Access to personal information: British and Canadian legislative approaches

*Tom Onyshko**

I. INTRODUCTION

A. Computers and the information revolution

We live in an age that places increasing emphasis on information. The proliferation of computers and affordable systems for storing large amounts of data has allowed government and the private sector to collect more information about individuals than ever before.

The computer has made it possible to save huge amounts of information, to retrieve information almost instantaneously, and to manipulate information in ways that were previously impossible. Computer systems exist today which could store a twenty page file on every person in the United States, then find and retrieve one file in a maxi-

* LL.B. Mr. Onyshko is currently articling with the firm Wilder, Wilder & Langtry. The author wishes to acknowledge the helpful comments of Professor Philip Osborne, Faculty of Law, University of Manitoba.

mum of four minutes.[1] But not only has the storage and manipulation of information been improved; modern technology also allows the easy transfer of large amounts of information over the telephone lines.

The new technology has a great potential impact on the privacy of the individual. Computer technology encourages extensive record-keeping, the centralization of records, and the transfer of information between record-keepers; all these trends are producing an environment in which the violation of the individual's privacy is more likely.[2] As Murray Rankin points out: "[I]n the past, the major protection of the individual's privacy was the difficulty of access to large masses of data, stored in a variety of ways."[3] While, in the past, time and effort was required to physically assemble a dossier which contained information from a variety of sources, today such a dossier can be compiled easily by computer searches that "cross-match" information from different data bases. "As more and more transactions are carried out through computers and more and more information is recorded on computers, the potential for invasion of privacy by matching records in different data bases increases," C. Ian Kyer writes.[4]

B. The importance of personal information

"We'd like to know a little bit about you for our files...."[5]

Personal information is information about an individual's characteristics and attributes. It can consist of facts: information about an individual's race, religion, marital status, health record, employment history or personal opinions or beliefs. It can also include other people's opinions about an individual – for example, an assessment of an individual's character made by his former employer.

The focus of this paper will be Canada's federal *Privacy Act*[6] and Britain's *Data Protection Act*[7], laws which give individuals access to their personal information held in computer data bases. (Access to information laws existing in the Canadian provinces are beyond the

---

1 M. Rankin, "Privacy and Technology: A Canadian Perspective," (1984) 22 Alta L. Rev. 323 at 329.

2 Canada, Department of Communications and Department of Justice, *Privacy and Computers* (Ottawa: Information Canada, 1972) at 91.

3 *Supra*, note 1.

4 C. Ian Kyer, "The federal Privacy Act," (1985) 2 Canadian Computer Law Reporter 189 at 189-190.

5 Simon and Garfunkel, "Mrs. Robinson," (1968).

6 S.C. 1980-81-82-83, c. 111, Schedule II.

7 1984 c. 35. Volume 8, Halsbury's Statutes of England, 4th ed. (London: Butterworths, 1987) 831.

scope of this paper.) Before I go any further, it may be a good idea to discuss just why we should worry about personal information in the first place.

There are two main reasons why personal information is important; the first is based on philosophical argument while the second is based on practical considerations. The first reason concerns the concept of "informational privacy" or an individual's right to control information about himself. Theorists argue that as others accumulate information about us, our ability to withhold information is eroded and our security is threatened.[8] Charles Fried contends that the ability to control information about ourselves is at the core of our personal liberty, a necessary prerequisite for "love, trust, friendship, and self-respect".[9] Speaking at a conference on privacy and computers in 1970, then federal Minister of Justice John Turner said:

> The erosion of privacy is the beginning of the end of freedom. Privacy is the foundation of the principle of autonomy at the core of human dignity. The right to privacy not only goes to the core of our being as individuals but also the core of our identity as a society or state.[10]

While informational privacy might seem an abstract concept, it can be illustrated in more practical terms. For most people, there are certain facts about themselves which they consider sensitive and do not wish to be generally known. For example, I might disclose information about my salary in order to get assistance from Legal Aid, or share information about my health with a doctor in order to be cured of a disease, but I would be justly angered should that information be released to the public.

Similarly, most people are shocked by newspaper stories about the careless disposal of personal information, like this one:

> Hundreds of confidential applications for Christmas Cheer Board applications were blowing in the wind Friday night after they were tossed into a garbage bin by provincial welfare staff.
>
> One passer-by said the yellow documents blanketed the sky at Portage Avenue and Arlington Street shortly after 8 p.m. Friday.
>
> "I was going for coffee and I looked up and the sky was full of them," Gerald Brandt said. "I couldn't believe that kind of stuff was just blowing around outside."

---

8 *Supra*, note 1 at 326. *[Murray Rankin]*

9 *Ibid.*, at 327.

10 *Department of Communications*, Telecommunications Study 5(b), Conference Report, Computers: Privacy and Freedom of Information (Ottawa: 1970) at 16. [as cited in R.A. Reiter, "The Legal Protection of Personal Information in the Context of Videotex: A Preliminary Inquiry" (1986) 2 Intellectual Property J. 273 at 277.]

> The forms identified Cheer Board recipients by name, address, telephone number, names and ages of children and where they went to school.[11]

Just as we abhor the invasion of a individual's physical privacy (by wiretap or camera surveillance, for example) so too should we abhor the violation of an individual's informational privacy. As personal information is a reflection of ourselves, it seems just that we have some control over it.

The second reason for the importance of personal information concerns the significance our society attaches to personal information. Personal information is used by others to make decisions directly affecting us: to assess our need for government assistance, to hire and fire us, to decide whether or not to extend us credit. Often, the people actually making decisions will never meet us face-to-face; instead they will rely solely on their records of our personal information. Thus personal information is important because it may determine how we are treated – whether or not we will receive certain benefits or penalties. The U.S. Privacy Protection Study Commission made the point well when it concluded in its 1977 report:

> The substitution of records for face-to-face contact in these relationships is what makes the situation today dramatically different from the way it was even as recently as thirty years ago. It is now commonplace for an individual to be asked to divulge information about himself for use by unseen strangers who make decisions about him that affect his everyday life. Organizations must have some substitute for personal evaluation in order to distinguish between one individual and the next in the endless stream of otherwise anonymous individuals they deal with, and most organizations have come to rely on records as that substitute.[12]

C. What should an ideal system of legislation include?

At this point I will discuss my views on what model legislation on personal information should include. Considering the importance of personal information, I contend that, at a minimum, individuals should have quick and easy access to the personal information held by government and private sector agencies.[13] They should have the right to see their personal information and the right to request that information be corrected where it is inaccurate.

---

11 "Confidential papers blow from welfare office trash," *The Winnipeg Free Press*, 22 January 1989, at 1.

12 Privacy Protection Commission, *Personal Privacy in an Informational Society* (Washington, D.C.: U.S. Government Publications Office, 1977) at 4-5. *[As cited in Murray Rankin at 329]*

13 Note that in this paper, "agency" will be used as a generic term for all government and private sector institutions which gather, store or use personal information.

To ensure as much informational privacy as possible, model legislation should also regulate the collection and use of personal information. Information should not be collected unless needed, and certain types of information (for example, information on religious, personal or political beliefs) should not be collected at all, unless there are compelling reasons to do so. The means by which information is collected should not be covert or intrusive. When the information is being collected, the individual should be informed of the intended use of the information. And the use of personal information should be limited: information gathered for one specific purpose should not be used for another, and information from a variety of sources should not be combined to create comprehensive dossiers on individuals.

Further measures should be taken to help individuals gain access to their personal information. Legislation should establish a government-run privacy organization responsible for keeping track of where personal information is stored, helping individuals gain access to their personal information, educating the public about privacy concerns, and enforcing standards on the collection and use of personal information. As well, agencies that gather personal information should have a duty to assist individuals gain access to it. Confronted with an agency's unfamiliar system of organization (which may involve several data banks each containing different items of personal information), the individual is not the party best situated to determine where his information will be found. Instead, the individual should be able to make a "blanket request" for all the personal information that a particular agency holds on him; it would then be up to the agency to find all the relevant information.

There would be two mechanisms to enforce personal information standards. The government privacy organization described above would have the power to investigate the complaints of individuals and enforce the legislation against intransigent data-gathering agencies. However, as government agencies will often be the cause of complaints, enforcement of personal information standards would not be left solely in the hands of a government organization. Model legislation would also create a civil cause of action allowing individuals to personally sue agencies which misuse personal information or store inaccurate personal information. Strict liability would be imposed on data-gathering agencies sued in such actions.

To understand why model legislation should impose strict liability in these civil actions, consider the rationale behind the American principle of strict liability for the manufacturers of defective consumer products. As John J. Fleming writes on the American principle:

> The consumer is singularly dependent on the manufacturer for safety, ill-equipped to make an informed choice whether to incur the risks of the product and handicapped in proving fault. The manufacturer, on the other hand, is a convenient conduit for spreading the accident cost among consumers of the product who, in reality, thus buy compulsory insurance for themselves.[14]

The point to be stressed here is the inequality of the positions of the individual and the agency which stores personal information. The individual is often given no option but to divulge personal information in order to gain some benefit or avoid some penalty. The individual may not even be aware that he is being exposed to a risk where, for example, information collected from him by one agency is later transferred to another or information collected for one purpose is later used for another purpose. In general, the agency will have greater financial resources, as well as a complex administrative structure and a potentially hostile bureaucracy which may make it difficult for the individual to learn the full extent of the agency's actions. Finally, the subject matter involved here is intimately related to the individual: personal information is an extension of the individual himself, and the misuse of such information may affect not only his pecuniary interests but also his informational privacy.

