Young Offenders Act*. These are all categories of sensitive records.

The status of personal records obtained by any archive in the course of the past century is somewhat different, in the sense that a formal agreement with donors is less likely to exist. The archives of a Catholic or Anglican religious order or diocese would be a good case in point, since they were likely

---

[68] I am grateful to Gordon Dodds, the Manitoba Archivist, for allowing me to interview him in Winnipeg on March 8, 2000 for purposes of this guide and commentary.

[69] See **http://www.gov.mb.ca/chc/archives/fippa_mn.html**. What should impress laypersons and privacy officials about this directory is that most of the records listed appear to be slated for destruction rather than archival retention and eventual disclosure, thus reinforcing the view that many ~~most~~ personal records do not have historical value. This is certainly true for the vast amount of digital personal data currently being produced in advanced industrial societies like Canada. The Manitoba Archives estimates that it retains 4 to 5 percent of the total government output of records, and approximately 1 percent of what is archived can be considered primarily personal information (Personal communication, Gordon Dodds, March 30, 2000).

[70] These Manitoba model forms are deliberately written in general language, but ~~at least~~ they provide a good starting point for discussions with both donors and researchers. The Scotiabank Archives states that it keeps 0.5 percent of all of the records that the bank produces in a year: **www.scotiabank.com/archist2.htm**. With respect to archival retention, it is sensitive to what personal records it retains and what it gives out to users. The archives handles the personnel files of senior executives very carefully.

accumulated over time and retained for their obvious historical value, long before sensitivity to the protection of personal privacy was an issue, or at least an issue as visible as it has been during the past thirty years. Data protection legislation, such as in Quebec, applies to such archives (the archives of religious groups at Bishop's University are a current example) on an *ex post facto* basis.[71] A related reality is that many ongoing archives of specific organizations contain records of personal information for the second half of the twentieth century, which are inherently more sensitive from a privacy perspective than older records. Thus the B.C. Archives, for example, holds court records and correspondence that contain information restricted from disclosure under the federal Young Offenders Act, as well as adoption records and divorce records. Its collection of "non-government records" includes records from the Royal Jubilee Hospital in Victoria that contains patient registers and admissions and discharge books from the 1950s (but not patient files).[72] These are good examples of how sensitive personal information is often buried deep within records that are otherwise completely benign. Archivists have to keep fair information practices in mind as they contemplate permitting access to such information for legitimate research purposes in particular.

Another reality is that surviving records of any corporate entity are likely given to an external archives without substantial knowledge on the part of the company of what they really contain, especially if the records are reasonably old, as in the case of some of the Dominion Textile records. A decision is simply made to archive records that are still in existence and have not been destroyed according to record management criteria. A manuscript archivist then undertakes the task of organizing the collection and disposing of non-archival material. For example, depending on the size and age of a collection of papers, the archivist will weed out and dispose of duplicates, standardized forms, and records that are routine and transactional in nature.[73] Since public archives are never adequately funded, some deposited records may simply remain uncatalogued for long periods. The Manitoba Archives solicits funding for the organization of records before agreeing to archive them.
The National Archives has prepared selection criteria, or draft guidelines, for the archival retention of business records.[74] This document states up front that only 2 to 5 percent of the total records of a firm will be of interest to an archive. The listed categories of desired and desirable records are overwhelmingly of a general business nature. The most evident personal information would be the personal correspondence, diaries, and oral histories of senior company officers.

---

[71] My understanding is that the data protection situation in Quebec is made even more complex for archives there by the consent requirements established in the Quebec Civil Code. Joanne Burgess, the president of the Institut d'histoire de l'Amérique française, stated as follows: "The extensive revision of the Quebec Civil Code in 1994 further strengthened the protection of privacy in the private sector by regulating the behaviour of individuals and organizations not subject to existing legislation. Articles 35 to 40 of the new Code establish an extremely broad definition of privacy and of what constitutes invasion of privacy. Article 35 states that 'every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person or his heirs unless authorized by law.' The right to privacy is thus transformed into an inheritance which may be transmitted to one's heirs and continue to flourish after death." The author proceeds to discuss aspects of the *Loi sur les Archives* and the legislative review of Quebec's access to information and privacy legislation that render a complex situation even more complicated for archivists and historians. See http://www.yorku.ca/research/cha/html/english/burgess_bull_e.html.

[72] Information from Mac Culham of the B.C. Archives, which wisely administers access to such records in compliance with the B.C. *Freedom of Information and Protection of Privacy Act.*

[73] However, records of individuals appear to be the kind of records that archives are most likely to retain in the form of wills, personal correspondence, family papers and correspondence, oral histories, tax returns, photographs, memoirs, and diaries. See the Archives Association of British Columbia's "Archivist's Toolkit" and, especially, its Manual for Small Archives (1994 edition), which offers detailed guidance on how to run such an archive, many of which depend solely on volunteer staff, often share space with a museum, library, municipal hall, historical society, or a county museum, and largely depend on records of all sorts that are donated to them.

[74] National Archives of Canada, "Archival Retention of Business Records," Unofficial draft, revised by M. Stephen Salmon, Business Archivist, December, 1998.

One of the problems of small to medium-sized organizations is that records management systems are less likely to be in place than in larger companies. This means that personal records will not be systematically destroyed on the basis of record retention schedules. Bill C-6 may force progress on this score, but the problem of adequate resourcing for record management functions is an ongoing one. In fact, the culling of Human Resources or personnel records over time often does not happen, so that more personal information continues to accumulate in employees files than is really necessary for personnel management. The irony in such practices is the prevailing wisdom that the vast majority of personnel/Human Resources files have no permanent value from an archival perspective and are thus slated for destruction after an individual's working relationship (including pensions) with an organization has ended.[75]

The National Archives informed me that restrictions on access to records in its collections are negotiated at the time of acquisition and on an individual basis. Typically, the restrictions are listed in an accompanying binder. For the Molson Archives Fonds, for example, access requires the written permission of a family member, which permission is usually granted. Such restrictions are loosely based on privacy concerns and in keeping with the spirit of the federal *Privacy Act*. Corporate proprietary information could also be restricted, perhaps for a period of 20 to 30 years.
A business archivist at the National Archives remarked on the inclusion of social insurance numbers on boxes of payroll cards from mills of Dominion Textiles from the 1930s to the end of the Second World War. These numbers were added later (it would have to be after 1963-64), when pensions continued to be paid to particular individuals. From a privacy perspective, the existence of the social insurance number on a particular record is no more or less sensitive than information that could be derived from payroll cards about sex, race, age, and home address. Proper controls on access to this particular set of records should spell out, in a research agreement, what the qualified researcher intends to do, and can do, with the data in question.[76] The National Archives can be expected to be a leader in this regard. Smaller and less well-funded "archives" would be in a different situation.

Historians, who are one of the primary professional users of historical records in archives, perhaps naturally fear that signing **research agreements** will hinder the execution of their research and perhaps even result in censorship of what they can accomplish.[77] I would argue, at least on the basis of my experience in British Columbia, that that is not proving to be the case, even though privacy rules mandated by law do require archivists to review records in their care from a privacy perspective before allowing scholarly access to them (or controlling the process on the basis of research agreements).[78] Tensions, in this regard, are most likely to arise in the context of biographical research on living or

---

[75] I am grateful to Ian Forsyth, archivist of Simon Fraser University, for information on this issue.

