Information Privacy in the British Columbia Health Care System: Issues and Challenges

by

Rabia Chung

B.A., York University, 1989

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

in the Department

of

Political Science

The University of Northern British Columbia

May 1996

Abstract

This thesis investigates the challenges to the protection of privacy in the health care field and the regulatory response by the government of British Columbia to legislate information and privacy rights. Recent social, political, economic and technological developments all pose potential threats to privacy. An examination of the privacy literature demonstrates that the subject of privacy has captured the attention of many disciplines. Furthermore, the legal, philosophical, political and socio-cultural literature suggests diverse views exist about the definition and value of privacy. Nevertheless, in Canada and other western countries, privacy is considered an important value in a liberal democratic state. Specifically, "information privacy" where individuals have some control over the dissemination of personal information is a subject which has been gaining salience on the public agenda over the past thirty years.

In response to the modern welfare state's expanding data banks of personal information and the proliferation of computerization, several western democracies have enacted data protection policies. A comparative examination of data protection policies highlights different approaches to the protection of privacy in the United States and Canada. The government of British Columbia drew from these experiences and enacted stronger data protection legislation. The Freedom of Information and Protection of Privacy (FOIPP) Act gave the Information and Privacy Commissioner regulatory powers to overturn government decisions and to issue binding orders.

Privacy of health information is an important data protection issue. Traditionally, the medical relationship was confidential and free from third party interference. A critical survey of theories in the health literature describes the physician-patient relationship and information control. The proliferation of information within society increases the need to control and to limit the use of personal health records. Three trends in the health care field challenge the traditional professional relationship between the physician and the patient. First, the status of the physician changes as more individuals and organizations gain access to patient information. Moreover, consumers of

health services demand more information from physicians. Second, the multi-disciplinary approach to health care delivery requires the exchange and sharing of information among health care professionals. Researchers and public health officers require identifiable patient information to conduct studies and to protect public health. Third, government agencies request more information from the health care sector and recipients of social benefits. The information is used to regulate and control the publicly funded health care system. The provision of hospital insurance, medicare and other health care insurance programs entails the collection of large quantities of information. A variety of technologies including the Pharmanet computerized drug information system and card technologies provide administrative data and permit the sharing of health information among government agencies and health care professionals. Some critics and advocates suggest the new technologies reduce privacy further and increase the potential for a "surveillance society."

An examination of the policy literature, parliamentary debates and interviews with members of the policy community promoting information rights in British Columbia demonstrates that privacy is important both politically and symbolically. An assessment of the FOIPP Act and interviews with hospitals and self-governing professional bodies suggest patients and organizations have benefited from the legislative changes. The statutory requirements of the Act present some challenges to the financial and organizational resources of hospitals and self-governing professional bodies.

A study of the health policy environment and the protection of privacy highlights a number of important trends in Canada. These include: the increasing legislative and judicial protection of privacy rights, the emerging patient rights movement, the regulatory challenge for governments to balance the right to privacy with the need to provide efficient and effective services using information technologies and the influential role of the policy community in the field of data protection.

Table of Contents

List of Tables

List of Acronyms

British Columbia Civil Liberties Association (BCCLU)

Canadian Medical Association (CMA)

Freedom of Information and Privacy Association (FIPA)

Freedom of Information and Protection of Privacy (FOIPP) Act

Health Care Alliance (HCA)

Ministry of Health and Ministry Responsible for Seniors (MOH)

Ontario Medical Association (OMA)

Acknowledgement

There are a number of individuals who have contributed to the development of this thesis. I am particularly grateful for the encouragement and comments from my supervisor Dr. Mary Louise McAllister. I wish to thank her for the interest and enthusiasm shown throughout the process of this thesis. I have benefited from my association with the Political Science Faculty and the support of fellow Graduate Students.

I wish to thank my husband Derrick, for maintaining his sense of humour and listening to me discuss the subject of privacy over dinner on a daily basis. I believe he is well acquainted with the topic now. This thesis would not have been possible without his support and encouragement. I also wish to thank my family and especially my sisters for their words of confidence and support.

Chapter I - Introduction

The growth of the welfare state, the expanding role of the bureaucracy and the proliferation of information technology foster increasing concerns about the Canadian state's encroachment into the private lives of citizens. This is most notable by governments' growing collection and uses of personal information for efficient and effective service delivery. The emergence of data protection policies in western democracies reflects a rising tension between the protection of individual privacy and the information requirements of the modern state. Literature on data protection policies suggests that the origin of the privacy problem was the expansion of bureaucracy and its interaction with information technology.[1] This argument is supported by an examination of one particular policy area, health care. Today, the Canadian health-care information environment poses a tremendous regulatory challenge to governments. Health information is a valuable tool that facilitates the provision of services and the regulation of the health care system. From a "macro" perspective, socio-cultural, economic and technological developments promote the increasing use of health information by a diversity of individuals and organizations. The health literature suggests that the physician no longer exercises exclusive control over the patient record. In response to the proliferation of health care professions, physicians must exchange information with growing numbers of professionals in the health field. The role of the physician as the gatekeeper of health information is slowly being eroded. The medical profession's diminution of power and the state's intervention in the health policy field create some tension over the control of information. The publicly funded health care system presents a significant challenge to professional secrecy. Health care providers and patients must supply information to the public bureaucracy to facilitate the third party payment system. Moreover, provincial legislation in

---

[1]Priscilla M. Regan (1995). Legislating Privacy: Technology, Social Values, and Public Policy. The University of North Carolina Press, Chapel Hill. Regan observes on p. 14, that: "Although technology was the catalyst for public concern, most analyses concluded that technology, was not the policy problem. Instead, the problem concerned privacy invasions resulting from organizational uses of these new technologies."

Canada often overrides patient confidentiality. The statutory duty to disclose patient information occurs in the reporting of vital statistics, communicable diseases and notification of individuals who are unable to operate a motor vehicle safely.[2] To gather information, the government has created an elaborate system in which the treatment of every patient by a physician or in a hospital is reported to the health insurance authorities. In response to fiscal challenges, regulators are employing a variety of technological solutions for health information management such as computerized drug networks and personal identity cards. The new technologies store a vast quantity of health information, permit efficient management of data, reduce cost and control abuse in the system.

At the heart of the debate involving the free flow and exchange of information in a liberal state is the patient's right to self-determination or the right to control the use of personal data. The concept of privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[3] This concept received considerable attention beginning in the 1960s when bureaucrats assembled personal information in centralized and computerized databanks. By the early 1970s the institutional use of information technology (specifically databases) by public sector bureaucracies prompted debates on government surveillance practices and the need for data protection policies. Today, as more individuals and organizations acquire health information, the impetus to limit its disclosure and use grows stronger. In 1992, for example, the inclusion of health records in the British Columbia Freedom of Information and Protection of Privacy (FOIPP) Act gave patients the

[2]In British Columbia, the Communicable Disease Regulation requires physicians to report incidence of communicable diseases such as hepatitis, mumps, tuberculosis, syphilis and AIDS. Under the provincial Health Act, the medical health officer can order an individual suspected of having a communicable disease to undergo tests and treatment, and may place the individual in quarantine.

[3]Alan F. Westin (1967). Privacy and Freedom. Atheneum, New York. The use of this definition of privacy as the control of information about and access to oneself has been the basis for most policy discussions on privacy in the United States and Canada. Privacy as defined by Westin does not mean withholding information but rather the control we exert over information about ourselves.

right to exert control over the collection, use and disclosure of personal health information. Patients now have a broad legislated right to copy and have access to personal information, challenge its accuracy, make corrections and to authorize the release of medical information.

The government of British Columbia has sought to mediate the growing and complex problem of information control by including the health records of provincial bodies, hospitals, health care facilities, health organizations receiving funding, and self-governing professional bodies. The response by the policy community to the government's legislated protection of health records reflects a host of competing claims and values. When the FOIPP Act was first proposed in June 1992, the legislation was welcomed by the policy community that included public interest groups, academics, advocates and the media.[4] Conversely, some resistance to the legislation was evident from various interests including members of the health sector and self-governing professional bodies. Many members of health care organizations believed professional ethics, health care codes and guidelines provided adequate protection to patients. As a result of the FOIPP Act, some stakeholders note that the legislation has fulfilled certain expectations and provides benefits to patients.[5] A number of organizations indicate that the financial resources and time requirements needed to effectively implement and administer the Act presents significant challenges. According to members of the health sector and self-governing professional bodies, record-keeping practices have improved substantially. In many cases, the methods used for information collection, storage and dissemination have changed dramatically. On the other hand, one hospital representative points out that the legislative impact of the FOIPP Act was minimal since the organization's internal policies and procedures provided safeguards and access to information. The perspectives

[4] British Columbia. Official Report of Debates of the Legislative Assembly. 1st Session, 35th Parliament. Vol. 4, No. 20: 20: 2737 (June 18, 1992); Vol. 4, No. 24: 2867 (June 22, 1992) and Vol. 5, No. 1: 2949 (June 23, 1992). The Barry Jones Report titled "The Extension of Citizens' Information and Privacy Rights to all Public Bodies in British Columbia" on February 1, 1993 highlights the various interests involved in the debate on the proposed legislation and subsequent amendments.

[5] Personal interviews, refer to Chapter Five.

of the various interests and the policy community reflect a diversity of views and concerns. Similar to other public policies, the FOIPP Act represents a compromise. Individuals and groups compete for control over information. As a result, the protection of privacy needs to be balanced with other values which individuals regard as important such as reducing fraud and abuse of publicly funded programs. This is evident in the health field as patients try to retain some control over personal health information and to limit the non-medical use of health data. Government use of information technology contributes to the challenge. The provincial government faces competing and conflicting interests and demands: It is expected to protect individual privacy rights while providing efficient and effective services. It is a difficult regulatory problem to resolve.

The central purpose of the thesis is to explore challenges to privacy in the health field and the legislative impact of the British Columbia Freedom of Information and Protection of Privacy (FOIPP) Act. An examination of the Act and its policy environment illustrates some of the regulatory difficulties faced in other western democracies in the area of data protection. In this context four important questions are addressed. First, how is privacy protected in North America? Second, what problems of privacy arise in the health field? Third, what effect does public bureaucracy and information technologies have on privacy? Fourth, what is the impact of the British Columbia FOIPP Act on individuals and organizations that handle health information?

Rationale for the Study

The concept of privacy has been studied extensively by various disciplines resulting in a significant body of knowledge. Historians, social scientists, lawyers, political scientists and public policy analysts have examined access to information and privacy legislation both in Canada and abroad. The approach adopted for this study borrows from all of these disciplines. From a public policy perspective, a comparative analysis of the American and Canadian models of data protection policies contribute to the understanding of the legislative approach adopted in British Columbia. A survey of theories in the health literature illustrates the dynamics of the physician-patient

relationship and information control. Each perspective provides some insight on the patient rights movement and the demands made for access to, and privacy of, health records. A number of privacy issues are highlighted by the bureaucratic use of information technology to reduce costs and control abuses in the health sector. An investigation of the health field demonstrates a number of important trends within Canadian society: They include, the emergence of patient rights and the demands for information self-determination, increasing intervention of the state in the health care sector, the legislative and judicial recognition of the patient's rights to access health records and privacy, and the growing proliferation of health information management.[6] The debate on the legislated protection of health information presents an opportunity to explore the role of the policy community and the actors who are concerned with the protection of privacy. Public interest groups, advocates, health care representatives and self-governing professional bodies represent a variety of interests. Interviews with stakeholders provide empirical evidence on the impact of the FOIPP Act, strengths and weaknesses, and draw attention to the competing perspectives in the debate.

Definitions of Privacy

A review of the historical literature suggests that the concept of privacy is very subjective and has undergone extensive interpretation. An in-depth analysis of the privacy literature led Colin J. Bennett to the conclusion that; "...privacy is vague, ambiguous and controversial and that it embraces problems, tensions, rights and duties."[7] Bennett suggests the provision of a definitive list of concerns that encompass the term privacy is not possible. Many authors comment on the difficulties in finding a consensus on a definition of privacy.[8] The privacy legislation of the United

[6]The term information self-determination means to control information about oneself by determining when, how and to what extent information will be communicated.