Given these concerns, agencies should be strictly liable for the misuse of personal information or the storage of inaccurate personal information, with one defence.[15] The sole defence available would be that the agency had followed all the requirements of the model data protection legislation and, in the case of inaccuracy of personal information, had also taken reasonable efforts to ensure the accuracy of the information. "Reasonable efforts" would be defined so that it required some degree of active investigation by the data keeping agency; an agency which accepted personal information from a third party and relied passively on assurances that the information was correct would face the risk of liability should the information be inaccurate.

In addition to imposing strict liability, legislation should presume a minimum level of damages against data-gathering agencies sued in civil actions, even where no actual harm can be shown. There are two reasons for presuming damages. First, there is a good argument that the misuse of personal information automatically harms the "informational privacy" of an individual, even if the harm involved

---

14 J. Fleming, *The Law of Torts*, 7th ed. (Sydney: The Law Book Co., 1987) at 307.

15 In essence, I propose a modified form of strict liability which eliminates a number of defenses usually available. For example, an Act of God or the intervention of a third party would usually be available as defenses in a strict liability action. However, I believe that personal information should be stored in such a way that it is not vulnerable to these problems; accordingly, I would not permit these defenses.

cannot be quantified. Professor Edward J. Bloustein's comments on the American tort of intrusion of privacy might apply here:

> An intrusion on our privacy threatens our liberty to do as we will, just as an assault, a battery or imprisonment of our person does.... Unlike many other torts, the harm caused is not one which may be made good by an award of damages. The injury is to our individuality, to our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered.[16]

Second, even when actual damage has occurred, the individual may find it impossible to prove that the agency's action caused the damage. To begin with, the individual will often find it impossible to learn who had access to his personal information because the individual must rely on the organization being attacked to disclose its internal records or procedures. Moreover, the individual must then prove that one of the people who had access to the personal information acted on it to the individual's detriment; showing a causal connection between a person's knowledge of information and one of the person's actions can often be extremely difficult.

The case of *Gillett* v. *Nissen Volkswagen Ltd.*[17] illustrates some of the problems involved in proving damages. The facts of the case were as follows: Gillett was the sales manager of Nissen Volkswagen for several years but resigned from the position in 1967. Four years later, Gillett applied for the position of regional sales manager of Datsun Canada; a few weeks after the application, a representative of the company told Gillett that they had received an unsatisfactory credit report about him, and that the negative information had come from Nissen, Gillett's former employer. The information supplied by Nissen (which alleged that Gillett had been "let go" for dishonesty) was completely false; Gillett contacted Nissen and had him correct the inaccurate information. However, three weeks later, Datsun informed Gillett that the position had been filled. Gillett took Nissen and the credit reporting company to court for defamation, arguing that the damages should compensate him for the loss of opportunity of employment.

The court held Nissen and the credit company liable for defamation, but in assessing damages it denied the claim for loss of opportunity of employment. Gillett had been able to show that Datsun had narrowed its list of applicants to two candidates (with Gillett first) when

16 E.J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," (1969) 39 N.Y. Law Rev. 962 at 1002-1003. [as cited in: G.R. Segal, "The Threat From Within: Cable Television and the Invasion of Privacy" (1985-86) 7 Computer L. J. 89 at 116]

17 (1976), 58 D.L.R. (3d) 104 (Alta. Q.B.).

two things happened: the negative credit report arrived and Datsun learned of another man who was interested in the job. Datsun hired the new man a week later, based solely on his superior experience. Gillett argued that had it not been for the adverse credit report he would have been hired before the new candidate entered the picture. However, the court held that the "evidence on this point was not clear".[18]

By presuming a certain level of presumed damages, an ideal access to information law would ensure that organizations which store inaccurate information do not escape punishment simply because no damage can be shown. The threat of such liability should make organizations take extra care in gathering, storing, and using information.

Now that I have expressed my views on what an ideal system of laws should include, I turn my attention to the existing laws which provide for access to personal information. I begin with an examination of Canada's federal *Privacy Act*, then consider the British *Data Protection Act*. I conclude with a discussion which compares and contrasts the Canadian and British laws, and evaluates them with reference to the model legislation discussed above.

II. CANADIAN LEGISLATION ON ACCESS TO PERSONAL INFORMATION

THE CANADIAN APPROACH to access to personal information is complicated by the fact that we have a federalist system. Competence to make laws concerning access to personal information is split between the federal Parliament and provincial legislatures, depending on the subject area that the law involves.

The provincial governments of Manitoba, New Brunswick, Newfoundland, Nova Scotia, Ontario, and Quebec have enacted access to information laws which give people rights of access to personal information held by these provincial governments.[19] However, these

---

18 *Ibid.*, at 118. Note that although Gillett was denied damages for loss of opportunity of employment, he did receive general damages for pain and suffering and punitive damages against both Nissen and the credit reporting agency.

19 See: *Freedom of Information Act*, S.M. 1985-86, c. 6; *Right to Information Act*, R.S.N.B. 1987, c. R-10.3; *Freedom of Information Act*, S.N. 1981, c. 5; *Freedom of Information Act*, S.N.S. 1977, c. 10; *Freedom of Information and Protection of Privacy Act*, S.O. 1987, c. 25; *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, R.S.Q. A-2.1. All these statutes apply exclusively to the particular provincial government's records, leaving the private sector unregulated.

Although passed in 1985, the Manitoba Act did not come into force until September 30, 1988. Those interested in the Act should see: *Access Guide* (Winnipeg: Queen's

provincial laws are beyond the scope of this paper, and will not be considered here. My primary area of interest is the federal legislation.

A. The federal *Privacy Act*

The federal *Privacy Act*[20] governs access to personal information held in data banks (computerized or otherwise) belonging to the federal government. Unfortunately, the Act does not apply to any part of the private sector, although a report of a Parliamentary committee made in March of 1987 suggests that its coverage should be extended.[21] While this restriction of coverage is a glaring shortcoming, one must also remember that the federal government has probably become the largest single collector of personal information in Canada. As Nanci-Jean Waugh writes:

> The wide scope of federal responsibilities requires an intrusive federal involvement in previously private activities. For example, to enforce the *Income Tax Act*, Revenue Canada must obtain information about the individual tax payer's sources of income and charitable contributions; to enforce immigration and welfare laws, the Departments of Health and Welfare and Employment and Immigration must demand personal information about the particular individual's employment, sources of income, or other financial means of support; federal economic surveys necessitate knowledge of consumer spending plans and capabilities; and the enforcement of safety, banking, and housing laws compels individuals and corporations to provide formerly secret managerial information to federal agents.[22]

Passed in 1983 as a companion to the *Access to Information Act*[23] (which gives citizens rights of access to government information), the *Privacy Act* sets out procedures allowing individuals to gain access to their personal information held in federal government data banks and to correct information that is inaccurate. It also regulates the federal government's collection and disclosure of personal information, and establishes the position of "Privacy Commissioner" to investigate complaints made under the Act.

The *Privacy Act* replaces Part IV of the *Canadian Human Rights Act* which also gave individuals rights of access to personal informa-

---

Printer, 1988) and *Freedom of Information* (Winnipeg: Law Society of Manitoba, 1985). See also the *Personal Investigations Act*, C.C.S.M. P-33, which gives the subjects of reports prepared by consumer reporting agencies certain rights of access.

20 *Supra*, note 6.

21 Standing Committee on Justice, *Open and Shut: Enhancing the Right to Know and the Right to Privacy* (Ottawa: Queen's Printer, 1987) at 74-77.

22 Nanci-Jean Waugh, "A Critique of the *Privacy Act*," in *Canada's New Access Laws: Public and personal access to governmental documents*, ed. by D. C. Rowat (Ottawa: Carleton University, Dept. of Political Science, 1983) at 45.

23 S.C. 1980-81-82-83, c. 111, Schedule I.

tion.[24] The new Act broadens the definition of personal information and extends the review process by giving individuals the right of appeal to a court on refusals to release information. For the first time, the Act sets out conditions governing the disclosure of personal information to third parties (that is, parties other than the individual and the government institution which collected the information).

The Act defines "personal information" broadly as "information about an identifiable individual that is recorded in any form".[25] The definition sets out a list of ten examples, including: information relating to the race, national or ethnic origin, colour, religion, age or marital status of an individual; information about the education, medical, criminal, or employment history of an individual; the personal opinions or views of an individual; the views or opinions of others about an individual. However, the definition specifically exempts certain types of information, including information about the responsibilities and salaries of civil servants and information about individuals dead for more than twenty years.