[76] Provincial privacy acts, for example in Ontario and British Columbia, provide for the disclosure of identifiable personal information on the basis of research agreements, which likely include prohibitions on subsequent disclosure in identifiable form without the consent of the public body holding the data. See *Freedom of Information and Protection of Privacy Act*, R.S.B.C., 1966, c. 165, s. 35.

[77] My primary concern here is research agreements for the protection of privacy, but archives subject to freedom of information and protection of privacy acts are also imposing, or being required to impose by public bodies, enhanced research agreements to monitor compliance with other types of exemptions from disclosure, such as solicitor-client privilege and law enforcement. The B.C. Archives is an example of such practices, which run counter to the interests of archivists in promoting access to records held by them.

[78] As a scholar myself, I received direct requests from researchers for assistance in getting access to records covered by the B.C. Act. In at least several instances, it took only one telephone call to ensure that data custodians assisted the researcher with his or her perceived problem. My sense was that any complaints from academics about limits on research access (from a privacy perspective) did not reflect reality. They need to plan and prepare adequately in advance to obtain access to certain archival records; they also need to understand the public interest that is served by the existence of protective legislation, such as the B.C. Act. When I indirectly encouraged senior administrators to encourage those concerned about barriers to research access to consult with me, I heard nothing.

recently deceased persons. I would compare the situation of historians under privacy legislation to social scientists and medical researchers attached to universities and university-affiliated research institutions in British Columbia, whose collection, use, storage, and disclosure of personal information is now subject to the fair information practices in the B.C. *Freedom of Information and Protection of Privacy Act*.[79] From my perspective as both a researcher and a privacy advocate, there must be some tightening up, and consciousness-raising, about fair information practices, including consent, among members of the scholarly community.[80] The various ethical codes of the national research funding agencies also mandate such sensitivity, but without the force of law behind them.

5. The Purpose of Part 1 of the Act and its Intended Application

The long title for part 1 of the Act indicates that it is intended "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances…." Traditional archives, at least to date, have little to do with electronic commerce, at least so far, but they do engage in limited "commercial" activities.[81] More significantly, however, section 3 states that the purpose of Part 1 is "to establish … rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that **a reasonable person** would consider appropriate in the circumstances." (Emphasis added)

The **"reasonable person" test** is especially important in terms of dealing with the issue of whether customers, patrons, donors, and users have reasonable expectations of having personal information about them stored in an archive. Most people (if they ever had occasion to think about it) would be likely to find the archiving of certain kinds of information about them to be perfectly acceptable and normal. Archivists in various kinds and types of organizations, however, need to keep the "reasonable person" test in mind as they make decisions about whether to accept gifts of sensitive personal data in particular.

The "reasonable person" test imports an objective rather than subjective test. In other words, a Court

---

[79] See the results of a site visit that I conducted of the B.C. Cancer Agency as Information and Privacy Commissioner for British Columbia at **www.oipcbc.org/investigations**.

[80] Ian Forsyth, the archivist for Simon Fraser University's archives, has found the privacy provisions and research agreements in the B.C. act relatively easy to work with in terms of accomplishing the dual goals of an archivist and a privacy protector (Telephone interview, March 24, 2000). Forsyth states that he does not find it difficult to persuade researchers that they should comply with fair information practices when they are working with the personal data of other people.

[81] But if parts of the Actual holdings of a traditional archive were put on a web site, and charges were imposed for access to such information (necessarily including personal information), then the activity would likely fall within the scope of electronic commerce. A "commercial" activity of an archive could include charging for provision of photocopies and the lending of microfilm, the rental of lockers, and user fees for access to records, if it "discloses the information outside the province for consideration." (Section 30[1] of the Act) Such commercial activities are admittedly incidental to the operations of a non-commercial entity (most archives), but a decision on the coverage of such activities in practice will depend upon the Privacy Commissioner of Canada and the Federal Court of Canada.

applies an "objective" test for determining what a "reasonable person" in the shoes of the customer would conclude, as opposed to the "subjective" view of the customer in question. What this really represents in practice is a judge's ability to apply his or her own views on what is reasonable (which is another reason why archives should be careful in their dealings with courts, judges, and official privacy protectors).

The personal records of a law firm or a medical, psychiatric, or dental practice would be examples of areas to be very careful about in terms of disclosure to a user.[82] Because the Act calls for the proper collection and disposal of personal information, this issue can be re-stated as deciding when personal information, already held for long periods by an archive, can be made available to researchers. The qualifying reality test, however, is that many of the most sensitive personal records (psychiatric records, for example) are regularly destroyed by those who created them.

The relevant definitions in section 2 could likely be construed to cover the range of archives that exist in Canada and that are not already covered by earlier privacy legislation:

- An **organization** [which is what the Act covers] includes an association, a partnership, and a person [including a corporation or company]
- **Personal information** means information about an identifiable individual
- A **record** includes any correspondence, memorandum, photograph, film, microform, videotape, and machine-readable record

The scope of this intended coverage of personal information (which parallels existing provincial and territorial legislation) is one reason why a sub-theme of this guide and commentary is that **any archive should comply with the national standard established by the Act, whether they are technically covered or not**. Practically every archive will contain some records that the Act would likely cover. Moreover, it will be cheaper for an archive to act as if the Act covers it than it will be to pay lawyers to provide opinions on jurisdiction. Official data protectors will also not enjoy being told that they have no jurisdiction over certain collections of personal records (even if it is technically true). Cultivation of positive working relationships with the latter should occur even if, at the end of the day, compliance is largely based on voluntary self-regulation. Those living persons whose records are stored in an archive are also not going to be interested in Jesuitical distinctions over definitions and jurisdictions.

There are three additional provisions in sections 2 and 30 of the Act that turn discussions of its intended scope into quite muddled waters. The federal government can only act to exercise its trade and commerce powers under the *Constitution Act, 1867* and decisions of the Supreme Court of Canada by regulating **commercial activity**, which the Act defines as follows:

"commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

---

[82] Physicians in private practice in British Columbia normally destroy patient records six to ten years from the date of the last entry, unless the patient is a minor. The expectation is that all patient records will be destroyed eventually in a manner that preserves confidentiality. These obligations do not cease even if a physician ceases to practice or sells or transfers a practice. See Royal College of Physicians & Surgeons of British Columbia, Policy Manual (June, 1995), pp. D2-1, and M4-1 to M4-2.

This definition means that any organization that is in business and that collects, uses, or discloses personal information in the course of doing business will be bound by the Act for all of its activities (or, at the very least, those that are of a commercial character). On the other hand, if any organization is not in business, such as a charitable or an educational organization, its regular activities will not be subject to the law, because they are not of a commercial character. However, if that organization engages from time to time in commercial activities, such as selling its membership lists, for example, that particular transaction would be subject to the Act.[83] The House of Commons added this particular clarifying sub-clause during third reading, which further illustrates the ambitious reach of the drafters and framers of Bill C-6. Thus the selling, bartering or leasing of donor, membership or other fundraising lists by archives will fall under the coverage of the Act, if not already covered by a provincial or territorial act.[84]

A second major definition dealing with the scope of the Act seemingly limits its application to federal works, undertakings, or businesses that are within the legislative authority of Parliament. The list that follows these terms at least includes navigation and shipping companies, railways, airlines, radio broadcasting stations, and banks. Most such large organizations are likely to maintain some kind of archive, which would thus be subject to the Act.