[7]Colin J. Bennett (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States. New York, Cornell University Press. p.13.

[8]Many authors note the difficulties in trying to define the concept of privacy, particularly in the philosophical and legal writings. Writings by Arthur Schafer (1980) claim it is an ambiguous term. Alan Westin's (1967) Privacy and Freedom begins by stating "Few values so fundamental to society as privacy

States, Canada and British Columbia does not include a definition of privacy. Canadian policy-makers in the 1980s, following the review of the Federal Privacy Act, tried unsuccessfully to include a definition of privacy in the legislation. This situation is not unique to Canada. One school of thought, "...treats privacy like the proverbial elephant - we may not be able to define it exhaustively, but we can always recognize one when we see it."[9] This problem becomes clear as one considers the many arguments for privacy that include claims against intrusive behaviour by police such as wiretapping and the right to make decisions in private affairs. Bennett provides a description of the many claims to privacy; "...privacy has referred to the exclusiveness of physical space around an individual, to the autonomy of decision making without outside interference, and to the right to control the circulation of personal information."[10] There are three generally recognized areas of privacy, territorial privacy (property), privacy of the person, privacy in the informational context. Three dominant ideas encompass the concept of privacy. First decisional privacy includes decisions on private behaviours such as marriage and family relations. Second, a "reasonable expectation of privacy" is necessary against intrusion and surveillance such as wiretapping.[11] Third, informational interests include "the interest of the individual in controlling the dissemination and use of information that relates to himself or herself or to have information

---

has been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists" on page 7. David O'Brien's book Privacy, Law, and Public Policy (1979) New York, Praeger Publishers, on p. vii states: "Privacy is a confusing and complicated idea." Despite the lack of consensus among social scientists and philosophers on the meaning of privacy Colin J. Bennett in Regulating Privacy: Data Protection and Public Policy in Europe and the United States (1992) highlights common themes as the loss of human dignity, autonomy or respect that occurs form a loss of control over personal information, p.26.

[9]Paul Sieghart (1976). Privacy and Computers. London, Latimer New Dimensions, p. 13. See Priscilla M. Regan's (1995) Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill, The University of North Carolina Press. Regan observes that the difficulties in conceptualizing privacy may present problems for policy formulation and legislating the protection of privacy.

[10]Colin J. Bennett (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States. p.13.

[11]Institute of Medicine (1994). Health Data in the Information Age: Use, Disclosure and Privacy. Edited by Molla S. Donaldson and Kathleen N. Lohr. Washington, D.C., National Academy Press, p.143.

about oneself be inaccessible to others."[12] Claims to privacy include the right to control the circulation of personal information that is collected and stored. This claim commonly referred to as information privacy or data protection is the basis for the study.

Alan F. Westin provides a classical definition of "information privacy" as: "The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[13] Westin refers to privacy as a claim, not a right. This implies privacy is important but not absolute. Arthur M. Miller's definition is even more concise "...the individual's ability to control the circulation of information relating to him."[14] Charles Fried claims privacy is "the control we have over information about ourselves."[15] The information control definitions are cited extensively by other scholars and have survived the criticisms of J. McCloskey, L. Lusky and R. Parker. These authors argue that the definitions are either too broad or too narrow.[16] The issue of information privacy did emerge in the 1960s largely as a result of growing demand for personal information. A definitional approach to privacy as "control over personal information" has widespread acceptance in many western democracies. David M. O'Brien explains why this approach is appealing. "...[I]t embraces a broad range of privacy interests; it appears appropriate and applicable to the problems associated with personal information held by government agencies; and, finally, it lends itself to normative arguments for

[12]Ibid. p.143 cited Westin's (1967) Privacy and Freedom.

[13]Alan F. Westin (1967). Privacy and Freedom. p.7.

[14]Arthur M. Miller (1971). The Assault on Privacy: Computers, Data Banks, and Dossiers. Ann Arbor, The University of Michigan Press, 1971, p.25.

[15]David M. O'Brien (1979). Privacy, Law, and Public Policy on p.11 cites Charles Fried in An Anatomy of Values. Cambridge, Mass.: Harvard University Press, 1970. The social commentary in Westin's Privacy and Freedom, Miller's Assault and Privacy and Fried's An Anatomy of Values focused increasing attention on the new technologies (especially computerized and centralized databases) and its implications for privacy.

[16]Arthur Schafer (1980). "Privacy: A Philosophical Overview." In Aspects of Privacy Law: Essays in Honour of John M. Sharp. Edited by Dale Gibson. Toronto, Butterworth & Co. (Canada) Ltd., pp. 9-11.

legislating privacy safeguards."[17] The health field is especially vulnerable since individuals provide very intimate details about themselves and want to control disclosure and use of the information. The focus of this study is "information privacy" and the control individuals have over the collection, storage and dissemination of personal information.

Privacy and Confidentiality

A review of the health literature suggests that the use of the terms "privacy" and "confidentiality" are interchangeable. A clear distinction, however, does exist between a right to confidentiality and a right to privacy. Confidentiality arises in a situation where the individual provides information to another and expects that it will be kept confidential and not disclosed to third parties.[18] Jean V. McHale states: "The person who imparts the information binds the recipient by an obligation of confidentiality."[19] On the other hand, the issues of privacy may arise "...whether or not we regard the information as confidential."[20] Privacy is a broader concept than confidentiality. McHale distinguishes the terms quite clearly: "The right to privacy relates to the right of the individual to control access to his own personal information, and this does not simply cover information which he has passed on to others expressly or impliedly expecting them to keep it in confidence. It applies to all personal information."[21] Information of a confidential nature has been protected within the medical relationship for decades and is considered worthy of protection. There are layers of personal information that are not considered confidential but are worthy of protection. Privacy protection legislation applies only to personal information. Personal information is defined as "information about an identifiable individual that is recorded in any form" and includes

[17]David M. O'Brien (1979). Privacy, Law and Public Policy, p.13.

[18]Jean V. McHale (1993). Medical Confidentiality and Legal Privilege. New York, Routledge. p.56.

[19]Ibid. p.56

[20]Ibid., p.56.

[21]Ibid., p.56.

information such as the name, address, telephone number, race, origin, color, political or religious beliefs, age, sex, sexual orientation, marital or family status and any identifying number, symbol or other particular assigned to an individual. Information relating to genetics such as fingerprints or blood type, and personal history regarding an individual's education, finances, health, criminal or employment history; and their personal views or the views of others about them are included in the definition of personal information.[22] The majority of privacy legislation in North America indicates that personal information must be recorded and relate to an identifiable individual. A privacy and access to information statute will provide individuals with some control over personal information. By restricting the collection, use and disclosure of personal information and allowing access to and correction of records held by institutions; the control over information or information privacy advances.

The Value of Privacy

Western societies in general consider the right to privacy an important value that has legal and moral protection.[23] It is not an absolute value and can be overridden by other values. A number of explanations in the literature describe the importance given to privacy. A dominant theme originating to John Stuart Mill is the utilitarian argument for privacy. According to Arthur Schafer, the liberal arguments by Mill advanced "...the psychological, sociological and political utility of individual privacy."[24] Priscilla M. Regan writes about privacy in American history and suggests that: "Its roots go back to England, as reflected in the political thinking of Thomas

[22]British Columbia, Ministry of Government Services (1995). Information and Privacy Handbook: An Interpretive Guide to the Freedom of Information and Protection of Privacy Act. Second edition. Prepared and published by Interact Public Policy Consultants, Vancouver. See Erin Shaw, John, Westwood and Wodell Russell (1994). The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. Prepared for the B.C. Civil Liberties Association and B.C. Freedom of Information and Privacy Association, Vancouver, p.10. The authors note that this definition of personal information has been included in privacy legislation of various Canadian jurisdictions.

[23]Arthur Schafer (1980). "Privacy: A Philosophical Overview." p.14.

[24]Ibid. p 15.

Hobbes and John Locke and the form of liberal democratic government that derived from that thinking."[25] Westin argues that privacy is necessary for individuals or groups to deal with the social stresses of life since it allows opportunities to escape.[26] Fried notes that privacy helps in the development of relationships and is a necessary element of "love, trust, friendship, respect and self-respect."[27] According to James Rachels privacy is essential to control accessibility and inaccessibility to ourselves and allows different types of relationships to develop.[28] Stanley Benn, a philosopher, examines privacy from a non-utilitarian perspective and identifies some of the intrinsic values of privacy, including respect for persons and self-consciousness experienced by humans.[29] Social scientists Paul Halmos, Philip Slater and Edmund Leach describe privacy as a negative value in liberal society. The authors espouse the view that too much privacy may lead to isolation, alienation and anti-social behaviour. In summary these authors claim that; "...an excessive emphasis on the value of privacy produces social pathology rather than social health."[30] Regan explains the social significance of privacy and its importance. "...[I]ndividuals share common perceptions about the importance and meaning of privacy, because it serves as a restraint on how organizations use their power, and because privacy - or the lack of privacy - is built into systems and organizational practices and procedures."[31] The diverse views expressed in the literature reflect the legal, philosophical, political and socio-cultural understanding of the value of privacy.

---

[25]Priscilla M. Regan (1995). Legislating Privacy: Technology, Social Values, and Public Policy. p.43

[26]Arthur Schafer (1980). "Privacy: A Philosophical Overview" cites Alan Westin's Privacy and Freedom on p.15.

[27]Ibid. p. 15. Schafer cites Charles Fried in An Anatomy of Values. Cambridge, Mass.: Harvard University Press, 1970.

[28]Ibid. p.15. Schafer cites James Rachels.

[29]Ibid. p.18. Schafer cites Stanley Benn.

[30]Ibid. p.19. Within the social sciences there has been strong arguments against attaching too much importance on privacy. Schafer observes that a "number of Western social scientists have argued that privacy has become an unhealthy obsession of comtemporary liberal society." p.18.

[31]Priscilla M. Regan (1995) Legislating Privacy: Technology, Social Values, and Public Policy. p.23.

Privacy and Liberal Democracy

The theory of information privacy has its roots in classical liberal doctrine of "human rights, limited government, the rule of law, and a separation between the realms of state and civil society."[32] Bennett asserts: "Privacy is not a precondition of "democracy"...[as such] but of a particular type of democracy - one that is individualistic, possessive, and non-communitarian, rather than participatory and communitarian."[33] One proponent, Westin, articulates the view that privacy is a prerequisite for liberal democracy.[34] Kenneth Kernaghan and John W. Langford describe why privacy is important in the liberal democratic state. "Within our liberal democratic state, individual privacy is seen as an essential ingredient in the exercise of free political choice, the maintenance of family life, and the enhancement of individual creativity."[35] The view espoused by Westin represents a pluralistic approach to democratic theory. Bennett refers to criticisms made of this perspective by those who contend that other democratic values such as "cooperation, community consciousness and active participation" are equally important in postindustrial society.[36] Both authors agree that privacy is not a precondition of democracy and the theory of information privacy is closely linked to John Locke as opposed to Jean Jacques Rousseau. Rousseau believed that: "The central test of democracy is participation, not the existence of constitutional rules protecting individual rights or the degree of competition between centres of power."[37] Westin and Bennett believe that balancing individual and group privacy and limiting

[32]Colin J. Bennett. "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." Science, Technology, & Human Values. Vol. 16, No. 1 (Winter 1991), p.59.

[33]Ibid. p.60.

[34]Alan F. Westin (1967). Privacy and Freedom, pp.24-24.

[35]Kenneth Kernaghan and John W. Langford (1990). The Responsible Public Servant. Halifax, The Institute for Research on Public Policy. p.104.

[36]Colin J. Bennett (1992). Regulating Privacy, p.35.

[37]Ibid. p.33.

the disclosure of personal information and surveillance are necessary in a liberal democratic society.[38]

One basic element of pluralist theory is that politics in a liberal-democratic society is a competitive process among groups with widely distributed powers. From a pluralist perspective; "...privacy bolsters the boundaries between competing, countervailing, overlapping centers of power."[39] The pluralist approach may be instrumental in explaining the emergence of data protection issues on the political agenda of several democracies. Governments are not neutral players but promote and defend their own interests. The bureaucracy will compete to protect its size, budgets, programs and responsibilities. Individuals and groups strive to maintain control over personal information to avoid the loss of human dignity, autonomy, or respect. As Bennett puts it: "The individual has an interest in ensuring that his or her information is accurate, relevant, and timely; that it is being utilized by those with authorization; and that it is not communicated beyond those who 'need to know'."[40] A number of examples in the privacy literature, most notably by American commentators, describe the use of personal information to deny governmental services or to discriminate against individuals. Governments, bureaucrats, and citizens require some degree of privacy to promote individual and often conflicting interests.