A personal information bank is defined simply as "a collection or grouping of personal information".[26] This broad definition makes no distinction between manual or automated files, thus avoiding one of the failures of the British *Data Protection Act*.

B. Substantive provisions of the Act:

1. Rights of individuals

The *Privacy Act* gives Canadian citizens and permanent residents rights of access to their personal information in government data banks. An individual who gains access to his personal information under the Act can also request a correction of any information that they feel is inaccurate or incomplete.[27] Should such a request be denied, the individual has a right to require that a notation be attached to the file, describing the correction requested; the individual also has the right to require that this notation be sent to any person who used the file in the last two years.[28]

To exercise the right of access an individual must follow a certain procedure set out in the Act.[29] First, the individual must make a request in writing to the administrator of a particular institution's data

24 *Supra*, note 1 at 336-338.
25 *Supra*, note 6, s. 3.
26 *Ibid.*
27 *Ibid.*, s. 12(2)(a).
28 *Ibid.*, ss. 12(2)(b) and 12(2)(c).
29 *Ibid.*, s. 12.

banks.[30] The request must either specify the data bank that the individual believes contains the relevant personal information, or "provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution."[31] In the period from 1983 to 1986, over 76,000 requests for access to personal information were made.[32]

To decide which bank likely contains the information of interest, an individual can consult the government's index of personal information banks. The government is obliged to compile and publish such an index annually.[33] As thick as a telephone book, the 1987 edition lists over 2,200 government data banks by institution and includes a brief summary of the purpose and contents of each bank.[34] The index and copies of the official "Personal Information Request Form" are available at public libraries and some post offices.

Once an individual has made the request for access, the administrator of the data bank must respond within thirty days of its receipt.[35] The administrator must allow access to the individual's personal information, or deny access on the basis of one of the exemptions set out in the Act. If access is allowed, provisions in the regulations permit the administrator to charge a fee; the average fee charged is $12.00.[36] If access is denied, the administrator need not disclose whether the individual's information is held in the data bank; however, the administrator must cite the particular exemptions which would prevent access, assuming the information existed.[37]

If denied access, the individual can complain to the Privacy Commissioner who will investigate the complaint and determine if access was lawfully denied. In 1986-87, the Privacy Commissioner investigated 256 complaints involving denial of access; about one fifth of the complaints were found to be justified.[38]

---

30 *Ibid.*, s. 13.

31 *Ibid.*

32 R. de Cotret, "Statement by the President of the Treasury Board," Access to Information Act and Privacy Act Bulletin (No. 6, November 1986) 1 at 3. The vast majority of the requests were made to five government institutions: the Department of National Defence, the Canadian Penitentiary Service, the Public Archives, the Royal Canadian Mounted Police, and the Department of Employment and Immigration.

33 *Supra*, note 6, s. 11.

34 *Personal Information Index* (Ottawa: Supply and Services Canada, 1987).

35 *Supra*, note 6, s. 14.

36 *Supra*, note 32. While the average fee is $12.00, the average cost of processing a request for personal information is $1100.00.

37 *Supra*, note 6, s. 16.

38 J. W. Grace, *Annual Report, Privacy Commissioner, 1986-87* (Ottawa: Supply and Services Canada, 1987) at 42. In 1985-86 the Privacy Commissioner investigated 185

Should the Privacy Commissioner confirm the administrator's decision to deny access, the individual can appeal his decision to the Federal Court, Trial Division.[39] In a hearing in the Federal Court, the government bears the burden of establishing that the access to the information was properly denied.[40] The court has the power to examine any information except Cabinet documents and it can review information from an "exempt bank".[41] The Act provides that an application for court review will "be heard and determined in a summary way" in accordance with special rules under the *Federal Court Act*.[42] However, when access is denied on the basis of particular exemptions, the procedure involved is more elaborate; the hearing will be held *in camera*, the government institution which holds the information can require that the hearing be held in Ottawa, and counsel for the government institution must be permitted to make *ex parte* submissions.[43]

2. Directives on personal information

The *Privacy Act* requires government institutions to follow certain directives concerning the collection, retention, and disclosure of personal information. However, these directives cannot be enforced by individuals; instead, their enforcement is the job of the Privacy Commissioner and the Treasury Board of Canada. (The powers and functions of the Privacy Commissioner and the Treasury Board will be discussed in more detail, below.) Five directives regarding personal information are contained in sections 4 to 8 of the Act.

The Act's first two directives concern the collection of personal information. A government institution is prohibited from collecting personal information unless it "relates directly to an operating program or activity of the institution."[44] Unfortunately, this is the extent to which the Act regulates what information may or may not be col-

---

complaints and found about one third of them to be justified. See: J. W. Grace, *Annual Report, Privacy Commissioner, 1985-86* (Ottawa: Supply and Services Canada, 1986) at 35.

39 *Supra*, note 6, s. 41.

40 *Ibid.*, s. 47.

41 *Ibid.*, s. 45. On the subject of reviewing information from exempt banks, see my discussion of exemptions to the *Privacy Act*, *infra*.

42 *Ibid.*, s. 44.

43 *Ibid.*, s. 51. Section 51 applies when an individual makes an application to the Federal Court after being denied access on the basis the exemptions set out in s. 19(1)(a) and (b) or s. 21. For a case which involved s. 51 procedures, see: *Robertson* v. *Minister of Employment and Immigration* (1987) 13 F.T.R. 119. The judge there notes that he permitted counsel for the person applying for access to read the disputed document on an undertaking that he not divulge the contents to his client.

44 *Ibid.*, s. 4.

lected; considering the broad range of activities and programs of government, the provision hardly seems much of a limit at all. The Act also sets out some guidelines on *how* information is to be collected: it holds that a government institution shall, "wherever possible", collect personal information directly from the individual, and that the institution shall inform the individual of the purpose for which the information is being collected.[45] However, the institution need not follow these guidelines where they might result in the collection of inaccurate information or "defeat the purpose or prejudice the use for which information is collected".[46]

The Act's next two directives concern the retention and use of personal information. Government institutions are required to take "all reasonable efforts" to ensure that personal information is accurate, complete, and up-to-date.[47] The Act also puts limits on the use of personal information. It states that:

> Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under section 8(2).[48]

Thus, the Act provides some measure of control over "cross-matching", the compiling of information from various data banks, since it generally prohibits the use of information for a purpose unrelated to the purpose for which information was obtained. However, it does not prohibit government institutions from transferring information among themselves, as long as the information is used for a purpose "consistent" with the original purpose for collection, or for one of the purposes set out in section 8(2). Unfortunately, as we will see, section 8(2) allows the transfer of information for some questionable purposes.

The Act's final directive governs the disclosure of personal information to third parties (that is, parties other than the individual and the institution); section 8(2) of the Act sets out thirteen instances in which information may be released.[49] The section permits information to be released: for the purpose for which the information was obtained, or a consistent purpose; to meet a requirement included in any federal statute or regulation; to comply with a subpoena or warrant; and, for research or statistical purposes, should the researcher undertake that

45 *Ibid.*, s. 5(1) and 5(2).
46 *Ibid.*, s. 5(3).
47 *Ibid.*, s. 6.
48 *Ibid.*, s. 7.
49 *Ibid.*, s. 8(2)(a)-(l).

the information will not be released in a form "that could reasonably be expected to identify the individual to whom it relates".

Two other instances in which section 8(2) allows disclosure are more controversial. The section allows the release of information to any investigative body specified in the Act's regulations, on a written request, for the purpose of law enforcement.[50] This provision has come under fire from the beginning. In testimony before the Parliamentary committee which considered the draft legislation, representatives of the Canadian Civil Liberties Association noted:

> It is rare when the law permits investigative agencies to invade residential privacy without a judicial warrant. Why should the law permit such agencies to invade *informational* privacy without an analogous safeguard? The adoption of such a safeguard would help to ensure that proper grounds existed before such extraneous use could be made of personal information. The "tunnel vision" so often associated with investigatory agencies should be made subject, where possible, to independent evaluation. Apart from situations of imminent peril to life or limb, such disclosures should require a judicial warrant.[51]

The McDonald Commission of Inquiry into R.C.M.P. practices also criticized this provision, arguing that the test for necessity for access to personal information was not clear enough.[52]

The second controversial provision in section 8(2) permits the disclosure of personal information "for any purpose where, in the opinion of the head of the institution ... the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure".[53] Commentators have criticized this open-ended provision strenuously. As Murray Rankin writes:

> It is disturbing that the opinion of the government official is to be final in the Canadian Act. Indeed, the decision of the official is not even restrained by any "reasonable grounds" test. There is no requirement that the individual concerned be notified of a government decision to disclose information, although he or she has the right to complain to the Privacy Commissioner. There is no right to seek judicial review of the Privacy Commissioner's recommendation in this regard.[54]

A Parliamentary committee charged with reviewing the *Privacy Act* has expressed similar concerns. The committee suggested that individuals should be notified of impending "public interest" disclosures of

---

50 *Ibid.*, ss. 8(2)(e) and 8(2)(k).