When Bill C-54, as it then was, was tabled in the House of Commons in early October, 1998, it had one great surprise in store, even for privacy advocates, in the form of section 30, the so-called transitional provisions, because Industry Canada effectively extended the reach of the Bill a considerable way into the traditional jurisdiction of the provinces in order to seek to protect electronic commerce by means of the exercise of its trade and commerce power.[85] Section 30(1) states that the Act does not apply to any organization that collects, uses, or discloses personal information within a province whose legislature has the power to regulate such activities, "**unless the organization does it in connection with the operation of a federal work, undertaking or business** [a very limited list, as just noted] **or the organization discloses the information outside the province for consideration**." By this astonishing stroke of the legal pen, the Act applies almost immediately not only to **commercial** uses of personal information by federal undertakings, but also to commercial uses of personal information **in the form of disclosures** that cross provincial and territorial boundaries. For the latter transactions to be covered, there must be a disclosure for commercial purposes, not just an internal transfer of information within an organization. I do not know enough about commercial uses of information by various kinds of archives to understand whether there is any likelihood of their being captured by section 30's interprovincial reach. [HB: unlikely, since they are public bodies anyway.] In any event, the provisions of section 30(1) will not come into force until three years after the likely date of entering into force of the Act, which is January 1, 2001, unless an organization is a federal undertaking or engages in commercial **disclosures** of personal information outside a province.

Now that the House of Commons has finally passed Bill C-6, organizations in the private sector and their trade associations will be bringing considerable pressure to bear on provincial and territorial

---

[83] I am especially grateful to Heather Black of the Department of Justice for clarifying the meaning of commercial activity for me as well as many other aspects of the relationship between the Act and archives.

[84] Since questions will necessarily arise as to whether the Yukon or British Columbia privacy acts cover such aspects of the work of the Yukon Archives or the B.C. Provincial Archives, both organizations would be well advised to ensure that they comply with the spirit of the Act for these purposes.

[85] Although this "intrusion" into the sphere of the provinces will likely attract constitutional challenges from the largest provinces, archives would be unwise to rely on them as a form of escape from the rigors of the Act.

governments to adopt the Act as it is written, or to harmonize its own initiatives in response to the Act over the course of the next several years. The Industry Minister, John Manley, announced that Quebec would be recognized in regulations as already having acts that comply with the standards set by the CSA Code and the Act. Thus, privacy standards and the oversight of the Commission on Access to Information already cover any archive located within the province of Quebec. This Commission is very aware of data protection problems already posed by sensitive records held in archives of religious organizations in particular.

Section 4(1) sets out, most explicitly, the intended **application** of part 1 of the Act. Most importantly, it "applies to every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of **commercial** activities." (Emphasis added) Ironically, a second qualification establishes that the Act does not cover the employee information of such organizations, unless the organization is a federal work, undertaking, or business. Section 4(1) is the federal government's key exercise of its trade and commerce power, but it does not have the legal authority to protect the personal information of private sector employees in general.[86] In practice, any archive should make sure that it ensures fair information practices for the personal information of its employees, volunteers, and consultants, whatever their legal status under the Act.

Section 4(2) takes the negative approach to the intended application of part 1 by specifying what it **does not apply** to:

- Any government institution to which the *Privacy Act* applies; [Since the National Archives of Canada (which is *the* repository of the Government of Canada) is covered by that Act, Part 1 of the Act does not apply to it. The National Archives proposed an amendment, wisely, to the effect that records deposited in federal institutions, but created in the private sector, would remain subject to the provisions of the Act. This would at least have covered a significant loophole, which will again have to be addressed on a practical basis.

- Any individual with respect to personal information that the individual collects, uses or discloses for **personal** or **domestic purposes** and does not collect, use or disclose for any other purpose; [the intention is to exclude from the scope of Part 1 personal information that is used within a household or by an individual solely for what are traditionally regarded as private activities, such as address lists of friends and relatives, diaries, letters, personal e-mail, greeting cards, and photographs. Ironically, if such records found their way to an archive, controls on access would likely have to be put in place to ensure compliance with fair information practices, since the uses of the information would no longer be strictly personal or domestic. This best practice should occur on a legal or self-regulatory basis.]

- Any organization in respect of personal information that the organization collects, uses or discloses for **journalistic, artistic or literary purposes** and does not collect, use or disclose for any other purpose. This is the same language discussed above concerning section 7(1)(c). It essentially means that most personal information

[86] This is a significant limitation of the Act that provinces and territories will have to remedy. Quebec already offers such protections to all employees in the province.

collected by an archive will not be covered by Part 1.[87] The intent of the drafters of the narrowly-framed language of section 4(2)(c) was to protect the broad rights of freedom of expression set out in section 2(b) of the *Charter of Rights and Freedoms*.[88] The Department of Canadian Heritage and Industry Canada gave verbal assurances to the National Archives that Bill C-6 would have little or no impact on archives, because of section 4(2)(c). Again, my strong recommendation is that archives treat personal records in compliance with fair information practices and not seek refuge in statutory exemptions, such as these ones. The motivation should be there for all archives to be models of sensitivity to privacy, while at the same time continuing with their important tasks of making accessible the historical memory of the country for legitimate purposes. The burden of achieving a suitable balance may be greater for smaller archives, especially those that are non-public entities.

Section 4(3) is a paramountcy clause establishing that part 1 of the Act applies (after it comes into force), unless another Act of Parliament specifies that a provision operates despite the provision of this part. For example, a revised National Archives Act would have to specify that it took precedence over Part 1, if that was the intention of Parliament.[89]

6. How Part 1 of the Act modifies Schedule 1 and the CSA Code

Sections 5 to 10 of Part 1 qualify the principles set out in the CSA Code in Schedule 1. The complexities in the resulting discussion are the results of drafting practices, which the drafters believe were required in the circumstances. The main changes from the Schedule (section 7) have to do with when organizations can collect, use, or disclose information without the **consent** of an individual. Industry Canada decided that since the CSA Code has an open-ended list of inappropriate activities, it needed to close the loop with considerable precision as to what are acceptable and unacceptable practices.

Section 5 sets out the standards for compliance with the obligations established in the Schedule, subject to any other modifications set out in sections 6 to 9. The legal obligation to comply with the principles and practices in the Schedule only derives from the use of the word **shall** in the Schedule. When the word **should** is used in the Schedule, it indicates a **recommendation,** but not an

---

[87] However, I do regard it as problematic that the House of Commons and the Industry Canada drafters did not accept the intelligent proposal of the Association of Canadian Archivists that subsection 4(2)(c) "be extended without reservation, or any on-going reference to or approvals from the Privacy Commissioner, to include … 'any organization in respect of personal information that the organization collects, uses or discloses for archival or heritage purposes, or for scholarly or statistical research.'" See **aca.archives.ca/official.com/c54/c54brief.htm** at p. 4.