The Rise and Fall of Privacy

Arthur Schafer describes a number of long-term trends in society that have enhanced individual privacy.[41] The move away from closely knit rural communities increased the psychological and physical space between members. Community bonds and moral norms weakened as individualism

[38]Ibid. p.3.

[39]Ibid. p.60.

[40]Ibid. p.34.

[41]Arthur Schafer (1980). "Privacy: A Philosophical Overview." p.2.

was pursued. "The cumulative effect of these social developments has been to provide increased scope for anonymity, personal non-conformity, and, in general enhancement of the ethos of individual privacy."[42] Schafer asserts that a number of countervailing historical trends has been more powerful than the societal changes. First, environmental factors led to high population density neighbourhoods. Second, business factors encouraged the use of credit and the need for credit ratings, as well as door-to-door and telephone solicitation. Third, technological developments such as computers permit monitoring and surveillance by government and business. "The massive amounts of personal data which these new techniques have generated can now be stored, organized and disseminated in computer-usable form. One result of this has been that otherwise harmless (because scattered) data becomes threateningly transformed into comprehensive dossiers."[43] According to Schafer the increase in the bureacratic organization of social institutions, particularly by governments, made surveillance techniques appear inevitable and desirable. "Even if this information is not actually used/misused to harass or injure, the loss of "informational privacy" can have a profoundly inhibiting effect on people."[44] The writings of Paul Sieghart on the impact of computers, suggest the control over information will be lost as the nature of communication changes.

> More transactions will tend to be recorded; the records will tend to be kept longer; information will tend to be given to more people; more data will tend to be transmitted over public communication channels; fewer people will know what is happening to the data; the data will tend to be more easily accessible; and data can be manipulated, combined, correlated, associated and analysed to yield information which could not have been obtained without the use of computers.[45]

Modern information systems enhance our ability to link data and to share information across time and space. Fourth, the developments in mass media through "commercialization and

[42]Ibid. p.2.

[43]Ibid. p.3.

[44]Ibid. p.4.

[45]Paul Sieghart (1976). Privacy and Computers, pp. 75-76.

sensationalism" have reduced individual privacy.[46] All of these trends described by Schafer have led to a decline in privacy in the postindustrial society. Privacy may decline even further with the growing need for information and the technological imperatives that have become an integral part of the information society. This thesis will examine many of the issues discussed above within the context of British Columbia's recent FOIPP Act. The approach taken in this research is outlined below.

Methodology

Information was collected from a variety of sources including; government and non-government reports, discussion papers, the FOIPP Act and accompanying manuals, parliamentary debates, policy and procedure manuals, academic books, theses, journals, legal cases, statutes, surveys, conference proceedings and newspaper articles. Other sources included personal and telephone interviews with a member of the British Columbia Legislative Assembly, a public interest group, hospitals, self-governing professional bodies and the Information and Privacy Commissioner of British Columbia. Participants from hospitals and self-governing professional bodies received copies of the interview notes and provided signed letters of acknowledgment. Permission to use the information for this thesis was obtained.

The chapters are organized to reflect a number of political, social, economic and technological factors that are changing the public policy environment. These factors include, citizen demands for greater government accountability and the courts' protection of rights; the patient rights movement in North America; the use of information technology to control costs and curb abuses of publicly funded programs; and the rise in policy advocacy. Chapter II focuses broadly on the protection of privacy in North America. The origin of public concerns about privacy is traced to the 1960s as public bureaucracies collected increasing amounts of information from citizens. The expansion of the welfare state required individuals to provide detailed records to receive benefits and services.

[46]Arthur Schafer (1980). "Privacy: A Philosophical Overview", pp. 2-3.

The introduction of computerization increased the possibilities and opportunities to collect and store large quantities of information. Several western democracies enacted data protection policies to regulate the collection, use and disclosure of information and to hold the bureaucracy accountable for its information handling practices. Canadian policy-makers studying data protection policies drew on the experiences abroad, in particular the United States Privacy Act of 1974 and the OECD Guidelines. A comparative analysis of the privacy legislation in the United States and Canada points to major differences between the two political systems. In 1992, the government of British Columbia enacted the Freedom of Information and Protection of Privacy (FOIPP) Act. The provincial legislation differs in a number of ways from the federal Privacy Act. The courts have begun to recognize the right to access personal information and the Canadian Charter of Rights and Freedoms is judicially interpreted to recognize privacy interests.

Chapter III considers challenges to information control in the health care system. A number of perspectives describing the changing nature of the physician-patient relationship and the physician's control over information illustrate the socio-cultural transformations within the health sector. Recent literature suggests patients are beginning to reject the dominance of the medical profession and demanding access to health records. The flow and exchange of information increase with the rise in health care consumerism as patients visit more specialists, health care professionals and paraprofessionals. From a health researcher's perspective the impact of increasing privacy protection may be detrimental to society. The necessary cost of health research may inevitably be a loss of privacy. Others would argue that the cost is too high. Public institutions providing third party payments require certain types of information for administrative purposes. The utilization of health information for non-medical and social purposes is troubling to privacy advocates. The protection of privacy and confidentiality of personal health information may be threatened as the quantity of health records increase and become available to multiply users. Some of the issues involving the protection of health information include confidentiality, privacy, disclosure, privilege, access and ownership of health records. In British Columbia, a number of events involving the

inadequate storage and disposal of patient records in the province illustrate weaknesses of information protection practices in the health sector.

Chapter IV investigates the relationship between bureaucracy, information technology and the citizen. The increasing role of the bureaucracy and proliferation of information technologies in the health field raises some concerns about the collection, use and disclosure of personal health information. Policy-makers today must balance the needs of public institutions or provincially regulated bodies to collect and use information with the citizen's rights to privacy. Ministry of Health officials across Canada promote various technologies that will increase administrative efficiency. Health information management is becoming an integral part of the health care system. The application or promotion of various types of information technologies grows steadily as economic pressures to reduce expenditures in health care continue. The recent implementation of the Pharmanet Information System in British Columbia for example, will contain the prescription drug history of the entire province. Pharmanet is scrutinized by advocates and public interest groups who are concerned about the privacy implications.

Chapter V examines the policy literature on the issues dealing with privacy protection and the various interests participating in these discussions. In British Columbia, similar to other western societies there is an increasing political will among individuals, groups and organizations to examine potential threats to privacy. A policy community involving public interest associations, academics, advocates and citizens are striving to influence government policy on access to information and privacy protection issues. The British Columbia Civil Liberties Association (BCCLA) and the British Columbia Freedom of Information and Privacy Association (FIPA) represent two organizations that actively promote freedom of information and privacy rights. Privacy advocates, civil libertarians and citizens continue to express concerns over data protection as more creative ways to collect, store and share information develop. Members of the policy community are making increasing demands for government accountability and responsiveness to

issues on privacy. Many individuals, groups and organizations support the rights to access personal health records and patient privacy. Health sector organizations such as hospitals and self-governing professional bodies like the College of Physicians and Surgeons and College of Pharmacists are trying to effectively administer the FOIPP Act. Some organizations describe how the legislation pose challenges as a result of limited resources and time constraints. The protection of privacy represents an important public policy issue that concerns many individuals, groups and organizations in British Columbia.

Chapter II - The Protection of Privacy

"Information privacy" is a concept which refers to the ability to control the circulation of personal information and as such, is an important value in western societies. In Chapter I it was noted that the bureaucracy's use of technology to store, organize and disseminate personal data is one trend that has led to a decline in privacy. Privacy or the lack of privacy has become a public concern in post-industrial societies. Priscilla M. Regan suggests: "The idea of privacy is symbolically relevant and politically important."[1] This chapter examines some of the concerns posed by the bureaucratic use of information technology and the response by the governments of the United States, Canada and British Columbia. An analysis of the models of data protection policies offers some insight on the different systems of government, the power and influence of the bureaucracy, and the role of special interest groups. A central theme that emerges in the discussion below is that Canada and British Columbia drew from the experiences in other jurisdictions. The Council of Organization for Economic Co-operation and Development (OECD) Guidelines on fair information practices were instrumental in the development of Canadian data protection legislation. In the formulation of policy both governments were critical of different models of data protection policies and were selective in their choice of policy instrument. The United States' self-regulatory model of data protection differs from Canada's ombudsman or advisory model. The model in British Columbia represents a variation of the Canadian model, with greater emphasis on regulation and less reliance on an ombudsman role. Policy-makers in British Columbia identified the need for stronger data protection regulation at the provincial level and rejected an advisory role for its data protection agency. An examination of the American constitutional right to privacy and the Supreme Court of Canada's recognition of privacy interests highlights the increasing role of the judiciary in protecting privacy. The impetus for data protection policies can be traced to the 1960s when public concern over the large scale collection of personal information by public

[1]Priscilla M. Regan. "Ideas or Interests: Privacy in Electronic Communications." Policy Studies Journal, Vol. 21, No. 3 (1993), p. 451.

bureaucracies grew. By the early 1970s, the focus was on computerization in government organizations, in particular the use of databases.

In the 1960s, several advanced industrial societies were concerned with the protection of information privacy. The vast quantity of literature originating from the late 1960s to early 1970s serves to illustrate the growing attention to privacy protection. Information privacy or data protection issues surfaced on the political agenda in several western democracies. The development of the welfare state and the requirement for the collection of large amounts of personal information lent support for the regulation of administrative use of information. Some commentators suggest that claims to privacy became insistent in our post-industrial society.[2] "Postindustrialism" a word coined in the late 1960s was at the center of the scholarly debate on data protection.[3] Two elements of post-industrial society; bureaucracy and information technology, were influential in the development of data protection legislation. The growing pressures for legislative action were directly related to the bureaucratic use of personal data and the expansion of information technology in government administration. Policies to protect personal information, promote bureaucratic accountability and to regulate governments' information practices were seen as critical. In response to concerns about privacy seventeen democracies enacted data protection laws as shown in Table 2.1.

---

[2]Canada, Task Force established jointly by the Department of Communications/Department of Justice (1972). Privacy and Computers. Ottawa, Information Canada. p.126.

[3]Colin J. Bennett. Regulating Privacy: Data Protection and Public Policy in Europe and the United States (1992), p.51.

Table 2.1 Data Protection Legislation in Postindustrial Countries		
OECD Countries	**Data Protection Legislation**	**Date**
Sweden	Data Act	1973/82
United States	Privacy Act	1974
West Germany	Data Protection Act	1977
Canada	Privacy Act	1977/82
France	Law on Informatics & Liberties	1978
Norway	Personal Data Registrars Act	1978
Denmark	Private Registrars Act	1978
Austria	Data Protection Act	1978
Luxembourg	Data Protection Act	1979
Iceland	Act on the Systematic Recording of Personal Data	1981
New Zealand	Official Information Act	1982
United Kingdom	Data Protection Act	1984
Finland	Personal Data File Act	1987
Ireland	Data Protection Act	1988
Australia	Privacy Act	1988
Japan	Personal Data Protection Act	1988
The Netherlands	Data Protection Act	1988
Source: Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (1992): 57		

Bureaucracy and Information Technology

The move towards industrialization led to an expansion in the state's function and responsibilities. The growing provision of social and health services required more formal, discriminating and complex record-keeping systems. Colin J. Bennett suggests "the relationship between citizen and state assumed all the formalized, routine, institutionalized, and impersonal characteristics that we come to associate with bureaucracy."[4] Before computerization the bureaucracy was responsible for the collection of information for administrative, investigative and statistical purposes. The new technologies expanded the opportunities available to pursue these goals. Bennett describes how information technology "...can relieve officials of tedious tasks such as copying, filing;...it makes for more speed and efficiency in dealing with the public; it enhances the analytical capabilities of an organization; it helps rationalize administrative work; and it supposedly enable more accurate

[4]Ibid. p.19. Bennett cites H. H. Gerth and C. Wright Mills, from Max Weber: Essays in Sociology, New York, Oxford University Press, 1946, pp. 196-244.

and fine-drawn decisions concerning clients and customers."[5] Individually, bureaucracy and information technology did not create the problems associated with information privacy.[6] It was the interactive relationship between the two elements that spurred the debate on the national and international scene. "Before the computer arrived, there was no data protection movement, though there was bureaucracy and a privacy issue (confined to questions of surveillance and physical intrusiveness). Information technology was the catalyst that generated the policy problem."[7] Alan F. Westin as well as other analysts agree that the development in information technology did contribute to the emerging policy debate beginning in the 1960s.