51 *Minutes of proceedings and evidence of the Standing Committee on Justice and Legal Affairs* (32nd Parliament, 1st Session: 1980-81) at 23A:13.

52 *Supra*, note 1 at 340.

53 *Supra*, note 6, s. 8(2)(m)(i).

54 *Supra*, note 1 at 341.

personal information and have the right to contest such disclosures in the Federal Court.[55]

In addition to these particular criticisms, C. Ian Kyer suggests that the Act's disclosure provisions are generally inadequate because of insufficient measures to prevent their abuse:

> There are only minimal checks against abuse. In the case of information disclosed to an investigative body, a copy of the request is to be kept for possible review by the Privacy Commissioner appointed under the Act. In the case of public-interest disclosure, the Privacy Commissioner is to be notified at or before the time of disclosure to permit the Commissioner to decide whether to let the individual know of the disclosure. Although the Act gives individuals the right to complain to the Privacy Commissioner about improper use, there is no requirement to notify individuals of the use made of their personal information. The Privacy Commissioner, whose office is permitted to carry out investigations of the government agencies and departments governed by the Act (these are specified in a schedule) to ensure compliance, is the principal check on unauthorized collection and use of information. The Privacy Commissioner, however, is limited to making a report including recommendations to the department or agency involved in the case of non-compliance. A copy of any such report is presented to Parliament as part of the Commissioner's annual report. Last year [1984] was the first year that departmental audits were carried out by the Privacy Commissioner and the results of those audits are not yet available. Only time will tell whether the Commissioner has enough staff and a sufficient mandate to make this check effective.[56]

3. *Exemptions*

Not all personal information is accessible under the *Privacy Act*; there are three exceptions to the general rule of access. First, some information is defined as completely outside the scope of the Act and, thus, is unaffected by the Act's access or regulatory provisions. Second, some information, while within the scope of the Act, is exempt from the Act's access provisions. Third, some information is held in specially created "exempt banks," to which administrators can deny any access.

Personal information found in "Cabinet documents" is completely outside the scope of the *Privacy Act*.[57] "Cabinet documents" are defined very broadly to include discussion papers intended to present background information or analyze policy, and records of discussions between crown ministers.[58] Critics contend that the complete exclusion

---

55 *Supra*, note 21 at 24-26.

56 *Supra*, note 4 at 189.

57 *Supra*, note 6, s. 70.

58 *Ibid.* Section 70(1) of the Act defines Cabinet documents to include, among other things: memoranda presenting proposals or recommendations to Cabinet; discussion papers, presenting background explanations, analyses of problems or policy options to Cabinet; briefs or records prepared for Ministers on matters before Cabinet. However, all Cabinet documents lose their exempt status after twenty years, and discussion

of this broad category of documents is one of the Act's major faults. Information about an individual dead for more than twenty years and library or museum materials intended solely for reference purposes is also outside the scope of the Act.[59]

Assuming that an individual's personal information comes within the scope of the *Privacy Act*, the individual may be denied access if his information falls within one of the Act's exemptions to access. Although there are several exemptions from access, they may be grouped into two categories: mandatory and permissive exemptions. The Act's only mandatory exemptions concern personal information obtained in confidence from provincial, municipal or foreign governments.[60] An individual who seeks access to information falling within these exemptions will be denied; as the exemptions are mandatory, a data bank administrator has no discretion to release this personal information, even where no harm would come from the release.

In addition to these mandatory exemptions, there are several permissive exemptions. When an individual seeks access to information falling within one of these latter exemptions, the information may be released at the discretion of the data bank administrator. However, the Act sets out no test to govern this exercise of discretion, and the Federal Court has ruled that it will not substitute its own discretion for that of the administrator.[61] Thus, the court's power of judicial review will be limited to determining whether or not the disputed personal information legitimately falls within the exemption upon which access was denied.

Permissive exemptions cover a wide variety of types of personal information including information damaging to national security, federal-provincial affairs, and relations with foreign governments,[62] as well as information relating to law enforcement, the security of prisons, and government security clearances.[63] Further permissive exemp-

---

papers lose their exempt status if they are more than four years old or the decisions to which they relate have been made public (s. 70(3)).

59 *Ibid.*, s. 3 (definition of "personal information") and s. 69.

60 *Ibid.*, s. 19.

61 See: *Information Commissioner* v. *Chairman of the Canadian Radio-Television Telecommunications Commission* [1986] 3 F.C. 413.

62 *Supra*, note 6, ss. 20 and 21. Note s. 21 also permits the denial of access to personal information injurious to the defence of any state allied with Canada or suppression of subversive activities within Canada.

63 *Ibid.*, ss. 22, 23 and 24. One exemption regarding law enforcement permits the denial of access to information relating to the investigation of any provincial or federal offence, without proof that this information would be damaging (s. 22(1)(a)). Exemptions regarding prisons cover not only information injurious to prison security, but also information which would disrupt a penal program (see ss. 22(1) and 24). The

tions concern information which is subject to solicitor-client privilege and information which, if released, would threaten the safety of individuals.[64] Likewise exempt is information about the physical or mental health of the individual making the request and which it would be "contrary to the best interests" of that individual to see.[65]

A data bank administrator who seeks to deny access to an individual must choose the exemptions to be relied upon carefully. The Federal Court has declared that it will take a liberal interpretation of the *Privacy Act* when reviewing refusals of access to personal information.[66] In particular, the court has ruled that a government institution cannot later rely on exemptions which were not cited at the time when the applicant was given notice of refusal of access. In the case of *Davidson* v. *Canada (Solicitor General)*, the court held that the government was "bound by the grounds of refusal asserted by the head of the government institution in his notice of refusal" and could not argue other exemptions at the court hearing.[67] Furthermore, when non-exempt information is included in a file along with exempt information, the former must be released to the individual making the request. The case of *Robertson* v. *Minister of Employment and Immigration*[68] illustrates

---

exemption regarding security clearances is limited; it permits the denial of access to information which would reveal the identity of an individual who furnished information in a security clearance investigation conducted for the federal or provincial government (s. 23).

64 *Ibid.*, ss. 25 and 27. Another permissive exemption permits the denial of access when the personal information of the individual making the request is mixed with personal information relating to other individuals (s. 26). In fact, information which concerns other individuals *will* be denied if disclosure would violate the non-disclosure provisions of the Act (ss. 26 and 8).

65 *Ibid.*, s. 28.

66 See: *Reyes* v. *Secretary of State* (1984), 9 A.L.R. 296 (Fed. Ct., Trial Div.) at 299:

> It must also be emphasized that since the main purpose of these "access to information" statutes is to codify the right of public access to government information ... such public access ought not to be frustrated by the courts except upon the clearest grounds so that doubt ought to be resolved in favour of disclosure....

Similar statements can also be found in *Davidson* v. *Canada (Solicitor General)* (1987), 9 F.T.R. 295 at 300.

67 (1987), 9 F.T.R. 295., at 300. However, it remains unclear whether the government can argue sections of the Act not cited in its notice of refusal if it advises the individual of the change some time prior to the individual's application to Federal Court. While Justice Jerome suggests the answer is "no" in *Davidson*, he explicitly refused to rule on this point in the earlier case of *Reyes* v. *Secretary of State*, *supra*, note 66.

68 (1987), 13 F.T.R. 120. In this case, the Federal Court considered whether certain paragraphs of a letter, which had been kept from the applicant on the basis that they were alleged to contain exempt information, should be released.

the lengths to which the Federal Court will go to sever "harmless" information from the exempt information which accompanies it.

In addition to the power implicit in all the *Privacy Act*'s access exemptions discussed above, the government has the express power to declare data banks containing files which consist predominantly of certain types of exempted information to be "exempt banks".[69] Administrators need not disclose *any* personal information included in such a bank.[70] In fact, an administrator will neither confirm nor deny the existence of any personal information in an exempt bank, and will not cite specific exemptions when refusing access.[71]

Furthermore, before the case of *Ternette* v. *Solicitor General of Canada*,[72] the Solicitor General took the position that an individual could not apply to the Federal Court for a review of documents contained in an exempt bank. Instead, the Solicitor General claimed that the court's review power was restricted to determining whether a bank had, in fact, been declared exempt and also claimed that this court review could be made only on the request of the Privacy Commissioner. *Ternette* overturned these positions and resulted in the re-opening of many banks that originally had been declared exempt.

The facts of *Ternette* were as follows: Shortly after the *Privacy Act* came into force, Nick Ternette, a community activist, applied to see personal information held in an exempt R.C.M.P. data bank, SOR/83-374. The bank's administrator refused to either confirm or deny the existence of any information in the bank. Ternette complained to the Privacy Commissioner. The Commissioner investigated and found that he too could not confirm or deny the existence of records in the bank, but assured Ternette that his rights under the Act had been respected.

Ternette appealed to the Federal Court, Trial Division. Ternette's counsel argued that the court could (at the request of an affected individual) review personal information in a file to determine whether the file had been properly included in an exempt bank. (A reasonable interpretation of section 45 of the Act would support the argument that the court had power to examine the contents of a file in an exempt

69 *Supra*, note 6, s. 18. Note that the banks must consist of files predominantly containing information exempted by ss. 21 or 22 of the *Privacy Act*.