[88] Section 2(b) defines the following fundamental freedom: "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication."

[89] In the fullness of time, I would support customizing the governing legislation of any federal, provincial, or territorial archive to incorporate fair information practices in sectoral legislation more suitable to archival work than such omnibus legislation as the various *Privacy Acts* or The Act.

obligation.[90] All of the principles quoted above contain mandatory obligations in the forms of shall or shall not. The same obligations appear in most of the sub-sections of each principle, including consent, so on the whole it can be said that Part 1 of the Act gives full legal force to Schedule 1 (which is the only point that is important for archivists).

Section 5(3) also repeats an important provision in the form of a **reasonableness test** that also appears in the purpose clause (section 3). This will likely become an important tool in the hands of individuals who choose to complain to an organization and/or the Privacy Commissioner about specific practices of an organization. Thus, it bears repeated quotation in full here:

5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

A considerable amount of case law exists in the Anglo-American legal world on the meaning of the reasonable person test. It is also language that an archive can rely on for defense of traditional archival practices, even if it is not covered by Part 1 of the Act. Alternatively, a reasonable person test may warn an archive that an existing or contemplated collection or disclosure practice for personal information is risky from a privacy perspective.

Section 7 deals extensively with when an organization can legitimately collect, use, or disclose personal information without the knowledge or consent of an individual. Section 7(1) states that an organization may collect personal information without the knowledge or consent of the individual (principle 3) only if**:**

(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; [generally irrelevant to the work of an archive] or

(c) the collection is solely for journalistic, artistic or literary purposes; [likely relevant to the work of an archive and certainly relevant to users] or

(d) the information is publicly available and is specified by the regulations. [This highly problematic concept is intended to apply to records like the listings in a phone book]

Section 7(2) provides in part that an organization may **use** personal information without the knowledge or consent of the individual only:

---

[90] One of the great mysteries of the CSA Code is its mixing of "shall's" and "should's" throughout. The intention of the drafters was to ensure that compliance by the private sector did not become too onerous; hence the delicious irony in the fact that this self-regulatory code will now have the force of law.

(a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention; [could apply, in unusual circumstances, to an archive in the context of information about its patrons and clients, for example]

(b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual; [could apply to an archive, but again in very unusual circumstances]

(c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used; [discussed above]

(d) it is publicly available and is specified by the regulations; [a contentious issue that awaits clarification, but is unlikely to impact on archives] or

(e) it was collected under paragraph (1)(*a*) or (*b*).

Section 7(3) provides in part that an organization may **disclose** personal information without the knowledge or consent of the individual only if: ...
(**c.1**) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

…

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

…

(**f**) **for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;**

(**g**) **made to an institution [meaning an archive] whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;** [this provision allows organizations engaged in commercial activities to transfer records containing personal information to an archive without having to seek the consent of the individuals concerned.] [It is useful that this clause does not limit itself to an "archive" as such, since libraries and museums in this country regularly have archives attached to them, which may house significant collections of "records" and "personal information" as defined in section 2 of the Act.]

(**h**) made after the earlier of

(i) one hundred years after the record containing the information was created, and [this phrase lends further legitimacy to the archival practice of opening up

records completely after the passage of one hundred years]

(ii) twenty years after the death of the individual whom the information is about; [this is in effect a rather attractive test of the period of time after which personal information ceases to be especially sensitive]

(**h.1**) of information that is publicly available and is specified by the regulations;

…

(**i**) required by law.

(4) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

….

7. The Exercise of Access Rights: Sections 8 and 9

The potential exercise of rights of access to one's personal information is so complicated in the Act that the issue is treated separately here. For an archive subject to Part 1 of the Act, an individual has to be informed of how their personal information has been used, shall be given access to it, and can challenge the accuracy and completeness of the information and have a record amended as appropriate. (See Principle 9 above) The granting of access rights to any kind of information held by an archive could become so burdensome in practice, that the details require some elaboration here. This may be an area of information practices where an archive will have to have special exemptions in practice, since it will be highly impractical to try to inform any individual whether there is information about him or her in a particular archive. It is hard to imagine in practice that privacy rules will require an archive to do research on this issue, as opposed to facilitating research by the individual requester. The practical reality is that the National Archives is already responsible for private sector records that occupy approximately 47 kilometers of space, so a requirement for archives to search for information about particular persons makes no sense and is practically impossible.

Section 8 provides that a request for access to information has to be in writing, an organization has to help anyone who asks for help in preparing such a request, and it has to respond "with due diligence" not later than thirty days after receipt of the request. An organization can extend these time limits for another thirty days if meeting the original time limits "would unreasonably interfere" with its "activities," or the time required "to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet." Alternatively, the organization may extend the response time "for the period that is necessary in order to be able to convert the personal information into an alternative format." An organization has to notify the applicant of a time extension and indicate "their right to make a complaint to the Commissioner in respect of the extension." As a practical matter, this will largely become a source of aggravation to the staff of the Privacy Commissioner, since there is little that they can do about delays of this sort that are not systemic in character and, especially in the introductory phases of the legislation, some organizations will have considerable problems even

locating records that individuals want to access.[91] If an organization fails to respond within a time limit, it is deemed to have refused the request, which will lead the Privacy Commissioner's staff to make suitable inquiries about available explanations for this state of affairs.

Section 4.9.4 of Schedule 1 mandates that an organization "**shall** respond to an individual's request within a reasonable time and at minimal or no cost to the individual." (Emphasis added) But this is qualified by section 8(6) which stipulates that an organization may charge an individual for access only if it has informed the person of the approximate cost, and the individual has not withdrawn the request. I perceive this as a great source of potential conflict as non-archival organizations try to recover some of their costs of finding, severing, copying, and mailing records. The issue can be referred as a complaint to the Privacy Commissioner and then, upon receipt of the Commissioner's report, to the Federal Court of Canada. (Sections 11[1] and 14[1]) If an organization refuses to grant an individual access to his or her data, they have to give written reasons. A complaint to the Privacy Commissioner can also challenge such a refusal. The organization also has to retain requested information long enough "to allow the individual to exhaust any recourse under this Part that they may have."

Section 9 sets out a very complex process for refusing access to personal information in the first instance, if it would reveal "third party information," which means information about individuals other than the applicant. Most personal information files in fact contain information that belongs to others and not to the applicant, unless the third parties are reporting on the applicant, in which case the right of access exists. Such third party information should be **severed** from the record in question, when it is possible to do so (which is usually possible). Severing such a record is a tedious process, especially if a record is lengthy or a number of persons appear in it;. At the very least, the person doing the severing has to review the record on a line-by-line basis, unless he or she is absolutely certain, for example, that the record is a standard form which normally contains no third party information. Severing is not required if the third party consents to the access (which will require consultation), "or the individual needs the information because an individual's life, health or security is threatened." That strikes me as a rare eventuality.

Section 9(7) modifies principle 4.9 by setting out additional circumstances when access to personal information may be refused:

1. the information is protected by solicitor-client privilege;

2. to do so would reveal confidential commercial information;

3. to do so could reasonably be expected to threaten the life or security of another individual;

However, there is an obligation to sever two categories of information that do not have to be disclosed (confidential commercial information, or a threat to life or security of another individual).