Comparative studies by David H. Flaherty and Bennett, suggest that a common perception of the "privacy problem" in several nations led to the adoption of a variety of data protection policies. The movement of data protection from the systemic to the institutional agenda was the result of four factors: "...specific plans for the centralization of population data in governmental agencies; the accompanying proposal for personal identification numbers; the occurrence of decennial censuses in many countries around 1970; and a spate of alarmist publications."[8] Each factor led to increased concerns about information privacy, although centralized and computerized population data banks spurred the greatest anxiety in several countries. Centralization of personal record-keeping systems heightened the privacy debate internationally. Beginning in 1968, Americans became fearful about the potential for surveillance and social control with the establishment of a register that contained the tax information of the entire population.[9] The issue of information privacy and its protection rose to the political agenda as the application of computers in government "presented new relationships and different policy problems, ones that the courts were

[5]Ibid. p.20.

[6]Ibid. p.20.

[7]Ibid. p.118.

[8]Ibid. p. 46.

[9]Ibid. p.46.

unable to resolve" in the United States.[10] Moreover, it was the abuse of power demonstrated by the Watergate scandal that captivated and held the attention of the press, public and privacy advocates. Bennett argues that: "The Privacy Act would not have been passed in 1974 had it not been for Watergate. Its enactment was seen as part of a wider effort to open up the executive establishment and cleanse the government of the murky and conspiratorial influences of the Nixon White House."[11] The incentive for policy-makers to address data protection issues was strong due to the political pressures for increased government accountability.

The tendency of bureaucracies to maintain control over information is well-known and documented. This tendency was "checked" somewhat by legislation introduced in countries such as United States, Sweden, The Federal Republic of Germany, France, the United Kingdom and Canada. In essence, data protection policy's "target group is mainly the bureaucracy, and its "impact" is defined and evaluated in terms of reducing bureaucratic power."[12] Flaherty observes how "...aspiring bureaucrats are constantly inventing new ways to use existing data for other administrative purposes, whether to enforce an agency's mandate, to respond to new governmental or legislative directives, or for law enforcement."[13] Regan draws similar conclusions about the American experience. Regan describes how federal agencies began to use new computers and telecommunications to advance the efficiency of government record-keeping; to detect and prevent fraud, waste, and abuse; and to conduct law enforcement investigations.[14] According to Bennett; "The policy response to the "privacy" problem among advanced democratic states has been to enact

---

[10]Ibid. p.67.

[11]Ibid. p.72.

[12]Ibid. p.208.

[13]David H. Flaherty (1989). Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States. London, The University of North Carolina. p.1.

[14]Priscilla M. Regan. "Privacy, Government Information, and Technology." Public Administration Review, Vol. 46, No. 6 (November/December 1986), p. 630.

data protection laws."[15] Data protection agencies promote bureaucratic accountability and monitor the information collection initiatives of officials in several countries.

The literature on computerization and government databanks refers to the collection and storage of large quantities of personal data as the catalyst to the privacy debate.[16] In Britain and the United States proposals to centralize computer information systems met with resistance and controversy. In attempts to promote liberal democratic values such as individual autonomy and limits to government, Britain and the United States identified: "The need for policy to protect personal information and prevent bureaucratic misuse of that information."[17] Regan argues that bureaucracies have a vested interest in personal information that may account for privacy invasions. "As bureaucracies recognize the significance of personal information both as essential to their own internal operations and as a resource in the external environment, they will seek to protect or increase their information capabilities."[18] Bureaucrats do enjoy some degree of autonomy in making decisions. Information is a valuable resource that adds to bureaucratic autonomy. The American experience with data protection policies and the resistance towards an independent regulatory agency highlight the bureaucracy's desire to maintain independence.

---

[15]Colin J. Bennett. "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." Science, Technology, & Human Values, Vol. 16, No. 1 (Winter 1991), p.50.

[16]The works of authors such as Alan F. Westin (1967), Arthur M. Miller (1971) and Paul Sieghart (1976) highlight this point. James Rule, Douglas MacAdam, Linda Stearns, David Uglow also comment on the privacy concerns that arose from the use of government databanks in The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York, Elsevier, 1980.

[17]Priscilla M. Regan. "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations." Journal of Public Policy, Vol. 4, Part 1 (February 1984). p.19.

[18]Ibid. p.23.

The Protection of Privacy

The United States

The development of data protection policies in the United States rests on the assumption that individuals have an interest in protecting their own privacy. The unique experience of the United States and the recognition of a "right to privacy" is traced to an influential article written in 1890 by Samuel Warren and Louis Brandeis. The Warren and Brandeis article, *The Right to Privacy* first appeared in the Harvard Law Review.[19] The subject of privacy has since captured the interest and attention of legislative bodies and courts. One year earlier Judge Thomas M. Cooley wrote in *A Treatise on the Law of Torts* the original definition of privacy as "the right to be let alone."[20] The Warren and Brandeis article is a source of reference for court decisions and opinions dealing with a right to privacy in the United States since the 1890s. The American courts have since developed a considerable body of law relating to privacy. This is noteworthy in comparison to the Canadian experience. Historically, Canadians generally, have not relied heavily on the judiciary to protect privacy interests. Judicial conservatism was an important factor. The United States has long relied on the judicial process to resolve privacy issues. The right to privacy in America has the protection of common law, the Constitution and beginning in 1974, data protection legislation.

In 1965, privacy achieved the status of a constitutional right in the United States. The term privacy does not appear in the U.S. Constitution. The Supreme Court in Griswold v. Connecticut concluded that constitutional guarantees in the First, Third, Fourth, Fifth and Ninth Amendments

---

[19]Samuel Warren and Louis Brandeis. "The Right to Privacy." Harvard Law Review, 4 (1890), 193-220. Richard F. Hixson writes that as early as 1886 the US Supreme Court four years before the Warren and Brandeis Article in Boyd v. United States enforced the protection of private activities using the Bill of Rights. The Court held in Boyd v. United States that federal subpoenas for certain business records violated the due process clauses of the Fourth and Fifth Amendments. Hixson adds that "with this, privacy won a permanent place in American jurisprudence." See Richard F. Hixson (1987). Privacy in a Public Society: Human Rights in Conflict. New York, Oxford University Press, p.71.

[20]Colin J. Bennett (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States cites on p.66 Thomas M. Cooley (1888). A Treatise on the Law of Torts, 2nd ed. Chicago, Callaghan, p.29.

create "zones of privacy."[21] In this case the Court struck down a state law that prohibited the use of contraceptive devices. Furthermore, by the 1960s, the expansion of computerization in government organizations created concerns about traditional constitutional balances and threats to basic liberties.[22] Social commentators warned of the dangers associated with massive information systems that would "...enhance the power of executive over legislatures; make federal Washington master over the states; diminish authority and effectiveness of the courts; and promote the creation of elaborate computer data banks that would threaten privacy, due process and dissent."[23] During the 1960s and 1970s numerous books, studies and commission investigations on computers were appearing in several democracies. As noted earlier, the Watergate scandal is one plausible explanation for the enactment of national privacy laws in the United States. The scandal led to the enactment of federal and state privacy legislation from the mid-1970s to the present.

The United States Privacy Act of 1974 protects personal information held in government records. The Act requires the government to report all information files, ensure the quality of information, provide access to the individual's personal files, and to use the data only for the purpose in which it was collected. The Act provides a record of disclosure to individuals affected by the release of information. "It covers federal and state government files in general; consumer reporting for credit, insurance and employment, individual bank and financial record, patient medical and health records; education records, and records in a variety of other fields."[24] The Act is self-enforcing

[21]Ibid. p.66. Also see Richard F. Hixson (1987). Privacy in a Public Society: Human Rights in Conflict. New York, Oxford University Press. The First Amendment addresses freedom of religion, speech and the press, peaceful assembly and association. The Third Amendment protects the intimacy of private dwellings. The Fourth Amendment limits searches, seizures and arrests. The Fifth Amendment alludes to privacy in terms of self-incrimination and due process. The Fourteenth Amendment addresses the security of the persons, houses, papers and effects. The constitution protects one's body from assault, private places from trespass and personal property from theft.

[22]Alan F. Westin. "Civil Liberties in the Technology Age: Safeguarding the Framers' Guarantees Requires a Vigilant Congress and a Watchful Citizenry." Constitution, Vol. 3, No. 1 (Winter 1991), p.56.

[23]Ibid. p.56.

[24]Ibid. p.60.

and did not create an independent authority to address privacy issues. Regan explains the government's rationale:

> A regulatory agency with authority to overrule a bureaucracy's decision to collect certain categories of personal information or to exchange personal information with another bureaucracy would significantly curtail the autonomy and discretion of bureaucracies. This implementation framework imposes costs on a bureaucracy, in requiring accountability both to the independent agency and to individuals.[25]

The establishment of a regulatory body to monitor information collection practices would have severely limited the independence and power of the bureaucracy.

In the United States, the bureaucracy's opposition to the creation of an independent regulatory agency was extensive. After lengthy debates, the U.S. Privacy Protection Commission was established with investigative and advisory responsibilities. A regulatory or ombudsman agency was rejected based on the argument it would create "...a more 'adversarial posture' not needed at this time."[26] President Gerald Ford, in support of the bureaucracy, challenged the need for a separate Commission or Board.[27] The Office of Management and Budget (OMB), an existing federal agency was given the responsibility to oversee and implement the Privacy Act. Regan highlights three weaknesses of the Privacy Act.[28] First, the Act requires individuals to protect their own interests. Second, the enforcement scheme provides remedies only after abuses have taken place. Third, the legislation was insensitive to the existing power imbalance between individuals and federal agencies. The individual's interest in privacy is placed in opposition to the information requirements of public agencies. The client's dependency on an agency for benefits places the individual at a disadvantage. The United States, Freedom of Information Act (FOIA)

---

[25]Priscilla M. Regan. "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations." Journal of Public Policy, Vol. 4, Part 1 (February 1984), pp. 23-24.

[26]Ibid. p.29.

[27]Ibid. pp. 24-34. Regan provides an excellent summary on the policy debates at the Committee Hearings on the establishment of an independent regulatory agency and the final decision.

[28]Priscilla M. Regan. "Privacy, Government Information and Technology." Public Administration Review, Vol. 46, No. 6 (November/December 1986), p.633.

was enacted by Congress in 1966 and in 1974 was strengthened to provide wide access rights to individuals. In the 1980s, a number of federal laws were enacted which addressed the use of technology by federal agencies.

The Electronic Communication Privacy Act of 1986 and the Computer Matching and Privacy Protection Act of 1988 followed the initial development of privacy legislation in the United States. Westin writes that the new pieces of legislation were not the product of technological innovation by government agencies implementing computer systems. Instead the new statutes were "...perceived as critical, publicized as necessary and fought for in the political trenches by ad hoc coalitions of interest groups that have been "citizen's lobby" on privacy and due process protections in the computer age."[29] The mobilization of groups in the United States directly affected by computers included consumers, taxpayers, patients, the insured and bank account holders. The result of the data protection movement is that American society today has more privacy protection laws and voluntary organizational privacy rules than ever before. The Federal Privacy Act and state legislations have empowered individuals to examine and challenge their government records by "...allowing private employees access to their personnel files, patients to view their medical records, and consumers to inspect their credit-bureau files."[30] Westin warns that the activities of the courts, legislatures, interest groups, the media and citizenry must continue to protect individual and group rights as governments adopt larger and more integrated records systems. The American experiences with data protection legislation helped to shape and influence the policies of several democracies, including Canada.