70 *Ibid.*, s. 18(2).

71 *Supra*, note 21 at 47; *Minutes of proceedings and evidence of the Standing Committee on Justice and the Solicitor General* (33rd Parliament, 1st Session: 1984-85-86) at 29-18. In the latter source a government official confirms that administrators do not cite specific exemptions when denying access to exempt banks. However, I can find no justification for this practice; in fact, s. 16 of the *Privacy Act* would seem to require that specific sections always be cited on the refusal of access.

72 (1984), 9 A.L.R. 24 (Fed. Ct., Trial Div.).

bank.[73]) The court agreed. Justice Strayer ordered the R.C.M.P. to file an affidavit stating whether or not a file existed on Ternette; the affidavit was to be placed in a sealed envelope, along with the contents of Ternette's file, if such existed. The envelope was to be opened only by the Court's Chief Justice, and the initial hearing on the file would be held *in camera*.

Events after the trial proved to be important.[74] Ternette's counsel asked the Department of Justice to confirm that all the files in the bank had been examined before it was closed to determine if the bank met the requirements under section 18(1). In September of 1985, the Solicitor General conceded to Ternette's counsel there was no evidence to suggest that the individual files had been examined to ensure they belonged in the exempt bank. The bank had been improperly closed. After this admission, the Department of the Solicitor General and the Privacy Commissioner began separate investigations of other exempt banks.[75] They found that other banks had been improperly closed. As a result, many exempt banks were subsequently re-opened. When the *Privacy Act* first came into force, nineteen banks were declared exempt; today only five banks are still exempt.[76]

While the opening these banks is perhaps the most important contribution of *Ternette*, the case did not end there. The Canadian Civilian Security Intelligence Service (C.S.I.S.), which took over operation of data bank containing Ternette's file, continued to deny access. After persistent efforts by Ternette's counsel, C.S.I.S. released portions of the file in February of 1987, four years after the original court ruling.[77] Further portions of the file were released in November of 1987 and January

---

73 *Supra*, note 6, s. 45. The section reads:

> Notwithstanding any other Act of Parliament or any privilege under the law of evidence, the Court may [in the course of proceedings challenging the exempt status of personal information] examine any information recorded in any form under the control of a government institution, other than [a Cabinet document], and no information that the Court may examine under this section may be withheld from the Court on any grounds.

74 J. W. Grace, *Annual Report, Privacy Commissioner, 1985-86* (Ottawa: Supply and Services Canada, 1986), *supra*, note 38 at 22-23.

75 *Ibid.* See also: "RCMP secret file system in jeopardy, says Chumir," *The Calgary Herald*, 1 December 1986, p. B2. A copy of the Department of Justice's "Report on Exempt Banks" was obtained by a Parliamentary committee which reviewed the *Privacy Act*. Ironically, the report indicates that the Department of Justice's own investigators were denied access to the four of the twenty exempt banks: *supra*, note 21 at 47.

76 J. W. Grace, *Annual Report, Privacy Commissioner, 1986-87*, *supra*, note 38 at 25.

77 T. Philip et al., "Prying open a secret file," *Alberta Report*, 2 March 1987, p. 36.

of 1988.[78] The information released raised serious doubts about the propriety of the data-gathering activities of the R.C.M.P. It showed that the R.C.M.P. had kept close watch on Ternette from 1966 to 1980 as a potential subversive, even though he had never been convicted of a crime and the R.C.M.P.'s own investigators concluded in the early 1970s that he was not a threat.[79] The case continues today as C.S.I.S. refuses to release further information from the file on the ground that it might identify informants who provided information about Ternette's activities.[80]

The *Ternette* case is a powerful critique of the *Privacy Act*. Arguably, the eventual release of personal information from Ternette's file was more a result of pressure brought to bear by media attention and the persistent efforts of Ternette's counsel than the access provisions of the Act. The arbitrary closing of many exempt banks and the method of release of Ternette's personal information display an unwillingness on the part of government to respect the spirit of the Act, while the length of time between Ternette's application and the eventual release of information is appalling. In light of these facts, one is forced to consider whether the government has taken the provisions of the *Privacy Act* seriously.

4. The Privacy Commissioner and the Treasury Board

The Privacy Commissioner is an ombudsman, appointed to ensure the smooth operation of the Act. He and his staff can receive and investigate complaints by individuals. The Act gives them broad investigatory powers and it is an offence to obstruct them while they are attempting to perform their duties under the Act.[81]

The Commissioner can apply to the Federal Court for a review of information included in exempt banks.[82] In addition, he can appeal a refusal of access to Federal Court on behalf of the person denied; thus, some remedy may be available to people without the financial re-

78 T. Philip and R. Woloshen, "The secret life of a rent-a-radical," *Western Report*, 30 November 1987, p. 22; "Secret file reveals 14 year RCMP surveillance of activist," *The Globe and Mail*, 11 November 1987, p. A3. I obtained information about the latest release of information in an interview with Mr. Ternette, conducted November 28, 1988.

79 *Ibid.* The personal information released in January of 1988 is notable for its incomprehensibility. It consists of approximately a dozen highly edited pages of blurry photocopies in which only a few phrases or sentences on each page remain intact. On a few pages, virtually the only information presented is the name "Nick Ternette".

80 The position of C.S.I.S. was set out in an affidavit filed July 15, 1988, in the *Ternette* action (Federal Court file no. T-522-84).

81 *Supra*, note 6, ss. 34 and 68.

82 *Ibid.*, s. 36.

sources to take a worthy matter to court.[83] However, while the Commissioner has all these powers, his ability to *enforce* the Act is limited to making requests and recommendations; he cannot compel government officials to follow the Act's provisions.

The Privacy Commissioner is also responsible for an annual report to Parliament on the Act.[84] The reports contain statistics on the number of investigations and complaints, and discuss new privacy issues. (Surprisingly, the reports are also quite readable.)

While the Privacy Commissioner performs a watchdog function, the institution ultimately responsible for the enforcement of the *Privacy Act* is the Treasury Board of Canada.[85] The Board is responsible for ensuring that federal data banks are run according to the Act's standards, for issuing guidelines to data bank administrators explaining the operation of the Act, and for compiling and issuing the yearly data bank index.[86]

C. Critique of the Act

Praiseworthy features of the *Privacy Act* include its improvements over the preceding federal access legislation (primarily the provisions regarding court review of government refusals of access), its wide definitions of "personal information" and "data banks" (the latter extending coverage to both computerized and manual records), and the powers it extends to the Privacy Commissioner (particularly, his investigatory powers and his power to appeal a denial of access to the federal court on behalf of an individual). However, the Act is more notable for its shortcomings, of which there are several – the first being its coverage. The Act applies only to federal government data banks; private sector banks that exist within the federal jurisdiction remain unregulated. The immunity of Cabinet documents from the Act's provisions is disturbing; so too is the broad definition of what constitutes a Cabinet document, which could exempt just about any document prepared in the process of formulating government policy.

---

83 *Ibid.*, s. 42.

84 *Ibid.*, ss. 38-40.

85 *Ibid.*, s. 71. Section 71 requires that a particular federal Minister be designated as responsible for the enforcement of the Act; the Minister, in turn, is a able to delegate his powers to another government body. Although the Minister of Justice was designated to enforce the Act, he promptly delegated his responsibilities to the Treasury Board.

86 In June of 1983 the Treasury Board issued a set of guidelines for administering the *Privacy Act*; weighing in at over a kilogram, the guidelines are a sure-fire cure for even the most ardent bureaucrat's insomnia. See: Treasury Board of Canada, *Interim Policy Guide: Access to Information Act and the Privacy Act* (Ottawa: Supply and Services Canada, 1983).

The Act puts no real limits on the way personal information can be collected; neither does it effectively limit the type of information that can be collected. The Act's provisions regarding disclosure of personal information to third parties have been criticized, particularly the provisions allowing disclosure to investigatory bodies and "public interest" disclosure. Safeguards to prevent abuse have been characterized as generally inadequate. Murray Rankin also faults the Act for failing to provide judicial review outside of cases involving the denial of access: "It is very regrettable that judicial review of government practices with respect to the collection, retention and disposal of information is not likewise permitted."[87]

Regarding the access provisions, the Act puts the onus on the individual to determine which government data banks hold the information he is interested in. No doubt this will result in the necessity for multiple requests; individuals will be forced to hunt for information by trial and error. Furthermore, the broad definitions of some of the exemptions from access (for example, information "injurious to the conduct ... of federal-provincial affairs" and information "injurious to the conduct of international affairs [or] the defence of Canada"[88]) will probably lead to harmless personal information being excluded from access.

Finally, the position of Privacy Commissioner seems inadequate because, although the Commissioner has wide powers of investigation, he lacks any enforcement powers; instead, the power to enforce the Act is put in the hands of the Treasury Board of Canada. This curious division of powers gives ultimate power to an organization with only passing interest in the Act. Indeed, it could be argued that the Treasury Board would be more likely to represent the interests of data bank administrators, emphasizing expediency and the smooth operation of government data banks over the privacy and individual rights concerns expressed in the Act. In fact, the experience of the *Ternette* case suggests that the government has failed to take the Act as seriously as it should.