My expectation is that there will be no obligation on archives to grant access to personal information held in archival records as opposed to other categories of personal records held by archives for administrative purposes, such as registration forms for patrons.

8. Complaints Investigated by the Privacy Commissioner of Canada (ss. 11-13)

[91] My point reflects my experience as Information and Privacy Commissioner for BC from 1993 to 1999.

The enforcement mechanisms associated with the Act largely rely on the Privacy Commissioner of Canada. A dissatisfied individual may file a written complaint with the Commissioner concerning an alleged contravention of a provision in Division 1 of the Act, or for an organization's failure to follow a recommendation in Schedule 1. The Privacy Commissioner may also initiate a complaint on his own, if he decides that there are reasonable grounds to conduct an investigation. The Privacy Commissioner's Office has operated essentially a complaint bureau for the federal private sector since 1978 and thus has a well-established routine for processing complaints.[92] It is unlikely that a privacy complaint would be made against an archive for breach of a standard first information practice.[93] It is possible, however, that a data subject could at least complain his or her information should not have been archived without specific consent, but the record to date for major archives makes this as unlikely prospect.

Section 11 specifies that the basis for a complaint must be a contravention of the measures for the protection of personal information set out in Division 1 (sections 5 to 10), which are mandatory obligations, or for not following a recommendation set out in Schedule 1. In practice, the scope of potential complaints is broad, because one can be filed against an organization for not following any recommendation set out in Schedule 1 (the CSA Code). Someone could conceivably complain, for example, that an archive was holding personal records in breach of the requirement for destruction in principle 4.5.3 of the Schedule. Again, the absence of such complaints in the past is a positive sign for the future.

A complaint dealing with section 8 issues (*i.e.* failure to assist an applicant with a timely response to a request for personal information, or failure to meet statutory time lines for responding) must be filed within six months of the actual occurrence of a refusal to respond, or the expiry of a time limit for responding, to such a request. Although the Privacy Commissioner may allow for a period longer than six months, it would stand to reason that would be the exception and not the rule.

The Privacy Commissioner must give notice of a complaint to the organization complained against. If an archive, for example, was not previously aware of the particular complaint, it will have a strong incentive, as noted above, to deal directly with the complainant to resolve any matter. The advantage for the complainant of using the services of the Privacy Commissioner's office is that a resolution would likely be subject to approval by it as well, making it harder for an organization to seek to brush off the individual complainant. At present, the National Archives and the Office of the Privacy Commissioner have a positive working relationship on issues that arise from complaints.

Section 12 sets out of the powers of the Privacy Commissioner with respect to investigations. These powers are, in fact, the standard arsenal available to a government official with investigative duties. They sound more threatening and heavy-handed to an organization complained against than they are likely to be in practice, unless such an organization proves to be resistant or recalcitrant in the face of the exercise of statutory jurisdiction.

---

[92] The web site of the Privacy Commissioner is http://www.privcom.gc.ca

[93] There are several dozen complaints each year at present against the National Archives, but they concern such matters as delays in granting access to information or refusals to grant access to third party information with respect to military and civilian personnel records housed in the Archives, or the records in the Archives of such agencies as the Canadian Security Intelligence Service, Corrections Canada, Immigration, and Indian Affairs.

In the first instance, the Commissioner has the right to require the production of any records or things considered necessary for the investigation of a complaint. In fact, he or she may even order the appearance of persons before the Commissioner and compel them to give oral or written evidence. In this capacity, the Commissioner has the same powers as a superior court in a province or territory (which means, in practice, that the Commissioner may seeks help from such courts, if his requirements are not satisfied). Based on the experience of the past twenty-two years, it would be highly unusual for the Privacy Commissioner of Canada to have to take such draconian steps to compel evidence, although John Reid, the Information Commissioner of Canada, has recently flexed his muscles in this regard, because of what he views as excessive delays in responding to requests for access to general information

The Commissioner has the power to administer oaths to those called to give evidence in the investigation of a complaint. Again, under normal circumstances, that would be an unusual practice, just as it would be highly unusual for such an official to conduct an oral inquiry in the course of investigating a complaint. Nevertheless, it would likely be a strong inducement for cooperation and compliance for the Commissioner to be able to threaten an initially uncooperative organization, including an archive, with an oral hearing.

The Privacy Commissioner has the power, at a reasonable time, to enter the premises occupied by an organization like an archive after satisfying any security requirements of the organization with respect to such premises. Once the Commissioner's staff have exercised their right to enter the premises of an organization for purposes of investigating a complaint, they may speak privately with any person in these premises or make any other inquiries that they see fit, such as looking at paper files or requiring access to digital records. They may also examine or obtain copies of any records found on the premises that contain "any matter relevant to the investigation."

Despite these powers, the Act intends to promote resolution of complaints in as informal a manner as possible, so the Privacy Commissioner is not restricted as to ways of taking evidence and obtaining other information deemed to be relevant, even if such "evidence" would not be admissible under the strict rules of a court of law, including the practice of cross-examination.

An essential requirement for dispute resolution also appears in section 12. Although the Commissioner does not have to do so, there will be strong pressures on the incumbent and his or her staff to resolve complaints by attempting mediation and/or conciliation between the complaint and the organization complained against. Based on federal, provincial, and territorial experience with privacy complaints and related matters, the effort at mediation is likely to be highly necessary and productive, given the limited and finite financial and human resources of those involved. Commission staff are likely to use a variety of strategies to find an accommodation between the parties. The success of the scheme will depend largely on the effectiveness of such approaches to problem solving with organizations covered by the Act.

The Commissioner has one year to prepare a written report for the various parties to a complaint, which must include the Commissioner's findings and recommendations, any settlement that the parties reached and, as appropriate, a request for the organization's response with respect to actions taken or not taken. Section 13(2) provides that the Commissioner is not required to prepare a report in the following circumstances:

1. the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;

2. the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this part, or the laws of a province;

3. the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was filed is such that a report would not serve a useful purpose; or

4. the complaint is trivial, frivolous or vexatious or is made in bad faith.

This safety valve should help to protect an archive from endemic problems, such as disgruntled ex-employees.

9. The Role of the Federal Court of Canada (ss. 14-17)

Unlike certain provincial and territorial privacy legislation, the federal Privacy Commissioner does not have regulatory power as such (although there is an intelligent inclination among those regulated to comply with his recommendations). The ultimate enforcement power in the Act lies with the Federal Court of Canada-Trial Division, at least in certain circumstances.