The privacy issue with its roots in the United States had a great influence abroad and is evident by the large number of foreign publications referring to the American experience and relying on

[29]Alan F. Westin. "Civil liberties in the Technology Age: Safeguarding the Framers' Guarantees Requires a Vigilant Congress and a Watchful Citizenry." Constitution, Vol. 3, No. 1 (Winter 1991), p.61.

[30]Ibid. p.62.

American commentary, most notably the book written by Alan Westin in 1967 *Privacy and Freedom*.[31] Before 1967, James Rule observes that a privacy policy did not exist in the United States and abroad.[32] The legislative activity since the 1960s in a number of parliamentary democracies was extensive. The development of privacy legislation in Canada did draw on the experience across the border. The American approach was rejected by Canadian policy-makers who favoured a system that would promote ministerial accountability and rely less on the courts. In addition, Canada adopted the guidelines set by the Council of Organization for Economic Co-operation and Development (OECD).

OECD Guidelines

The development of policies to protect and preserve personal privacy is widespread in democratic societies. In 1981, the OECD, published the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" that serves as a minimum standard for members. Canada formally became a signatory member in 1985. The OECD subscribes to the following principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability.[33] The OECD contends that transborder data flow should not circumvent domestic privacy legislation in member countries. In addition, the OECD encourages member countries to adopt "...appropriate domestic legislation; encourage and support self-regulation; provide reasonable means for individuals to exercise their rights; provide adequate sanctions; and ensure that there is no unfair discrimination against data subjects."[34] The guidelines were influential in the development of Canadian federal legislation dealing with information management and privacy protection.

---

[31]James Rule et al. (1980) The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. p.112.

[32]Ibid. p.111.

[33]Organization for Economic Co-operation and Development (OECD). Guidelines on the Protection of Privacy and Transborder Flow of Personal Data. Paris, OECD, 1981, pp. 10-11.

[34]Ibid. pp. 10-11.

Canada

Canada, a parliamentary democracy, did inherit the British concept of ministerial accountability and a legacy of restrictive government information availability. In the early 1970s the lobby efforts of political backbenchers, Barry Mather and Gerald Baldwin helped to push forward the federal legislation. The media's attention coupled with the successful experience of the American legislation were pivotal to the enactment of Canada's Privacy Act. The federal government under Pierre Elliott Trudeau introduced Bill C-43 to provide rights to gain access to government information and privacy protection. The Access to Information and Privacy Acts were passed in 1982 and proclaimed into law on July 1, 1983, under one piece of legislation, Bill C-43. The Government's inclusion of privacy provisions in Bill C-43 was to circumvent the use of freedom of information legislation to delve into government records with personal information. The result was a number of exemptions under the general rule of access. The Access to Information Act prohibits disclosure of any file that contains personal information, unless the individual consents or the data is publicly available. The Privacy Act replaced Part IV of the Canadian Human Rights Act of 1977, which included data protection provisions. The new Privacy Act broadens the definition of personal information and includes a number of exemptions. The Act defines personal information as "information about an identifiable individual that is recorded in any form" and includes information relating to an individual's race, religion and marital status; their education, criminal or employment history; their personal views or views of others about them.[35] The review process was extended to include a right of appeal to a court if a federal agency refused to release information. The Act includes the conditions under which disclosures to third parties are permitted. The Privacy Act did not receive as much public attention as the Access to Information Act. The Liberal government's motivation to implement Bill C-43 is unclear, although it appears to be a response to the efforts by lobbyists, broadcasting by the media and the successes of the American legislation. Jill Wallace argues that the initial motivation to introduce legislation was not

[35]Canada. The Privacy Act, Bill C-43. Ottawa, Queen's Press, 1983.

the result of some political will or crisis in Canada.[36] The lobbying efforts of academics, professional groups such as the Canadian Bar Association and the Canadian Institute of Public Administration and public interest groups for freer access to government information were instrumental.[37] The Privacy Act gave Canadians a legislative guarantee that personal information would be protected and addressed principles of fair information practice.

Privacy protection on the national level focuses on the development of fair information practices in government data banks falling under federal jurisdiction. The federal Privacy Act established the right of Canadians to know the existence of personal information files held by federal public bodies and the right to examine, correct and challenge the information. The Act sets out rules and standards for the collection, protection, use and disclosure of personal information. Citizens have the right to know the present and future use of their personal information. The Privacy Act is similar to legislation enacted in Sweden, West Germany and France. Each country's legislation includes five broad principles: "...access to one's own data; access, completeness, and timeliness of recorded information; limitations on information which may be collected; procedures for challenging and correcting erroneous data; and protection of data from unnecessary disclosure."[38] The Access to Information Act, its companion statute is designed to achieve compatibility between information access and privacy. The access to information debate has concerned itself with political accountability and citizen participation in the affairs of government. The Acts created the positions of the Privacy Commissioner and the Information Commissioner with separate responsibilities and mandates. The Privacy Commissioner, an officer of Parliament with quasi-

---

[36]Jill Wallace (1987). "The Canadian Access to Information Act 1982." Public Access to Government-Held Information. Edited by Norman Marsh. London, Stevens & Son Ltd., pp. 123-124.

[37]Ibid. pp.123. Also see the study by Robert Hazell. "Freedom of Information in Australia, Canada and New Zealand." Public Administration, Vol. 67, No. 2 (London) (Summer 1989), p. 210. Hazell agrees that the Canadian Bar Association played an important role in Canada and found that in all three countries studied, the media were strong supporters of the legislation.

[38]James Rule et al. (1980). The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. p.112.

judicial functions has the power to mediate disputes, investigates federal public institutions to ensure compliance and can apply to the Federal Court for a review of government decisions. The Commissioner can only make recommendations and does not have the authority to order federal agencies to conform to standards or to give individuals access to personal information. The Commissioners cannot overturn a decision by the head of an agency. This follows the concept of ministerial responsibility, which states a minister is responsible only to Parliament. Despite the shortcomings of the legislation, federal policy-makers benefited from the experiments of other countries with data protection policies.

The legislative attempts to protect personal data by the United States and several European countries were instrumental in shaping Canadian privacy law. Bennett describes this process as "lesson-drawing" since the experiences abroad were influential in the Canadian policy development stage.[39] The OECD guidelines and the privacy principles in the American legislation with some variation found expression in the Canadian legislation. One explanation is an attempt to "harmonize data protection legislation" in different legal jurisdictions and to comply with international standards.[40] Canada, Britain, France, Sweden, Denmark and West Germany did depart from the influences of America by implementing a variety of privacy-protecting institutions. The Canadian legislation is dissimilar to the United States Privacy Act in a number of ways.

First, the American approach relegated privacy as a secondary value to access. "In the US Freedom of Information Act, a right of access to third-party personal information is granted provided such access does not amount to a 'clearly unwarranted invasion of privacy'."[41] The American Privacy Act states that records that must be open under the Freedom of Information Act

---

[39]Colin J. Bennett. "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing." Canadian Public Administration. Vol. 33, No. 4 (Winter 1990), p.549.

[40]Ibid. p.563.

[41]Ibid. p.564.

are not subject to the provisions of the Privacy Act.[42] The government or the individual whose privacy is being invaded has to demonstrate the invasion is unwarranted. Canadian policy-makers found the American approach "...incoherent, confusing and injurious to legitimate privacy interests."[43] Officials adopted the view that, "...[the] right of access should be set up so that a heavy onus rests upon the applicant to convince the agency concerned that injury to privacy would not result..."[44] The Canadian Privacy Act states that "the head of a government institution may refuse to disclose any personal information requested under subsection 12(1) about an individual other than the individual who made the request." On the other hand, the Canadian Access to Information Act prohibits the disclosure of a record that contains personal information as defined in Section 3 of the Privacy Act. Bennett notes the interrelationship between privacy and access legislation in Canada was due to inconsistencies in the American information law.[45]

A second major departure from the American legislation was the creation of a Privacy Commission, an independent body to oversee privacy protection in Canada. West Germany, France, Sweden and Canada did establish a Commission or Board with some independence from the executive branch of government. The Commission or Board monitors compliance to fair information practices as set out in the data protection legislation of each country. The American

[42]See Richard F. Hickson's book Public in a Public Society. Human Rights in Conflict, p.185 in which he cites one author's explanation of the dilemma facing agency bureaucrats trying to administer the Acts. Frank Rosenfeld's "Freedom of Information Act's Privacy Exemption and the Privacy Act of 1974." 11 Harvard Civil Rights Civil Liberties L.R. 596 (1976) on p. 627 states, "If they refuse to disclose the material they risk being sued by the party who requested the file under the Freedom of Information Act [FOIA]. Under the FOIA the court may award to a successful plaintiff his costs and attorney's fees. If, on the other hand, agencies release material, they risk being sued under the Privacy Act by the person who is the subject of the file. In that case, the plaintiff might win by showing that the file was exempt from disclosure under FOIA. A successful Privacy Act plaintiff can collect not only his costs and attorney's fees but also actual damage sustained because of disclosure." Hixson adds "if the official is going to err in his decision it is less costly to withhold the requested information and risk a suit under the FOIA." p.185.

[43]Colin J. Bennett (1990). "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing." Canadian Public Administration. p.564.

[44]Ibid. p.564.

[45]Ibid. p.565.

Privacy Act did not create an independent body. The OMB, an American federal agency addresses privacy issues and relies on the courts for enforcement. Canadian policy-makers did reject this approach since "simple reliance on the courts...would be inconsistent with Canada's parliamentary traditions."[46] The final decision was a compromise between the American policy of self-enforcement and the bureacratic approach in Sweden and France of a licensing regime. "Lessons from oversees, therefore pointed to a middle approach, a separate policy instrument solely concerned with privacy but relieved of regulatory or licensing responsibilities."[47] Bennett suggests that the concept of a privacy commission was fashionable due to recent establishments of ombudsmen in Canada and was consistent with constitutional norms.[48] Flaherty argues that, "The concept of the Privacy Commissioner as an ombudsman was the product of government thinking...[and]...featured a limited conception of data protection."[49] According to Flaherty an ombudsman role "...is only part of what is necessary for strong data protection."[50] Interestingly enough, the government of British Columbia in 1992 recognized the shortcomings of the federal legislation and was encouraged by a public interest association and academics to adopt a different approach towards privacy protection. The concept of an ombudsman or advisory role for the Provincial Information and Privacy Commissioner was rejected in British Columbia. The Canadian Privacy and Information Commissioners have jurisdiction over records and information in the federal public sector and exercise an ombudsman or advisory role. The Commissioners lack the power to issue binding orders but may take cases to the Federal Court of Canada if agencies fail to comply with their advice. The Canadian Privacy Act has a two-tiered review system in which an individual can forward a complaint to the Commissioner that may be followed by a

[46]Ibid. p.566.

[47]Ibid. p.567.

[48]Ibid. p.567.

[49]David H. Flaherty. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States. pp. 244-245.

[50]Ibid. p.245.

Federal Court review. One problem that has emerged is the inconsistencies in the Court's interpretation of the concept of privacy. In the Privacy Commission's *Annual Report 1993-1994,* for example, the Commissioner describes two cases, *Robert Sutherland and the Minister of Indian and Northern Affairs*, and *The Minister of Finance and Michael A. Dagg* in which the Federal Court applied different interpretations of privacy.[51] The Canadian Privacy Act also created a separate office for the Privacy Commission.

The decision to create a separate Federal Privacy Commission was based on the experiences drawn from the first Privacy Commissioner, Inger Hansen. Hansen found the co-existence of the anti-discrimination provisions of Parts I-III and the privacy provisions of Part IV of the Canadian Human Rights Act, 1977 were awkward and led to conflicts of interest. Part IV of the Act protected personal information contained in federal information banks.[52] In a statement to the Justice and Legal Affairs Committee of the House of Commons, Hansen noted: "As Privacy Commissioner, I could and I have become party to information that would be useful to the Human Rights Commission as a whole and yet I should not and I am not entitled to disclose it."[53] Hansen recommended that the office of the Privacy Commission be given a "separate and legal institutional mandate" and carried weight in the final decision. Today, the Canadian Privacy Commissioner's Office is a separate entity and functions outside the realm of the Human Rights Act. The enactment of the Access to Information and Privacy Acts did create two separate offices, an Office of the Information Commissioner of Canada and the Privacy Commissioner of Canada. The Privacy Commissioner's Office is far removed from the bureaucracy and deals exclusively with

[51]Canada, Privacy Commission. Annual Report 1993-1994. Ottawa, The Privacy Commission of Canada, p.18.