Happily, a recent report of the House of Commons justice committee addresses many of these criticisms of the Act, and may lead to important legislative changes. Released March 31, 1987, the report recommends provisions which narrow the exclusion of Cabinet documents, extend the coverage of the Act to the federally-regulated private sector, create civil and criminal remedies for certain violations of the

87 *Supra*, note 1 at 339.
88 *Supra*, note 6, ss. 21 and 22.

Act, and tighten control over the use of computer matching.[89] The report also contemplates a major expansion to the *Privacy Act*; it suggests that the Act should protect a broad range of privacy interests in addition to personal information.[90]

III. British Legislation On Access To Personal Information

A. The *Data Protection Act*

In Britain, one Act governs most aspects of the access to personal information question. Passed in 1984, the *Data Protection Act*[91] applies only to computerized or "automated" data bases; purely manual records are outside its scope. However, the Act gives individuals (known as "data subjects") rights of access to "personal data" held in government and private sector data bases and the right to have incorrect information corrected or erased by court order. In addition, it gives individuals rights to compensation for any damage suffered because of the loss, destruction or inaccuracy of personal information.

The Act puts certain duties on people who store and use personal data ("data users") and establishes the office of the Registrar to oversee the Act's operation. Among other things, the Registrar is responsible for maintaining a registry of data bases, open to inspection by members of the public.

The Act defines "personal data" as data "consisting of information which relates to a living individual who can be identified from that information ... including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual."[92] A "data user" is defined as a person who holds data; the definition applies to all persons who control the content and use of a collection of data processed by automatic means.[93] While the definition of a "data user" is rather broad, persons who run certain types of data bases are exempt from most of the Act's provisions. (See the discussion of exemptions, below.)

It should also be noted here that another access to information statute was enacted by the British Parliament in 1987. The *Access to*

89 *Supra*, note 21 at 29-33 (Cabinet confidences), 43-44 (computer matching), 49-51 (civil and criminal remedies), and 74-77 (coverage of federally-regulated private sector).

90 *Ibid.*, at 71-73.

91 *Supra*, note 7. *[UK Act]*

92 *Ibid.*, s. 1.

93 *Ibid.*

Personal Files Act[94] gives individuals rights of access to personal information stored by two British government authorities: the *Housing Act* local authority and the local social services authority. As this Act applies to records held in any form by these authorities, it may allow access to some manual records which originally fell outside the scope of the *Data Protection Act*.[95]

B. History of the Act

One of the first things to be noted about the *Data Protection Act* is that it came about primarily through the lobbying efforts of members of the data processing industry, not individuals worried about their informational privacy. As C. Ian Kyer notes:

> The *Data Protection Act* is not primarily the result of civil libertarian concerns. It is the result of concerns of private industry that lobbied the government to ratify the European Convention and pass the *Data Protection Act* in order to ensure that the United Kingdom did not find itself excluded from data flows from those European countries that had passed similar data protection legislation.[96]

In 1981, the Council of Europe adopted a special treaty entitled the *European Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*. The convention commits its signatories to adopt legislation protecting individuals from the dangers posed by computerized data bases. The convention sets out eight principles which legislation should embody:

1. information should be obtained lawfully and be processed fairly and lawfully;
2. information should only be held for one or more specified purposes;
3. information should not be used or disclosed in a manner incompatible with that (those) purpose(s);
4. information should be adequate, relevant, and not excessive in relation to the specified purpose(s);
5. information should be kept up to date;
6. information should not be kept longer than necessary;

---

94 1987 c. 37. Volume "A", Halsbury's Statutes of England, 4th ed., Current Statutes Service (London: Butterworths, 1987) 6 Civil Rights 17.

95 *Ibid*. Composed of only five sections, the *Access to Personal Files Act* does little more than provide that regulations will be drafted to permit access to personal information held by two British government authorities.

96 C. Ian Kyer, "The U.K. Data Protection Act: A Model for Canada?" (1985) 2 Canadian Computer Law Reporter 225 at 229.

7. an individual should be entitled to know whether data is held about him, to have access to it, and, where appropriate, to have it corrected or erased; and
8. appropriate security measures should be taken to prevent accidental loss of information, unauthorized access to information, or unauthorized disclosure or destruction of information.[97]

As a member of the Council of Europe, Britain was under outside pressure to ratify the convention by passing data protection legislation in accord with it. But perhaps more importantly, the convention does not permit transborder transfers of data to countries which do not have similar data protection legislation. As more and more European states passed data protection legislation in accord with the convention, Britain's data processing industry became increasing concerned that it would be shut off from European markets because of Britain's lack of legislation and began to lobby for a data protection act.

Thus, the history of the *Data Protection Act* may account for some of its more obvious flaws and explain why critics suggest that the Act is more concerned with protection of the rights of data base operators than the rights of individuals. As Jeremy McBride writes:

> The Act purports ... to implement the provisions of the [Council of Europe's] Convention – a necessary preliminary to ratification by the U.K. – but at most it is an attempt only to do the minimum required. This is true of the exemptions permitted; the unwillingness to take up the option to apply the proposed protection to manual files as well as to computerized or automatic systems and it may also be an appropriate comment on the enforcement machinery which is going to be established.[98]

C. Substantive provisions of the Act:

1. Rights of "data subjects"

Individuals have three basic rights under the *Data Protection Act*: the right to access to their personal information, the right to have that information corrected where it is inaccurate, and the right to compensation should they suffer damage because of inaccurate information or the unauthorized disclosure or destruction of information.

To exercise the right of access to personal information, an individual must apply in writing to the appropriate data bank.[99] To determine which data bank to apply to, the individual can consult the registry

97 R. Sizer and P. Newman, *The Data Protection Act: A Practical Guide* (Aldershot, England: Gower Ltd., 1984) at 24-30.
98 J. McBride, "Citizen's Privacy and Data Banks: Enforcement of the Standards in the Data Protection Act 1984 (U.K.)," (1984) 25 Les Cahiers de Droit 533 at 535.
99 *Supra*, note 7, s. 21.

which the Act requires the Registrar to maintain; the registry is supposed to list every data bank within the country which is covered by the Act. Once a request has been made by an individual, the data user has forty days to answer.[100] Where the data user refuses to comply with a legitimate request, the individual can seek a court order requiring compliance.[101] The data bank has the right to charge a fee for access; the maximum fee permitted by the Act's regulations is £ 10.[102]

To exercise the right to correct inaccurate information, an individual must apply to court. The individual must convince the court that the information is "incorrect or misleading as to any matter of fact".[103] Should the court agree, it can order the personal information be corrected or erased by the data user.

The right to compensation exists where the individual suffers damage because of the inaccuracy of personal information, the loss of personal information, or because of the unauthorized loss or destruction of personal information.[104] Should the individual prove such damage, he can also receive compensation for any "distress" suffered. It is a defence for the data user to prove that he "had taken such care as in all circumstances was reasonably required".[105]

2. Duties and rights of "data users"

The *Data Protection Act* imposes two duties on persons who run data bases: the duty to register their data base in the Registrar's registry, and the duty to uphold the data protection principles of the Council of Europe convention.

To register in accordance with the first duty, a data user must provide information about the scope and purpose of his data bank(s), so that an individual consulting the registry will be able to determine which data banks might hold information about himself.[106] The Act makes it an offence for a data user to hold personal information without having registered.[107] (Of course, data users who are exempt from the registration provisions of the Act are not required to register.) It is also an offence for a user to hold data in a way that conflicts with the statements made in the user's registration.[108]

---

100 *Ibid.*, s. 21.
101 *Ibid.*
102 Halsbury's Abridgement 1987 (London: Butterworths, 1987) at 1168.
103 *Supra*, note 7, s. 24.
104 *Ibid.*, ss. 23 and 24.
105 *Ibid.*, ss. 22(3) and 23(3).
106 *Ibid.*, s. 4(3).
107 *Ibid.*, ss. 5(1) and 5(5).
108 *Ibid.*, ss. 5(2) and 5(5).

In accordance with the second duty, a data user must uphold the eight principles of the Council of Europe convention on data protection.[109] Thus, a data user must ensure that personal information: is obtained and processed fairly; is held for only specified and lawful purposes; is not used or disclosed in a manner contrary to the user's specified purposes; is adequate, relevant, and accurate; is not retained longer than necessary; is available for inspection by data subjects; and, is protected by appropriate security measures. However, the principle regarding the disclosure of personal information is weakened by later sections of the Act, which allow the principle to be ignored in several situations.[110] One sweeping exception is contained in s. 34(5) of the Act; it permits disclosure where it is "required by or under any enactment, by any rule of law or by an order of a court." Section 34(5) has been criticized by Harry Cohen, a British MP.[111] He notes that it has permitted the British government to sell the electoral register in machine readable form at £ 15 per thousand names to private businesses, without requiring notice of these sales to the data protection Registrar. Cohen also writes that, despite the first data protection principle's injunction that "personal information shall be collected lawfully and fairly", the Home Secretary has refused to include a warning on the electoral registration form that the information collected will later be disclosed to whomever pays the price for a copy of the register.