A complainant who has received the Commissioner's report, or the Commissioner himself, may bring a somewhat **limited number of issues** before the Federal Court, including information transferred to a third party for processing (4.1.3), a failure to identify the purposes for collecting information (4.2), the requirement for knowledge and consent for collection, use, or disclosure (4.3), a refusal of service based on refusal of a demand for excessive information (4.3.3), a failure to limit data collection to what is necessary for an organization's purposes (4.4), not limiting use, disclosure, and retention (4.5), a breach of the accuracy principle (4.6), a failure to maintain security safeguards (4.7), and failing to inform a person about the uses of his or her information and granting access to it (4.9) The Commissioner may also appear before the court on behalf of any complainant. The law instructs that an application "shall be heard and determined without delay and in a summary way," which at least indicates a desire for speedy justice. (s. 17)

It would be prudent for all archives to take steps to minimize a review by the Federal Court, since judges have considerable latitude in fashioning solutions. Privacy Commissioners generally do not have the same level of flexibility in interpreting their legislation (particularly on questions of jurisdiction), as do the courts. The Act specifies that the court may rely on the following remedies, "in addition to any other remedies it may give:"

- Order an organization to correct its practices in order to comply with sections 5 to 10;

- Order an organization to publish a notice of any action taken, or proposed to be taken, to correct its practices;

- "award damages to the complainant, including damages for any humiliation that the complainant has suffered."

The prospect of civil damages should encourage organizations covered by the Act to comply as fully as possible with its requirements. Again, I find it highly unlikely that an archive would allow itself to become embroiled in such judicial proceedings, not least because of the costs of legal representation in such circumstances. Archives should resolve issues around the application of fair information practices well short of the courtroom door.

10. The Privacy Commissioner's Auditing Powers (sections 18-19)

A power that the Privacy Commissioner, or his delegate, is highly likely to undertake with respect to an archive subject to data protection legislation is an audit of its "personal information management practices." The Commissioner is required to have "reasonable grounds" for non-compliance before taking such a step. I would strongly encourage all archives to invite the Commissioner, or his provincial or territorial counterparts, to undertake an informal review to ensure that requirements are being met, whether based on law or policy. If the Commissioner does not have "reasonable grounds" to believe that the organization is in non-compliance, he cannot invoke his audit power under these sections. However, he could discuss the statutory requirements with an archive on an informal basis.

In British Columbia, I exercised auditing powers in the form of site visits, which were essentially educational (for my staff and me) and consciousness-raising exercises for staff of organizations being visited.[94] Given my emphasis elsewhere in this guide and commentary on the need for mutual education of all concerned about the existence of fair information practices in archives, I would strongly encourage archives to familiarize official privacy protectors with their operations on an ongoing basis.

11. Miscellaneous Provisions (sections 20-29)

Archivists need only know that the Privacy Commissioner has various obligations and powers including confidentiality and a power of publicity, as he and his staff conduct their work. These will provide further inducements to archives to promote fair information practices and thus avoid entanglement in such monitoring activities by careful compliance with them. The Commissioner has plenty of power if he needs to exercise it against various kinds of suspected villainy. What would be surprising about these requirements would be if they did not exist in a statute of this kind.

The Act contains a very innovative provision in section 23(1) encouraging the Privacy Commissioner to **consult with the provinces** for particular purposes of promoting compliance with the goals of the Act. The Commissioner may decide to do so on his own initiative, or at the request of an interested person, who could be a complainant, a civil libertarian, a legislator, or a privacy advocate (among others). The statutory language is very explicit about promoting the important goal of harmonization of enforcement across the country, since the rationale in this section is to "ensure that personal information is protected in as consistent a manner as possible." It seems reasonably clear that the

---

[94] See David H. Flaherty, "How to do a privacy and freedom of information act site visit." This guide, which exists in various short versions, is available on request from the author: **David@Flaherty.com**

intent of this section is to encourage greater interprovincial and territorial cooperation than has been the case in the past among those charged with the protection of privacy, which includes Privacy Commissioners, Ombudsmen, and the Commission on Access to Information in Quebec. This can only be in the public interest in a country with such a vast territorial expanse as Canada and such limited public resources for data protection.

Archives, in particular, will want to have to deal with similar fair information practices in each province and territory in order to minimize any costs of doing business. They will also have a significant self-interest in making the official privacy protectors well aware of their ongoing activities in data collection, storage, and disclosure, even if there is no statutory requirement to do so. The Act instructs the Privacy Commissioner of Canada and those he consults with under this section "to develop model contracts for the protection of personal information that is collected, used or disclosed interprovincial or internationally." (s. 23[2][c]) Archivists will want to consider the adoption of similar **model contracts,** or at least donation or accession agreements, for collections of records that they acquire that would not otherwise be, or remain, covered by privacy legislation. Similarly, one of the educational and promotional roles of the Privacy Commissioner is to "encourage organizations to develop detailed policies and practices, including **organizational codes of practice**, to comply with sections 5 to 10." (Emphasis added; s. 24[c]) Archives will want to have comparable codes of practice in place for records that would otherwise be unprotected by law ("privacy limbo") with respect to fair information practices.

There is unusual protection in section 27 of the Act for **whistleblowers**, defined as "any person who has reasonable grounds to believe that a person has contravened or intends to contravene a provision" of sections 5 to 10 on the protection of personal information. Such persons may notify the Privacy Commissioner and ask that their identities be kept confidential.[95] More interestingly from an archival perspective, section 27.1(1) extends similar protections to "employees, acting in good faith and on the basis of reasonable belief," who disclose information to the Privacy Commissioner in the following circumstances:

- The employer or any other person has contravened or intends to contravene a provision of Division 1;

- The employee … has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1;

- The employee .. has done or stated an intention of doing anything that is required to be done in order that a provision of Division 1 not be contravened;

An archivist might be motivated to notify the Commissioner of a collection or disclosure of personal records from an archive that he or she believed was in violation of established fair information practices. The definition of employee also extends to independent contractors. (s. 27[3]) It is a criminal offence to contravene section 27.1(1), or to obstruct the Commissioner or his delegate "in the investigation of a complaint or in conducting an audit…." (s. 28)

---

[95] The whistleblowers' provision in the Alberta *Freedom of Information and Protection of Privacy Act* has been used several times (Information from Bob Clark, Information and Privacy Commissioner).

12. Transitional and Coming into Force Provisions (sections 30 and 72)

The Act will apply on January 1, 2001 to organizations that disclose personal information outside a province for consideration. While the intent of this provision is to cover the private sector as such, it could conceivably regulate that particular aspect of the work of an archive that involved in return a payment or a service. It is admittedly difficult to give a practical example, but archives of various sorts should be forewarned, because they do engage in limited commercial activities (as noted elsewhere in this guide and commentary). Any archive that exchanged mailing lists of donors across provincial boundaries might be caught by this provision as well.

But the more important general significance of the transitional provision in section 30 is that the Act will apply on January 1, 2004 "to any organization in respect of personal information that it collects, uses or discloses within a province," unless a province or territory acts to preempt federal jurisdiction over its private sector. The various provinces are already examining their options in this regard, whether a constitutional challenge to the scope of the Act (as is likely from Alberta), or a decision on provincial data protection legislation for the private sector (as is likely from the other larger provinces). Quebec is the only province likely to be exempted from the Act because of section 26(2)(b). Thus, archives not subject to the Act for whatever reason stand a strong prospect of being included in the broad sweep of equivalent provincial or territorial legislation for data protection in the private sector within four years.