[52]Michael G. Cox (1983). "Personal Access: The Canadian Human Rights Act of 1977 and the Privacy Act of 1982." Canada's New Access Law: Public and Personal Access to Governmental Documents. Edited by Donald C. Rowat. Ottawa, Published by the Department of Political Science, Carleton University, pp. 19-44.

[53]Nanci-Jean Waugh (1983). "A Critique of the Privacy Act." Canada's New Access Law: Public and Personal Access to Governmental Documents. Edited by Donald C. Rowat. p. 48.

privacy issues, although it interacts with the Information Commissioner's Office. The Privacy Act allows individuals to obtain access to information about themselves, and is parallel to the Access to Information Act. The mandatory five year review by the Standing Committee on Justice and Solicitor General in 1987 of the Privacy Act led to the report titled *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. The Committee recommended one hundred and eight reforms to the Federal Act. The recommendations to extend the Act to crown corporations and all public institutions were never implemented by the federal government. The choice of a policy instrument in Canada was largely influenced by the approach adopted in the United States.

Essentially, the development of Canadian privacy law drew from the experiences of other countries. Policy-makers studying the American Privacy Act were able to adapt it "to Canadian circumstances and to avoid what were perceived as the worst flaws."[54] As Flaherty suggests: "The influential U.S. Privacy Act downplayed the importance of having an active agency to promote implementation. Furthermore, rather than rely on the courts to enforce the legislation as the Americans were doing Canadians can use the Commissioner as a mechanism to avoid the courts except as a last resort."[55] The 1981 OECD guidelines helped to shape the principles that are part of the Canadian federal legislation. Privacy legislation in British Columbia has a long history that dates back to 1968 when the courts created a tortious liability for an invasion of privacy. The British Columbia Privacy Act of 1968 failed to protect personal information voluntarily provided to government agencies.

---

[54]Colin J. Bennett (1990). "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing." Canadian Public Administration. p. 569.

[55]David H. Flaherty. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States. pp.246-247.

British Columbia

In 1968, British Columbia passed the Privacy Act and was the first Commonwealth jurisdiction to "establish an independent cause of action for unreasonable and unwarranted invasion of an individual's privacy."[56] Similar legislation was adopted in Manitoba and Saskatchewan. One explanation for the passage of the Act in British Columbia was the result of an incident involving the Pulp and Paper Workers Union of Canada at the Ritz Hotel in Vancouver.[57] In November 1966, the convention hall and the bedrooms of the leaders of the union were bugged by a private detective hired by a rival union, the International Pulp and Sulphate Workers Union. Two R.C.M.P. Officers had referred to the rival union a detective who could provide these services. A Royal Commission of Inquiry into the Invasion of Privacy was appointed following the publicity from this incident. The Report by the Commission recommended "the legislative creation of a civil remedy for invasion of privacy."[58] The Privacy Act of 1968, created two heads of tortious liability, "a general protection of privacy" and "a detailed tort protecting an individual from misappropriation of name or likeness for commercial purposes."[59] Section 2(1) states: "It is a tort, actionable without proof of damage, for a person, willfully and without claim of right, to violate the privacy of another."[60] No definition of privacy was included in the Act.

---

[56] Norman W. Sterling (1984). Discussion Paper on Privacy: Initiatives for 1984. Ontario, Provincial Secretariat for Resources Development, p.12.

[57] Philip H. Osborne (1980). "The Privacy Acts of British Columbia, Manitoba, Saskatchewan." Aspects of Privacy Law: Essays in Honour of John M. Sharp. Edited by Dale Gibson. Toronto, Butterworths & Co. (Canada) Ltd., p.87.

[58] Ibid. p.87. A number of provinces were also concerned with the invasion of privacy. Alberta appointed a Special Committee on Invasion of Privacy and the Ontario Law Reform Commission published a report titled *A Report on the Protection of Privacy*. Refer to Edward H. Humphreys (1980). Privacy in Jeopardy: Student Records in Canada. Toronto, The Ontario Institute for Studies in Education, 1980, p.10.

[59] Ibid. p.87.

[60] Ibid. p.87.

A second explanation for the enactment of privacy legislation by British Columbia and Manitoba in 1970 was that the two provinces had "...decided not to wait for the gradual evolution of doctrines for the protection of privacy by the courts, and...enacted statutes declaring a general right to privacy."[61] In the common law provinces of British Columbia and Manitoba, legislation was enacted to make it a tort to violate privacy since there was no specific common law tort for invasion of privacy. The Federal Task Force on Privacy and Computers notes that up to the 1960s the recognition of "privacy in tort law by the courts has...been sporadic and strictly confined to remedies sought for invasions definable in law in other areas."[62] In addition, the legislative attempts by other countries to protect personal information and the potential threats from modern technology were influential in the development of privacy legislation. Philip H. Osborne describes the rationale for the establishment of a tort for invasion of privacy by three provinces:

> ...the inadequacy of the protection provided by the established heads of tortious liability, judicial conservatism, and a dearth of cases combined with the increasing threats to privacy by modern technology, led the provincial legislatures of British Columbia, Manitoba and Saskatchewan to enact a tort of invading privacy. In deciding the form that this legislation should take, the provinces were guided by legislative experiments in other countries.[63]

Despite the legislative attempt to create a common law tort for the violation of privacy the B.C. Privacy Act had a serious limitation. The Act failed to address the inappropriate or unauthorized use of personal information voluntarily provided to another individual or an institution. Most of the information provided to government agencies are voluntary and concerns had arisen over unauthorized and inappropriate disclosure. In addition, the cost borne by individuals seeking protection through the courts was a disincentive that often outweighed the potential benefits.[64]

---

[61]Canada, Task Force established jointly by the Department of Communications/Department of Justice. Privacy and Computers. Ottawa, Information Canada, 1972, p.139.

[62]Ibid. p.141.

[63]Philip H. Osborne (1980). "The Privacy Acts of British Columbia, Manitoba, Saskatchewan." Aspects of Privacy Law: Essays in Honour of John M. Sharp. p.81.

[64] Norman W. Sterling (1984). Discussion Paper on Privacy: Initiatives for 1984. Ontario, Provincial Secretariat for Resources Development, p.12. Also see Edward H. Humphreys (1980). Privacy in

Freedom of information and privacy bills were introduced unsuccessfully in the British Columbia Legislative Assembly since the 1970s. In 1991, the election campaign by the provincial New Democratic Party (NDP) focused on an "Open Government Initiative" and stressed the need for more open and accountable administration. The window of opportunity to legislate stronger privacy rights and access to information rights was opened up in the province. As one commentator notes the statement by Gerald Baldwin that a good information access law could only be achieved by a "virgin government that hasn't been in power long enough to have lost its virtue" may be applicable to British Columbia.[65]

A Member of the Legislative Assembly for Burnaby North, Barry Jones was elected to the Legislature in 1986 and annually introduced a private member's bill on Freedom of Information. This was not the first government to introduce this type of bill. Beginning in January of 1972, Alex MacDonald introduced Bill 41, cited as the "Sunshine Law, 1972" to the Legislative Assembly. Table 2.2 highlights the history of freedom of information and privacy protection bills introduced in the province. Access to information legislation has been a long standing issue in British Columbia. It has a twenty year history of on-going discussions. In June 1990, the Social Credit Government had introduced an access legislation that was criticized by the media for having too many exemptions and resembling a secrecy law.[66] The NDP during the 1991 election campaign had a platform of open, fair and balanced government. Jones writes that, "...the new administration [in 1991] believed that freedom of information legislation was long overdue, particularly given that British Columbia was one of the last jurisdictions in North America to have

---

Jeopardy: Student Records in Canada, pp. 10-11. Humphreys observes that the B.C Privacy Act of 1968 involved procedures that were cumbersome and expensive.

[65]"Time is ripe for information law", The Vancouver Sun, November, 18, 1991, A12. The late Gerald Baldwin is considered one the architects of Canada' Access to Information and Privacy Acts. He fought long and hard in the 1980s for legislation at the federal level.

[66]"Time is ripe for information law", Vancouver Sun, November 18, 1991, A12.

such a law."[67] Jones points out that the previous administration was secretive and had a "siege mentality."[68] Jones was referring to a land deal by the previous government under Bill Vander Zalm and the administration's refusal to release information that involved public funds. A review of the media coverage during this period illustrates some concerns about government secrecy.[69] According to Jones the principles of information and privacy rights were presented to British Columbians in the 1991 election. The principles "were part of the mandate which the voters approved at the time...[and] is part of the provincial government's Open Government Initiative."[70] A strong supporter of freedom of information legislation Jones argues that it is important to "...open up the processes of government and make it easier for ordinary citizens to participate and influence, the decisions of government...[especially] in an age when citizens are feeling increasingly powerless, cynical, and alienated..."[71] Furthermore, Jones notes the concerns over privacy issues are increasing as: "Technical limitations on the ability of government to collect and store personal information are non-existent. In the absence of technical limitations...we need to create some legislative limits."[72] A data protection legislation for British Columbia was perceived as necessary to limit the bureaucracy's ability to collect personal information with the latest technology. On the other hand, the provisions of freedom of information legislation would encourage citizens to participate in the affairs of government. In 1992, a new piece of legislation was introduced by the NDP Government to provide wider access rights and stronger protection of

[67]Barry Jones (1993). Barry Jones Report: The Extension of Citizens' Information and Privacy Rights to all Public Bodies in British Columbia. Presented to Attorney General, Chair, Cabinet Caucus Committee on Information and Privacy. Victoria, Queen's Printer for British Columbia, p.1.

[68]Personal Interview with Barry Jones, Member of the Legislative Assembly, on January 23, 1996, in Burnaby, B.C.

[69]Media reports suggest the Social Credit Government refused to release reports and disclose information in other cases. See "Veitch declines to disclose amount of warrant request", The Vancouver Sun, March 28, 1991.

[70]Barry Jones (1993). Barry Jones Report: The Extension of Citizens' Information and Privacy Rights to all Public Bodies in British Columbia. p.9.

[71]Ibid. p.5.

[72]Ibid. pp. 5-6.

personal information under the custody of provincial public bodies. In 1993, the broader public sector was included in the Act.

Table 2.2 History - Introduction of B.C. Freedom of Information and Privacy Bills

Year	*Bill #*	*Title*	*Introduced by*	*Debates*
1972 1st session	41	"An act to provide for public scrutiny" - cited as the "Sunshine Law, 1972"	Alex MacDonald, NDP	1st Reading March 9th
1973 1st session	125	"An act to provide for public scrutiny" - cited as the "Sunshine Law, Revisited"	Garde Gardom, Liberal	1st Reading March 9th
1973 2nd session	16	"Public scrutiny" - cited as the "Sunshine Law Again Revisited"	Garde Gardom, Liberal	1st Reading September 19th
1976	33	"Freedom of information act" - cited as the "Macdonald-Gardom Sunshine Act, 1976"	Scott Wallace, Progressive Conservative	1st Reading March 30th
1976	79	"Access to information act" - cited as the "Open Door in Government Act, 1976"	Gordon Gibson, Liberal	1st Reading June 15th
1977 2nd session	M 202	"Freedom of information act" - cited as "MacDonald-Gardom-Wallace Sunshine Act, 1977"	Scott Wallace, Progressive Conservative	1st Reading January 31th Tabled August 4th
1977 2nd session	M 209	"Access to information act"	Gordon Gibson, Liberal Party	1st Reading June 23rd
1980-1986	M 209	"An act establishing the right to public information and the protection of individual privacy"	Eileen Dailly, NDP	May 8th, 1980 June 24th, 1981 June 20th, 1985 May 14th, 1986
1987-1991	M 205	"The freedom of information act"	Barry Jones, NDP	July, 1987 June 9th, 1988 July 13th, 1989 June 11th, 1990 May 13th, 1991
1991	12	"Access to information and protection of privacy bill"	Social Credit Government	Tabled June 24th
1992	50	"Freedom of information and protection of privacy act"	Barry Jones & Colin Gabelmann, NDP	June 18th
1993 2nd session	62	"Freedom of information and protection of privacy amendment act"	Barry Jones & Colin Gabelmann, NDP	June 23rd

Sources: British Columbia. Official Report of Debates of the Legislative Assembly 6476 (May 1, 1989) and Barry Jones Personal Notes "The 'Sunshine bill' and sequels 1972-1979" and "History of Freedom of Information Attempts", March 1996.