Data users who fail to live up to the duties imposed on them by the Act risk an investigation by the Registrar, who has the power to issue enforcement or "deregistration" orders. However, data users have a right to appeal these orders to a specially created "Data Protection Tribunal".[112] The Tribunal is composed of members who represent the interests of data users and individuals. Strangely enough, individuals are denied recourse to this tribunal to enforce their rights. As Nigel Savage and Chris Edwards note, "It is perhaps a measure of the gov-

---

109 *Ibid.*, s. 2.

110 *Ibid.*, ss. 26-28, 33, and 34. These sections allow the non-disclosure principle to be ignored when disclosure of personal information is necessary for national security reasons (s.27), for the prevention of crime or the collection of taxes (s.28), for payroll or accounting reasons (s.32), for statistical purposes (s.33), and where required by a law or court order (s.34). The Act also exempts personal information from the non-disclosure principle when the disclosure is "urgently needed for preventing injury or other damages" and provides that those prosecuted under the non-disclosure provisions of the Act will have a good defence if they had "reasonable grounds" for believing disclosure was necessary for that reason (s.34).

111 H. Cohen, "Harry Cohen, MP for Leyton considers the implications of the Data Protection Act on the sale of the electoral register," 2 Computer Law and Practice (No. 4, March/April 1986) 127.

112 *Supra*, note 7, ss. 13 and 14.

ernment's priorities in terms of data protection that users have a tribunal through which appeals can be heard, while data subjects seeking judicial support for their statutory rights against data users are directed to the ordinary civil courts."[113]

3. Exemptions

The *Data Protection Act* contains provisions which limit the protection that the Act affords to data subjects. To begin with, certain types of information are completely beyond the scope of the Act; for example, information held solely for the purpose of word processing and most information held wholly outside the United Kingdom.[114]

In addition to this exclusion, the Act also contains two categories of exemptions. The first category exempts certain types of information from the Act's registration and access provisions. Personal information falling into this category includes information held for the purposes of national security and information held for the purposes of keeping payroll records or business accounts.[115] While beyond the Act's access and registration provisions, data users holding these types of information are still bound to operate according to the Council of Europe's data principles (excepting, presumably, the principle of subject access). But there is no effective way of ensuring compliance, since they will not be registered and are beyond the powers of the Registrar. The provisions regarding the national security exemption are the most worrisome. They allow Ministers of the Crown the power to declare banks exempt because of national security concerns at will, and prohibit court review of such a declaration.[116]

The second category of exemptions exempts several types of personal information solely from the Act's access provisions. Thus, where access would probably result in prejudice to "the prevention or detection of crime" or "the apprehension or prosecution of offenders," no access is allowed.[117] Similar restrictions apply when the data held relates to the appointment of judges, solicitor-client privilege, or data held for statistical or research purposes.[118]

4. Duties and powers of the Registrar

---

113 N. Savage and C. Edwards, "The Legislative Control of Data Processing – The British Approach," (1985-86) 6 Computer L.J. 143 at 150.

114 *Supra*, note 7, ss. 1(8) and 39.

115 *Ibid.*, ss. 27, 32 and 33.

116 *Ibid.*, s. 27.

117 *Ibid.*, s. 28.

118 *Ibid.*, ss. 31 and 33(6).

The Registrar is the person charged with overseeing the operation of the *Data Protection Act*. The Registrar is responsible for running the registry (which contains information about all the data banks covered by the Act), for investigating complaints made by individuals against data users, and for ensuring that data users observe the eight data protection principles. To carry out the last of these responsibilities, a wide range of supervisory powers are available to the Registrar.[119] He can issue enforcement notices, which require a data user to take some specific action, or deregistration notices, which remove the data user's data banks from the registry and thus make it illegal for the user to continue to run a data bank. In addition, the Registrar can initiate prosecutions for offenses under the Act; offenses include operating an unregistered data bank and operating a data bank in a manner inconsistent with its registration.[120]

However, Jeremy McBride points out that although the Registrar has an impressive arsenal of enforcement powers, the Registrar lacks effective investigatory powers.[121] As well, McBride notes that all of the Registrar's enforcement powers can only be used when the Registrar is "satisfied" that it is necessary to do so; McBride suggests that judicial review may severely limit the circumstances in which the Registrar is able to use his powers.[122] Finally, McBride points out that the effectiveness of the Registrar will depend on whether "he shows an early willingness to use his muscle in an appropriate case" and whether his staff is large enough to properly fulfil the duties assigned to him.[123] Other commentators have also expressed concerns about the size of the Registrar's staff.[124]

D. Implementation of the Act

Although the *Data Protection Act* was given royal assent in July of 1984, the Act did not come fully into effect until November of 1987.[125] Until that time the Act's provisions regarding access to personal information, compensation for inaccurate information, and court-or-

119 *Ibid.*, ss. 10-12.

120 *Ibid.*, ss. 5 and 6.

121 *Supra*, note 98 at 547.

122 *Ibid.*, at 546-550.

123 *Ibid.*, at 542.

124 *Supra*, note 113 at 149 ("Given the relatively small staff at his disposal, the majority of the Registrar's activities and investigations are likely to be initiated by actual complaints from data subjects."); also, *supra*, note 96 at 229 ("The maintenance and supervision of the data protection registers will require a diligent registrar and a large and well-funded administrative staff.").

125 *Supra*, note 7, s. 42. See also: E.J. Howe, "Data Protection in the United Kingdom," 3 Computer Law and Practice (No. 6, July/August 1987) 204.

dered erasure of inaccurate information did not take effect. The interim period allowed data users to register their data banks with the Registrar and become familiar with the Act's requirements. Certain enforcement powers did not become available to the Registrar until the end of this period.

Unfortunately, the relaxed schedule of implementation has made it difficult to assess the success of the Act. I have been unable to find a single reported case dealing with the Act or its provisions. The lack of cases on the access and compensation provisions makes it difficult to assess whether the Act's strategy of giving individuals a limited civil remedy is an effective one. The lack of cases interpreting the powers of the Registrar makes it impossible to judge the validity of Jeremy McBride's suggestion that these powers will be limited by judicial review. Not only has there been a lack a case law; there has been little academic commentary on the Act.[126]

Some commentators have pointed out that a major obstacle to the Act's success may be a lack of resources available to the Registrar. As McBride notes, the goal of merely registering all the data bases covered by the Act is an enormous one: "The scale of the problem is vast and part of it is not knowing how many systems there are – estimates vary from the Home Office's cautious 80 000 to other estimates which may seem extravagant, varying as they do between 300 000 and half a million, but which in reality may be quite accurate given the high level of computer sales in the U.K."[127] Not only must the Registrar and his staff supervise the registration of these data banks, they must also investigate individual's complaints about particular data users and, where necessary, enforce the provisions of the Act against recalcitrant data users by prosecution or by issuing orders against them. In the face of this workload, the government White Paper issued before the debate of the *Data Protection Act* suggested that the Registrar "may need a staff of about 20."[128] Moreover, the initial experience of registration has suggested that the task is at least as large as McBride suspected, particularly because large organizations have often chosen to register their various data banks separately.[129] (This system of separate registrations

126 I have found only three significant publications on the Act: R. Sizer and P. Newman, *supra*, note 97; J. McBride, *supra*, note 98; N. Savage and C. Edwards, *supra*, note 113.

127 *Supra*, note 98 at 537-538.

128 White Paper, Data Protection: the Government's Proposals for Legislation, Cmd. No. 8539 (1982). I have been unable to learn what size of staff the Registrar was eventually given. [as cited in Savage & Edwards, *British Approach, supra*, note 113 at 144]

129 N. Savage and C. Edwards, "Implementing the Data Protection Act 1984," (1986) J. of Bus. L. 103 at 110.

forces the individual, not the organization, to decide which data bank most likely holds the information they are interested in; as well, it allows the organization to charge separate fees for each request for access to a different data bank.) As Nigel Savage and Chris Edwards wrote in an article published in 1986:

> The Home Office originally estimated the volume of registrations at 200 000 during the six month registration period November 1985 to May 1986. This estimate has always open to debate, given the wide coverage of the [*Data Protection Act*] extending deep into the public sector as well as the private sector. The actual figure may be nearer 700 000 and could be even higher, depending on how many organizations opt for multiple registration entries for their operations, rather than one entry.[130]

E. Critique of the Act

In defence of the *Data Protection Act*, it must be said that the Act does establish limited civil remedies for individuals who have been harmed by inaccuracies in their personal information. This sort of legislative innovation is laudable; however, it is difficult to decide whether it has been effective when no cases exist applying the Act's provisions. A second positive feature of the Act is its wide coverage of both private and public data bases. Unfortunately, it is also undeniable that the Act suffers from serious weaknesses, many of which may be attributable to its origins as a measure to protect the U.K. data processing industry, rather than individuals' rights.