13. Part 2 of the Act: Electronic Documents (sections 31-51)

The purpose of Part 2 is to provide for the use of electronic alternatives "where federal laws contemplate the use of paper to record or communicate information or transactions." (s. 32) The specific intent is to permit federal authorities to use "electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with documents or information[,] whenever a federal law does not specify the manner of doing so." (s. 33) This can include electronic payments to the government of Canada, the creation of electronic versions of statutory forms, and the filing or submitting of electronic documents with the government. (ss. 34-35)

From the perspective of the National Archives of Canada in particular, section 37 authorizes the retention of a federal document in electronic form, if it is maintained in an accessible and readable form "that does not change the information contained in the electronic document that was originally made, sent or received," and "any information that identifies the original and destination of the electronic document and the date and time when it was sent or received is also retained." The clear intent is to legitimate the electronic world of recordkeeping in a statutory world that had a "paper-bias."[96] Statutes and regulations that allow the use of an electronic alternative will be listed in Schedules 2 and 3 of the Act. (s. 38)

Section 39 of Part 2 authorizes a secure **electronic signature** as a substitute for a person's seal under specified circumstances, as a validation for an oath or affirmation (s. 44), and as a substitute for a witnessed signature (s. 46). A related provision sets out expectations for processes to ensure the

[96] Helpful general and specific explanations of why the federal government acted with respect to Parts 2 to 5 of the Act can be found in Michael Power, "Bill C-6: Federal Legislation in the Age of the Internet," Manitoba Law Journal, 26 (1999), 242-54. Power was the public servant intimately involved in the shaping of these Parts.

uniqueness of electronic signatures and the authentication of the user, including possible reliance on cryptography as one form of available technologies. (s. 48) This will occur on the basis of regulations issued by the Crown on the recommendation of the Treasury Board of Canada. The goal is to make it possible to use digital signature technology to prove who signed an electronic document. In this connection, the federal government already has a Task Force implementing the Government of Canada's Public Key Infrastructure (PKI), which relies on public key cryptography.

Part 2 of the Act is permissive and not prescriptive. It puts electronic and paper media on the same footing. Ministers, federal departments, agencies, and boards have the option of bringing the laws for which they are responsible under the purview of these provisions and also deciding when and by what means to offer services electronically to the public. Industry Canada, the Department of Justice, and the Treasury Board have various responsibilities and roles in this regard. The Association of Canadian Archivists and the Canadian Historical Association protested in vain against this laissez-faire approach, since it could result in multiple methods of creating electronic records and digital signatures, creating a potential nightmare for the archival preservation of electronic records that are of enduring value in a useable format. Encrypted information, to give a prime example, must be decoded at some point; otherwise, it will be unreadable.[97]

In its submission on the draft legislation, the Association of Canadian Archivists was "delighted" by the "heightened focus" on electronic records in Part 2, since it "properly underlines the growing primacy of electronic records as the recording medium of choice (and necessity) in government and business for many of their transactions." The Association also welcomed the emphasis on establishing the reliability of electronic documents as evidence for commercial and legal purposes (s. 36) and the accompanying requirements for record retention and documentation (s. 37).[98]

14. Parts 3 to 5 of the Act: Amendments to the Canada Evidence Act, the Statutory Instruments Act, and the Statute Revision Act

Part 3 of the Act consists of detailed amendments to the *Canada Evidence Act* to permit the use of electronic documents in court and their authentication as reliable, including such matters as:

- The authentication of electronic documents
- Satisfying the best evidence rule[99]
- Establishing the integrity and reliability of an electronic documents system and an electronic document
- Evidentiary presumptions with respect to secure electronic signatures

---

[97] Canadian Historical Association, "Seeking a Balance," pp. 3-4.

[98] Association of Canadian Archivists, "Brief to Parliament on Bill C-54."

[99] This incorporates the Uniform Law Conference of Canada's Electronic Evidence Act (1998). See Power, "Bill C-6," Manitoba Law Journal 26 (1999), 249-51.

- The ability of the courts to recognize various standards of electronic record-keeping

A clear goal of Part 3 is to offer a degree of certainty to persons who create and rely on computer-generated records in judicial proceedings rather than having to produce original paper records.

Part 4 of the Act consists of amendments to the *Statutory Instruments Act* to acknowledge that notices and acts published electronically by the Queen's Printer, especially the *Canada Gazette*, have the same legal force as their paper equivalents.

Part 5 of the Act gives official status to the electronic version of the Consolidated Statutes and Regulations of Canada by amending the *Statute Revision Act (R.S.C. 1985, c. S-20)*, which now becomes the *Legislation Revision and Consolidation Act*. The available electronic consolidation is unofficial. It will take some time to achieve the goal of on-line access to an official electronic consolidation of statutes and regulations as opposed to the unofficial versions that are currently available from the Department of Justice.[100]

In the case of both Parts 4 and 5, the original statute or regulation prevails in case of a discrepancy or inconsistency between the electronic and paper versions.

15. The Application in Practice of Part 1 of the Act to Archives: some final issues

The Transfer of Private Sector Records to Archives

A private sector organization that is subject to the Act should not be able to transfer records to any archives, if such records will be exempt from the fair information principles and practices that they enjoyed while in the custody and control of the organization. Such companies should ensure that their personal records are located in an external archive that can provide equivalent or adequate privacy protection. In my opinion, such organizations should use contractual or other means to provide a comparable level of protection once such information is held in an archive. The latter, for their part, should insist on such practices in accession agreements and thereby ensure that the various stated goals of archives are satisfied.

Thus it is inappropriate, in my view, for the National Archives to take any solace from the fact that it is not subject to the Act in the technical sense, since data protectors could wisely insist that private sector records should not be transferred to it for permanent storage, if the effect would be that the privacy protections available under the Act were in fact lost. In fact, the Association des archivistes du Quebec specifically argued "that private archival holdings given to the National Archives of Canada for archival or historic purposes must enjoy the same protection as federal government archives. In order to avoid any ambiguity in this regard, our association recommends that the National Archives of Canada be explicitly subject to Bill C-54. At the moment, it is difficult to tell what the drafters' original intentions are, and this creates a significant legal vacuum."[101] Parliament did not make the requested change, (as it did not make most of the changes recommended to it) but that does not

---

[100] See Power, "Bill C-6," Manitoba Law Journal 26 (1999), 253-54.

[101] Standing Committee on Industry, Hearings on Bill C-54, February 18, 1999.

mitigate the force of this recommendation with respect to how private sector records should be treated. For this purpose, the National Archives of Canada should request that the Department of Justice amend the *Privacy Act* for the particular purpose of legally ensuring that all personal records it holds are properly protected through fair information practices.

As noted above, acquisition or donation agreements and contracts should regulate transfers of private sector records to any archive, and the exercise of control over the use and disclosure of the records themselves, if the archive in question does not come under the protective umbrella of the Act. Ultimately, an organization subject to the Act has, in my opinion, obligations under Schedule 1 that include identifying personal information in its records that has archival value and ensuring, in an ideal situation, that its own moral and legal responsibilities are transferred to an archive in an appropriate manner, such as by contractual terms or other means. Alternatively, such an organization should maintain its own archive, as some large companies do, which would mean that the protective requirements of the Act are kept in place.