The British Columbia Freedom of Information and Protection of Privacy (FOIPP) Act received royal assent on June 30, 1992, to regulate public institutions, and was in force on October 4, 1993. The first phase of the legislation covers provincial bodies, including ministries and crown

corporations, boards, commissions and agencies. This new piece of legislation has wider applications than the federal legislation and its scope is greater than the 1968 Privacy Act. The FOIPP Act (Bill 50) includes access to information and privacy rights under one legislation. In February 1993, Jones made several recommendations to the Attorney General, Colin Gabelmann, to extend information and privacy rights to all public bodies receiving funding by the provincial government or operating under a statute in British Columbia. The British Columbia Freedom of Information and Protection of Privacy Amendment Act (Bill 62) was tabled in the Provincial Legislature on June 23, 1993. On November 1, 1994, public bodies such as municipalities, municipal police forces, school boards, colleges and universities, health and social service agencies and hospitals were included under the second tier of the Act, followed by self-governing professional bodies on November 1, 1995. Jones' decision to amend the FOIPP Act (Bill 50) and to include the broader public sector under one piece of legislation was based on observations made by representatives of other Canadian jurisdictions during consultation.

Before amendments to the FOIPP Act, the province consulted with Ontario to determine whether the local bodies should have a separate piece of legislation. In Ontario there are two acts. The *Freedom of Information and Protection of Privacy Act*, 1987 governs provincial bodies and the *Municipal Freedom of Information and Protection of Privacy Act*, 1989 covers local bodies. A number of representatives from Ontario believed the implementation of two separate Acts were costly and complicated.[73] Rita Reynold, a representative with the Municipality of Metropolitan Toronto stated that the two pieces of legislation "...created significant administrative problems for the municipalities, the province and the public."[74] The experiences of Quebec were referenced, since the province had one act, *the Act respecting access to documents held by public bodies and the protection of personal information* (1987) which included four articles that addressed the specific needs of local institutions. It is important to note that soon after, Quebec's Bill 68, *An act*

[73]Ibid. p.29.

[74]Ibid. p.30.

respecting the protection of personal information in the private sector became law on January 1, 1994. It represents the first statute in North America to develop rules for the private sector's use of personal information. The government of British Columbia drew from the experiences of Ontario and Quebec.

A number of policy options were available to the government of British Columbia including: amendments to Bill 50; regulations to Bill 50; confidentiality provisions in other Acts; and policy guidelines to Bill 50.[75] Three factors led Jones to recommend amendments to Bill 50 rather than the creation of a new piece of legislation to address local needs. The recommendations made to the Attorney General were based on the following factors:

> [T]he problems experienced in Ontario as a result of having a separate Act for local public bodies compared to the successful experience of Quebec; the pre-existing flexibility of British Columbia's provincial legislation (Bill 50) - a flexibility which may be under-estimated by many local public bodies; and the analysis of how every one of the specific concerns raised in local public body submission can be met within the framework of an amended Bill 50.[76]

The government's decision was to amend the existing Act using Bill 62 to address the needs of local bodies. British Columbia represents the only jurisdiction in North America to include self-governing professional bodies in its access to information and protection of privacy legislation. The FOIPP Act's inclusion of local public bodies is consistent with several provinces.

Eleven Canadian governments have some form of freedom of information and privacy legislation. These include: New Brunswick (1978), Newfoundland (1981), Quebec (1987 and in 1994 separate legislation for the private sector), the Federal Government (1982), Manitoba (1985/1986), Yukon (1986, revised in 1992), Ontario (1987 and in 1989 separate legislation for local government), Nova Scotia (1990, revised in 1994), Saskatchewan (1991), British Columbia (1992), Alberta (1994) and the Northwest Territories (1994). Prince Edward Island is the only province without

[75]Ibid. p.31.

[76]Ibid. p.32.

any form of access to information or privacy legislation. In the Federal Privacy Commission's *Annual Report 1994-1995* the Commissioner anticipated the adoption of legislation in Prince Edward Island as early as 1996 following the provincial legislative committee recommendations in 1994.[77] Table 2.3 provides a survey of the various public bodies covered by access to information and privacy legislation in six provinces. The FOIPP Act guarantees British Columbians stronger protection of personal information held by public bodies.

Table 2.3 Survey of Public Body Coverage in Six Provinces

Public Body	Alberta	B.C.	Nova Scotia	Ontario	Quebec	Sask.
Education Sector						
Colleges	yes	yes	yes	yes	yes	yes
School Boards	yes	yes	yes	yes	yes	yes
Universities	yes	yes	yes	no	yes	yes
Health Sector						
Hospitals	yes	yes	yes	no	yes	yes
Law Enforcement						
Police	yes	yes	yes	yes	yes	no
Local Government						
Municipalities	yes	yes	yes	yes	yes	yes
Self-governing Professional Bodies	no	yes	no	no	no	no
Other Local Government Bodies	yes	yes	yes	yes	yes	yes

Legislations:
Alberta, Freedom of Information and Protection of Privacy Act, 1994
British Columbia, Access to Information and Protection of Privacy Act, 1992
Nova Scotia, Freedom of Information and Protection of Privacy Act, 1994
Ontario, Municipal Freedom of Information and Protection of Privacy Act, 1989
Quebec, An Act respecting Access to documents held by public bodies and the Protection of personal information, 1987
Saskatchewan, The Local Authority Freedom of Information and Protection of Privacy Act, 1991

Sources: Barry Jones. Appendices to Barry Jones' Report Extending Freedom of Information and Privacy Rights in British Columbia. (1993):Appendix B and Canada, Privacy Commission. Annual Report 1994-1995. Ottawa, The Privacy Commissioner of Canada, p.24.

[77]Canada, Privacy Commission. Annual Report 1994-1995. Ottawa, Privacy Commissioner of Canada, p.25.

Before the enactment of the FOIPP Act, British Columbians did not have a legislated general right to examine their own personal information, held or used by government; nor the right to request correction of erroneous or inaccurate data. Privacy rights had minimal protection from various branches of law, statutes and government policy. Jones describes the extent of the new legislation: "Any record created by an employee or official of a public body in the course of their duties is a record of that public body and subject to the legislation."[78] The legislative protection of privacy was viewed as essential since it provided individuals' with more control over the collection, storage and use of personal information by government agencies and other institutions. Part Four of the Act established the office and powers of the Information and Privacy Commission. An Information and Privacy Commissioner was appointed by the Lieutenant Governor for a non-renewable six year term and was based on the unanimous recommendation by a Special Committee of the Legislative Assembly.

The British Columbia Information and Privacy Commissioner, an Officer of the Legislature, has the authority to regulate and monitor the information practices of provincial public bodies and organizations that come under the second tier of the legislation. In cases, where a resolution is not reached through negotiation the Commissioner has the power to order any public body to comply with the provisions of the Act. The Commissioner has the legislative authority to "...order the public body to change its policies of collecting, using, and disclosing personal information, to give citizens access to personal information about themselves, and to correct this information at their request."[79] The FOIPP Act differs from the Canadian Privacy Act. The data protection agency created by the Act has wider powers than its federal counterpart. The Federal Privacy Commissioner lacks the power to order agencies of the government to conform to standards or permit individuals access to personal information. The Federal Privacy Commissioner must seek

[78]Barry Jones (1993). Barry Jones Report: The Extension of Citizens' Information and Privacy Rights to all Public Bodies in British Columbia.

[79]Erin Shaw et al. (1994). The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. p.15.

redress through the courts, which entail substantial costs and delay impediments. An interest group association in British Columbia suggests that the court's scope of review is somewhat unclear.[80] The Federal Privacy Commissioner's *Annual Report 1993-1994* highlights inconsistencies in the Federal Court's interpretation of privacy. The Federal and Provincial Commissioners make recommendations, monitor how well the government adhere to standards and receive and investigate public complaints. The dual role of the Provincial Commissioner is similar to other provincial legislation. As noted earlier, an Ombudsman or advisory role for a data protection commissioner was rejected in British Columbia. FIPA's recommendation for a stronger role for the data protection commission was based on a number of factors. First, the Ombudsman does not have any decision-making powers and is seen as an advocate. The traditional role of the Ombudsman's Office would be jeopardized. FIPA believes that, "...binding review powers are indispensable to good access and privacy legislation."[81] Second, the Ombudsman stands apart from the executive and legislative branches of government. The Ombudsman is an officer of the Legislature. The Ombudsman's Office "...has more in common with the judicial branch than any other arm of government."[82] FIPA believed that the Ombudsman's power to make decisions on access to information and privacy legislation would be diminished by its traditional role. An Ombudsman has the responsibility of legislating access to information and privacy rights at the federal level and in the jurisdictions of Manitoba and New Brunswick. FIPA considered an independent specialist to address access to information and privacy issues essential. The Ombudsman's Office of British Columbia has dealt with public complaints on access to information, privacy and other issues over the years. The arguments for a separate office were similar to those made by Inger Hansen, when she served as the first federal Privacy Commissioner.

---

[80]David Loukidelis, Catherine L. Hunt and Valerie Osborne (1991). Information Rights for British Columbia: Recommendations for Access to Information and Protection of Privacy Legislation for British Columbia. Vancouver, B.C. Freedom of Information and Privacy Association Legislative Task Force, 1991, p.18.

[81]Ibid. p.15.

[82]Ibid. p.15.

Hansen believed privacy protection should be given its own mandate and should exist outside of the Human Rights Act. The United States Privacy Act of 1974, Canada's Federal Privacy Act of 1982 and the British Columbia FOIPP Act of 1992 represent various models of data protection policies.

Overview of the Models of Data Protection

The policy instruments selected to protect information privacy varied considerably among democratic countries. The decision to adopt a specific instrument is based on a host of factors. These include: the bureaucracy's interest in maintaining control over information, interest group pressure to make governments more open and accountable and electoral promises. Bennett provides a comprehensive list of five domestic characteristics that influenced the policy instrument decision in the United States, Sweden, West Germany and the United Kingdom. These include: "...the repertoire of policy instruments within the state; the preferences of the dominant social groups; the role of political parties in electoral competition; the position and power of bureaucracy; and economic constraints."[83] The United States Privacy Act, is an example of a self-enforcing law that relies on the assertion of individual rights in the courts and represents one model. The Act does not have a separate enforcement agency. Americans depend on the oversight roles of Congress and the Office of Management and Budget (OMB). A second model is the Canadian federal Privacy Act which established an enforcement agency with investigative and monitoring responsibility. Individuals can complain to the Canadian Federal Privacy Commissioner, who can apply to the Federal Court for a review of a government decision. Several provinces have introduced legislation with a stronger regulatory component. The 1992 British Columbia FOIPP Act has some similarities with the federal legislation, although the powers of the Provincial Commissioner are greater. The FOIPP Act confers to the Information and Privacy Commissioner significant powers to supervise information practices and respond to complaints, conduct investigations and issue binding orders to a public body. Canadian courts are playing an increasing role in the protection of privacy.

---

[83]Colin J. Bennett (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States. p.7.