First, the Act's coverage is restricted only to computerized or "automated" data bases – so that data users who wish to avoid the Act's provisions will be able to do so simply by transferring their sensitive records to manual files. (This fault has been alleviated somewhat by the *Access to Personal Files Act*, which allows access to manual records held by two British government authorities.[131] However, manual records held by the remainder of the government and the entire private sector are outside the scope of access legislation.)

Second, while the *Data Protection Act*'s definition of "personal data" does include matters of opinion about the individual, it doesn't include "any indication of the intentions of the data user in respect of that individual." "There is, therefore, some room for the astute data user to disguise opinions as intentions and thus frustrate the rights given to data subjects," Savage and Edwards point out.[132]

Third, while the Act has broad coverage of computerized data bases, it also contains a large number of exemptions, some of them

130 *Ibid.*
131 *Supra*, note 94.
132 *Supra*, note 113 at 148.

fairly broadly worded. And while the Act *does* allow for court review to determine whether a data bank is rightly considered exempt, it prohibits such court review when the exemption claimed is "national security" and a Ministerial certificate has been obtained by the data user.[133]

Fourth, the Act has been criticized for using several forums to resolve disputes. As McBride writes:

> Furthermore the Act does contain a degree of jurisdictional complexity which may prove a hindrance in the long term; thus there is a tribunal system for appeals against decisions by the Registrar; the criminal courts will be used where those decisions are not respected but the ordinary civil courts will be the forum for the victim of any violation of the standards laid down by the Act; and there is also a good chance that the Divisional Court may also be involved as judicial review by the person using the data or by the person who is subject of the data is by no means out of the question.[134]

One might argue that the "Data Protection Tribunal" is the best forum both for appeals of the Registrar's decisions and for actions for compensation by individuals.

Fifth and last, the resources available to Registrar may be insufficient to successfully carry out his duties under the Act. Given the size of the data processing industry and the huge number of data banks that are being registered, the extent of the Registrar's powers may ultimately prove irrelevant if his staff is so small that he is unable to perform even some of the duties assigned to him.

IV. CONCLUSIONS

MY REVIEWS of the *Privacy Act* and the *Data Protection Act* complete, I will now consider the differences and similarities that exist between the two Acts; in the course of my discussion, I will also consider how the Acts compare to model legislation.

On the whole, there are only two main differences between the Acts. The first is that the British Act gives "data subjects" the right to a private action for compensation when they are harmed by inaccurate personal information. No equivalent right is established by the Canadian Act and this is one area where it might be improved by following the British approach; however, conclusions about the effectiveness of the British approach are impossible because the sections establishing the right of a personal action have only recently come into effect. The second difference between the two Acts concerns their coverage. While

133 *Supra*, note 7, ss. 25 and 27.
134 *Supra*, note 98 at 536.

the British Act applies to all computer data bases, public or private, the Canadian Act is limited in coverage to federal government data bases. At the same time, the Canadian Act applies to manual *and* computerized records, while the British Act is limited to the latter. Extending the coverage of the *Privacy Act* to some parts of the private sector would be a laudable idea; as noted in my critique of the Act, a recent Parliamentary Committee report makes this suggestion.

More similarities than differences exist between the British and Canadian Acts. Many of the similarities point to places where the Acts fall short of the requirements of model legislation. In my introduction, I argued that an ideal system of legislation should: give individuals the right of access to their personal information and the right to have inaccurate personal information corrected; place limits on the collection and use of personal information; establish a government organization with a mandate to deal actively with personal information problems; place a duty on information-gathering agencies to help individuals gain access to the personal information they hold, and; establish a right of private action that would compensate individuals and penalize agencies which stored inaccurate information.

How do the British and Canadian Acts compare to this model legislation? To begin with, both Acts give individuals a right to see their personal information, and a right to have that information corrected if it is inaccurate. However, both Acts contain many broadly-worded exemptions to their access provisions. While it would be impossible to argue that access to personal information legislation should contain no exemptions, it is possible to argue that the exemptions in the British and Canadian Acts are too wide, allowing harmless information to be excluded from access. Furthermore, the access procedures established by the Acts will, in some cases, defeat any but the most persistent individuals. Under the Canadian Act, for example, if both the data bank administrator and the Privacy Commissioner deny the individual access, the only recourse left is an action in the Federal Court; a court action will involve time and cost, even if the Act dictates that the court must use a streamlined procedure when dealing with access to information applications. The existing access to information provisions are a good start, but perhaps legislation should go a step further, establishing procedures that not only allow but encourage access.

Both Acts fail to provide effective controls on what data may be collected, how it may be collected, and what it may be used for. While the Acts place some limits on the collection and use of personal information, the limits are very loose indeed, and no provision is made for court review. (Recall that in the case of the Canadian Act, the data bank administrator's judgement governs the disclosure of personal

information to third parties: the Act allows disclosure whenever an administrator thinks it in the public interest, and also allows access by investigatory bodies without the necessity of a search warrant.)

Neither Act establishes a civil cause of action similar to the one envisioned in my introduction. The British Act creates a limited civil action which imposes liability only when a wronged "data subject" can prove he was harmed by an agency's holding of inaccurate information.[135] The Act also allows an agency to escape liability for inaccurate information obtained from a third party by simply noting on the record how the information was obtained; no duty is placed on an agency to ensure that such information is accurate.[136]

Both Acts establish offices of "personal information ombudsmen"; however, the Canadian Privacy Commissioner has no power to enforce the Act, while the British Registrar is endowed with enforcement powers but may not have the necessary resources to use them effectively. There is no duty on data keepers under either Act to assist the individual locate his personal information within their organization; the result is that burden falls squarely on individual to hunt through the labyrinth organization of his foe to find needed information. The individual is left alone; at best, he might receive some help from the Registrar or Privacy Commissioner, but considering the wide scope of responsibilities of both officials, one is forced to question whether they will have the time or inclination to provide much assistance.

A. Access to personal information and the individual

This is not only a legal battle but a political one, too. All Canadians have the right to access to their files. *Nick Ternette*[137]

The invention of the computer gives rise in our time to a situation somewhat analogous to the discovery of iron in prehistoric times, for as the weapons fashioned of the new metal must have been a key element in the ancient power structures so the computer's ability to store, manipulate, and transmit data makes it a key component of power today. Indeed, some writers view the question of informational privacy as being, in essence, a political and not a legal issue. Progressively, institutions possess more and more information about individuals, while there is little reciprocal flow of information about the institutions back to the individuals.[138]

135 *Supra*, note 7, s. 22(1).
136 *Ibid.*, s. 22(2).
137 N. Ternette, as reported in: "Rebel for many causes," *The Winnipeg Free Press Weekly*, 23 October 1988, p. ST/3.
138 *Supra*, note 2 at 19.

My criticism of the British and Canadian Acts might be summarized in the following way: both put too heavy an onus on the individual to enforce his rights and both take measures that are insufficient when compared to the scope of the personal information problem. Faced with the prospect of searching through a registry containing thousands – or, in the British case, hundreds of thousands – of data banks, the individual will likely never even take the first step of determining whose data banks he wants to investigate. Jeremy McBride makes this observation about the *Data Protection Act*:

> [I]t is unlikely that most data subjects have the enthusiasm or the tenacity to use the access provision to discover the information held about them or to bring civil proceedings against those discovered to have violated the data protection principles. It would be almost impossible for any individual to calculate who might have information about him; in most cases anyway it is only likely to become an issue of importance to the individual when an adverse decision is taken in respect of him and the explanation, which may not actually be given to him, is that it was on the basis of information obtained or held by the decision-maker. If he gets to know of it then he might want a remedy but it is much more likely that he won't get to know of it....[139]

Perhaps the real problem with personal information legislation is that governments lack the will to take more effective measures designed at redressing the balance between individuals and information-collecting agencies. The offices of Privacy Commissioner and Registrar are both riddled by flaws in their make-up. Neither is the sort of comprehensive institution broadly responsible for privacy concerns that one would prefer; ideally, such an institution should play an active role in educating the public about privacy concerns and helping individuals find where their personal information is kept.

Governments appear unwilling to impose costly burdens on agencies which keep personal information – instead, they have established systems of access which require a minimal level of effort on the part of such agencies to operate. Yet there is a strong argument that those who intend to gain some benefit from the use of personal information should be expected to pay special costs associated with it. The point was made in my introduction: personal information is personal. Agencies which use personal information should expect to bear the costs involved in keeping the system open to access by individuals, and should also expect to be called into account when that information is inaccurate.

At the core of all personal information concerns is the tension between the interests of the individual and the institution. As a society which claims to value the integrity of the individual, we should be

139 *Supra*, note 98 at 538.

prepared to pay the price for ensuring that personal information is dealt with in a way that protects the rights of the individual. The issue becomes more important every day as we become an increasingly computerized society, one which grows increasingly dependant upon records. The more our society develops along these lines, the less powerful the individual will feel, and the greater will be the need for legislation which takes further measures to protect personal information.