Principle 4.1.3 of Schedule 1 imposes responsibility on an organization subject to the Bill for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization is required to use contractual or other means to provide a comparable level of protection while the information is being "processed" by a third party. By analogy, such duties could cover transfers of records to an external archive as well. However, from a strict legal perspective, it is doubtful that the term "processing" would encompass the permanent transfer of records to a public archive. While organizations subject to the Act should, ideally, not be able to escape from fair information practices by permanently transferring their records to an archive, the working of Schedule 1 and the Bill itself falls short of imposing this responsibility to ensure such duties cover the transfer of records to an external archive.

Section 7(3)(g) authorizes disclosure of personal information to an archive, without the knowledge or consent of the individual, but there is no implication that such information thereby loses all statutory protections, including the oversight of such practices by the Privacy Commissioner of Canada. Organizations subject to the Act should not consider transferring their personal information to archives that do not intend to follow the spirit and letter of the Act, and all archives, regardless of whether they are subject to the Bill, should apply the standards of the Act to the personal information that they hold that is not already covered by data protection legislation. While I fully appreciate that all archives are overburdened at present, like most other public institutions, they risk become marginalised, if they do not deal satisfactorily with the aspects of their ongoing work that should be protective of the privacy interests of individuals whose records are in their collections.

I recognize the related problem for archives that some personal information in their holdings was acquired, used, and managed by an organization (as defined in s. 2[1] of the Act) before it was transferred to the archives. The archival obligation, I would argue, is to ensure that an organization has a legitimate right to transfer personal information for archival purposes, and then for the archive to ensure that the personal information continues to receive an adequate level of data protection in accordance with the Act and progressive archival practices, such as those of the National Archives of Canada and the various provincial archives.[102] From a strict legal perspective, of course, it is far from clear that an archive has the responsibility to ensure that an organization has a legitimate right to transfer personal information to the archive – that is the legal responsibility of the organization itself. However, archives should be in an ideal position to clarify such legal rights as part of their

[102] The *National Archives of Canada Act* (1987), c. 1 does not provide detailed guidance on data protection principles and practices.

consideration of potential archival material. Archives should also ensure that, once transferred, personal information receives an adequate level of data protection, although it need not meet the standard set out in the Act, if that Act is not going to apply. The latter point illustrates the difference between a legal and a moral obligation.

The problem in archival settings is that personal information in its holdings was acquired, used, and managed by someone else before it was transferred to the archives. The essential consideration is that the **chain of accountability** for such information should not be broken just because the custody and control of the personal information has changed from the organization to an archive. In fact, the donation agreement should ensure that this chain of accountability is not broken with respect to compliance with fair information practices and that, in fact, the protective web is seamless.

Self-Regulation by Archives for Data Protection

Depending on its legal status, an archives covered by existing privacy legislation (federal, provincial, or territorial), or the Act, may simply choose to indicate to interested parties by notices on signs and forms that it acts in compliance with the specific law. It would be prudent for an archive that is not subject to such a data protection law, more especially one that holds records that are not covered by such a data protection law, to develop its own **privacy code** on the basis of the CSA Code as laid out in Schedule 1 of the Act. The CSA Code can easily be used as a basic **template** for such purposes. A customized privacy code for any archives could acknowledge the special nature of personal information collection, use, and disclosure in an archival setting. Archives that are not subject to data protection laws would thus be voluntarily subscribing to appropriate fair information practices as a matter of policy and not law. Fair information practices can also exist in the form of internally developed and approved mandates, objectives, internal policies and procedures at archives.[103] That is a way to seek to avoid privacy and data protection problems of any sort.

[103] Over time, as major archives in particular develop even more experience with the application of fair information practices to personal information in records in their custody and control, it would be highly desirable for the reasons for decisions on access, or refusal of access, to records be written out and made available to others, so that a "jurisprudence" on applied fair information practices for archival records can take concrete shape and be subject to national debate as required.

Acknowledgments: A particular pleasure of undertaking research and writing of this type is the satisfaction of learning from, and interacting with, very competent and accomplished persons from across this country. Without making them in any way responsible for the final product, I want especially to thank Peter Bower, the Executive Director, Access and Privacy, for the Manitoba Ombudsman; Patrick Burden, Strategic Planning and Policy Coordination, National Archives of Canada; Heather Black, Department of Justice; Mac Culham, Manager, Information and Privacy, BC Archives; Gordon Dodds, the Manitoba Provincial Archivist; Ian Forsyth, the Archivist for Simon Fraser University; Sarah Gawman, Access and Privacy Division, National Archives of Canada; Gary Mitchell, BC Provincial Archivist; Jane Nokes, Scotiabank Archives; Chris Norman, Director, Information and Data Management Branch, BC Information, Science and Technology Agency; Stephanie Perrin, Chief Privacy Officer, Zeroknowledge, and formerly of Industry Canada; Sandra Thomson, Alberta Provincial Archivist; Anne Rooke, Gerry Neary, and their colleagues at the Office of the Privacy Commissioner of Canada; and various staff of the National Archives of Canada who commented anonymously on an earlier draft. Those who know any of these valued contributors to my work will be aware of how unlikely they are to agree with everything that I have written.

Appendix 1:

DAVID H. FLAHERTY

David Flaherty is a specialist in the management of *privacy and information policy* issues. Most recently, he served a six-year, non-renewable term as the first *Information and Privacy Commissioner for the Province of British Columbia* (1993-99). He built an office of 25 staff with an enviable record for successful mediation of almost all access to information disputes. Flaherty wrote 320 Orders under the *Freedom of Information and Protection of Privacy Act*. He also pioneered the development of site visits to public bodies (hospitals in particular) as a form of auditing for compliance with fair information practices. His decisions and the annual reports of his former office are available at **www.oipcbc.org**.

Flaherty began his involvement with privacy issues as an assistant to Alan F. Westin at Columbia University in 1964. Flaherty's first book was **Privacy in Colonial New England** (1972). In 1974 he began to do comparative public policy work in Europe and North America that led to a series of books, including **Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States** (1989). His most recent publications are "Visions of Privacy: Past, Present, and Future," in C.J. Bennett and R. Grant, eds., Visions of Privacy: Policy Choices for the Digital Age (University of Toronto Press, 1999); and "Controlling Surveillance," in P. Agre and M. Rotenberg, eds., Technology and Privacy: The New Landscape (MIT Press, 1997). Flaherty has written and edited thirteen books. He has testified regularly in the US Congress and before the Parliament of Canada.

Flaherty is an Honours graduate of McGill University (1962) and has an MA and Ph.D. from Columbia University. His teaching career from 1965 to 1993 included Princeton University, the University of Virginia, and the University of Western Ontario, where he was professor of history and law from 1972 and from which he is now a professor emeritus. He was the first director (1984-89) of its Centre for American Studies. He has held fellowships and scholarships at Harvard, Oxford, Stanford, and Georgetown Universities. In 1992-93 Flaherty was a Fellow of the Woodrow Wilson International Center for Scholars in Washington, DC and a Canada-US. Fulbright Scholar in Law. He is currently an Adjunct professor in political science at the University of Victoria.

In the fall of 1999 Flaherty served as a Special Advisor to the Deputy Minister of Industry Canada in support of Bill C-6, the federal *Personal Information Protection Act*.

Additional details of Flaherty's career can be found in the Canadian Who's Who, or from **David@Flaherty.com**, 1939 Mayfair Drive, Victoria, BC V8P 1R1 (250-595-8897).