The Protection of Privacy by the Courts

The Canadian Charter of Rights and Freedoms of 1982 has given the courts a powerful role in the affairs of government. Before the Charter, the courts' primary concern was the division of power between governments. Canadian society is becoming more rights oriented and relies increasingly on the courts rather than elected representatives. The result is the Charter has given judges a substantive policy making role. The BCCLA and FIPA observe that the courts and elected officials are increasingly aware of privacy as an important value in our society. The courts' interpretation of privacy rights using Section 8 of the Charter led members of both organizations to assert: "Although these have not had a broad impact, they have signaled the courts' judgment that citizens' rights to privacy can override the efficiency of government operations and of law enforcement interests."[84] The Charter applies to all laws and policies made by federal and provincial governmental agencies and limits the activities of government in the affairs of private citizens. The term "privacy" is not mentioned in the Charter, however Section 8 is recognized as protecting privacy interests. Section 8 states: "Everyone has the right to be secure against unreasonable search and seizure." The Supreme Court of Canada has applied Section 8 to include a right to privacy. In one interpretation, the Supreme Court concluded in R. v. Dyment (1988): "Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual."[85] The Supreme Court judge added that: "Recent trends in health care exacerbate the problems relating to privacy in the medical context, particularly in light of the health-team approach in an institutional setting and modern health information systems."[86] The right to privacy is not absolute in the Charter. The courts must balance the individual right to privacy with societal goals. Section 1 of the Charter recognizes that the violation of a Charter right may occur

[84]Erin Shaw et al. (1994). The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. p. xxi.

[85]R v. Dyment [1988] 2 S.C.R. 417.

[86]Ibid.

if it is "democratically necessary in a free and democratic society." The Courts also recognize an individual's right to have access to medical records.

The Supreme Court of Canada in 1992 gave patients a legal right to access personal medical records.[87] In McInerney v. MacDonald, 1992 the judge concluded that: "The patient has a basic and continuing interest in what happens to the information and in controlling access to it."[88] The Federal Privacy Act under subsection 12(1) allows the individual to access personal information that is under the control of a government institution. Section 28 of the Act imposes limitations on access to medical records held by federal institutions. Section 28 states: "The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that relates to the physical or mental health of the individual who requested it where the examination of the information by the individual would be contrary to the best interests of the individual."[89] A similar provision is found in most legislation throughout Canada. Provinces with inadequate access legislation will have to abide by the court decision. The ruling did not apply to records held by hospitals only those of private physicians. In McInerney v. MacDonald, the judges did not address privacy issues in the decision. The control over health information is an important concern for patients throughout North America. An examination of the FOIPP Act will be presented in the following chapter, to determine the impact on the protection of health records under the custody or control of provincial public bodies, hospitals, health care organizations and self-governing professional bodies. The inclusion of health records in the Act will provide greater protection than the McInerney v. MacDonald ruling since the legislation includes privacy provisions and applies to hospitals and health care facilities. The judicial and legislative protection of privacy is not absolute nor free from criticisms.

---

[87]McInerney v. MacDonald [1992] 2 S.C.R. 138.

[88]Ibid.

[89]Canadian Statute. Privacy Act. 1980-81-82-83, c. 111, Sch. II "1".

The models of data protection policies adopted by the United States and Canada highlight differences in the two political systems. Nevertheless, the U.S. Privacy Act and the Canadian Access to Information and Privacy Acts have come under severe attack by critics who suggest the legislation in both countries are primarily symbolic in nature and has not alleviated the concerns of privacy advocates. The Canadian federal privacy legislation exemptions have been criticized by the media and public interest groups. The Canadian Federal Information and Privacy Commissioners are in a position to question and investigate the government's information practices, although the opportunity to exercise authority over federal agencies is somewhat limited. The government of British Columbia was cognizant of the weaknesses inherent in the federal legislation and responded by granting the Provincial Information and Privacy Commissioner the authority to issue binding orders. Today, Canadians are increasingly recognizing the court as an instrument in the protection of privacy. The most notable example, is the Canadian Charter of Rights and Freedoms of 1982, which has been interpreted to include the protection of privacy interests in a number of court decisions. Recent Supreme Court of Canada decisions makes it clear that the Charter, particularly Section 8 provides guarantees to privacy. The McInerney v. MacDonald decision was instrumental in granting patients the right to access information. The Courts have found that the protection of privacy using the Charter is not absolute, but must be balanced with community interests. The Charter does however protect individuals from intrusion by the state and provides a 'reasonable expectation of privacy'. Concerns about information privacy seem particularly acute when the issue is raised in the context of the health care arena. Patients throughout North America are exerting their rights to information self-determination. Patients are making increasing demands for access to health records and limits on the disclosure of information to third parties. The traditional perspectives on the physician-patient relationship and information control in the health care system come under attack as the patient rights movement emerges in Canada.

Chapter III - Challenges to Information Control in the Health Care System

A discussion of the various models of data protection policies indicates a growing movement towards the protection of personal information. Health care information represents one of the most sensitive types of personal information available. Socio-cultural, economic and technological developments in the health field diminish the control by physicians over patient information and pose some challenges to individual privacy. The first part of this chapter presents a critical survey of the traditional and contemporary theories on the physician-patient relationship. The traditional perspectives illustrate the degree to which information was controlled in the health care sector. A number of competing models suggests patients are exerting greater influence in the medical relationship and demanding more information from physicians. Today, the health record serves both medical and non-medical purposes for a multitude of disciplines. Health care professionals and researchers demand detailed patient records. The physician's control over information diminishes further by computerization and centralization of health records. The publicly funded health care system represents a serious challenge to privacy. Health care providers must furnish the public bureaucracy with patient information to facilitate the third party payment system. According to Lorne E. Rozovsky: "Once the government was given the mandate to pay for the hospital care and medical care of Canadians, it was essential that the government be given the right to know what it is being paid for."[1] The health record is a valuable tool for physicians, health care professionals, researchers, health administrators and bureaucrats. More individuals and organizations are examining the health record. As a result, regulation that limits the disclosure and uses of health information becomes critical. The protection of health information involves a number of important issues. These include: confidentiality, privacy, disclosure, privilege, access and ownership of health records. Professional codes of ethics; health care guidelines, policies and common law represent a number of strategies available to address the issues. Alan F. Westin,

[1]Lorne E. Rozovsky and Fay A. Rozovsky (1984). The Canadian Law of Patient Records. Toronto, Butterworths & Co. p. 74.

writing about the American experience describes how the use of medical records outside the physician-patient relationship poses threats to individual privacy. Westin's list of organizations that have an interest in the medical record include, health insurance companies, government payers, law enforcement agencies, welfare departments, schools, researchers, credit grantors and employers.[2] The situation across the border is not unique. Canadian provinces have encountered similar problems. The 1980 report by the Commission of Inquiry into the Confidentiality of Health Information (The Krever Commission) provides much evidence. The Krever Commission Report, although dated, describes numerous examples of how confidential health information was seriously undermined in Ontario.[3] A number of problems in the British Columbia health care system are highlighted by recent events that involved inadequate storage and disposal of health records. The government of British Columbia is responding to growing concerns about access to information and privacy rights. Health records are covered under the provisions of the British Columbia FOIPP Act to protect all personal information held by public bodies. The Act guarantees patients a legislated right to access personal health records, to challenge the accuracy of the information and to restrict unauthorized use and disclosure. Clearly, the traditional authority exercised by the medical profession is diminished with increased regulation of health records. The health literature offers a number of perspectives on the traditional and contemporary role of the physician and highlights the control over information in the medical relationship.

---

[2]Alan F. Westin (1976). Computers, Health Records, and Citizen Rights. Washington, D.C., U.S. Department of Commerce. National Bureau of Standards, p.27.

[3]Horace Krever (Commissioner). Report of the Commission of Inquiry into the Confidentiality of Health Information. Volumes I, II and III. Royal Commission Report. Toronto, Queen's Printer for Ontario, 1980.

Models of The Physician-Patient Relationship and Information Control

A number of theoretical approaches in the health literature describe the physician-patient relationship and the control over information. Each model contributes to our understanding of the physician's position of authority and the regulation of information exchange. The medical paternalist and sick-role models illustrate the dominant role of physicians. The first model stresses the importance of the public interest and the role physicians play in protecting patients from harm. The second approach emphasizes the competence of doctors in the treatment process and the powerful status designated to the medical profession. The third, a conflict theory perspective challenges the medical paternalist and sick-role models and represents the emerging physician-patient relationship. Two models, the doctor-judgment approach and the consumer theory of health care, focus on information control in the medical relationship. In the health literature a wide variety of models are espoused to describe the physician-patient relationship. The five models selected represent traditional and contemporary views of the relationship and to varying degrees prevail in the Canadian health care system.

The "medical paternalist" model is a dominant way in which physicians view the physician-patient relationship. Allen Buchanan defines paternalism as "...interference with a person's freedom of action or freedom of information, or the deliberate dissemination of misinformation, where the alleged justification of interference or misinforming is that it is for the good of the person who is interfered with or misinformed."[4] The medical profession justifies paternalistic acts as necessary to protect the public interest. The main argument for withholding information and misinforming patients or family members is based on the Prevention of Harm Argument, which states: "The physician's duty - to which he is bound by the Oath of Hippocrates is to prevent or at least to minimize harm to his patient; giving the patient information X will do great harm to him; therefore

[4]Allen Buchanan (1982). "Medical Paternalism." Medicine and Moral Philosophy. Edited by Marshall Cohen, Thomas Nagel and Thomas Scanlon. Princeton, New Jersey, Princeton University Press. p.215.

it is permissible for the physician to withhold information X from the patient."[5] In North America, patients exert rights to self-determination and the arguments favouring medical paternalism are increasingly looked upon negatively. Buchanan's observation that the dissemination of misinformation is a paternalistic act is important in understanding why patients may want to examine personal health records. One concern shared by civil libertarians and privacy advocates is the harm that may occur from the disclosure of inaccurate or outdated information. One method to combat medical paternalism is to provide the opportunity to view personal information and to challenge the accuracy of the record. Hospitals and health care institutions traditionally did not permit patients to see their records. The rationale used by these institutions was that the patient would not understand the medical jargon; the information would be taken out of context and mislead the patient; and frivolous lawsuits would result.[6] Talcott Parsons' introduction of the sick-role perspective provides further insight on the dominant role of physicians.

According to Parsons, patients view physicians as possessing "high levels of technical competence" and are therefore given high status.[7] The result is an "asymmetric relationship between these functionaries in the health-care system."[8] The Parsonian model is based on two beliefs. "The first is that the patient is in an undesirable role - the so-called sick role - that requires him or her to co-operate with others in order to leave that role. The undesirable nature of the sick role places the patient in a powerless position relative to the physician."[9] The second belief is that the physician is in a powerful position compared to the patient and "this power is legitimated by the sick-role

[5]Ibid. p. 221.

[6]Lorne E. Rozovsky (1994). The Canadian Patient's Book of Rights: A Consumer's Guide to Canadian Health Law. Second edition. Toronto, Doubleday Canada Limited. p. 88.

[7]B. Singh Bolaria and Harley D. Davidson (1994). Health, Illness and Health Care in Canada. Second edition. Toronto, Harcourt Brace and Company Canada, Ltd. p. 184.

[8]Ibid. p. 184.

[9]Ibid. p. 186.

model."[10] The potential for social control is, therefore enforced by the dominant position of the physician. Critics suggest the "sick-role" model focuses primarily on the physician's perspective and pays minimal attention to the patient's role and expectation. A conflict model of society is espoused by critics of this traditional perspective.

Proponents of the conflict theory consider the "sick-role" concept a "...social control mechanism for maintaining the status quo, and the competence gap as a means of creating inequality in the professional-client relationship."[11] This inequality is perpetuated by the physician's control over the transmission of information.[12] Based on the conflict theory perspective "The major tactic used by physicians to retain their dominance is information control, while patients attempt to contain that dominance by information seeking in the "micropolitics" of the medical encounter."[13] Supporters of the conflict model contend that values will clash as "...processes of conflict resolution ranging from accommodation and negotiation to the exercise of domination and force" between the two parties unfold.[14] The conflict model of society is useful in understanding the emerging physician-patient relationship. Patients are exerting pressure for an increasing role in the medical relationship and demanding greater accountability from medical professionals. The recognition by legislators and the courts that patients have a legitimate interest in health records challenge the traditional perspectives. Consumers of health services are also acquiring the knowledge to make decisions and are choosing a variety of health care options. The medical

[10]Ibid. p. 186.

[11]Marie Haug and Bebe Lavin (1983). Consumerism in Medicine: Challenging Physician Authority. Beverly Hills, Sage Publications, Inc. p. 15.

[12]Ibid. p. 15.

[13]Ibid. p.15. Haug et al. cites Howard B. Waitzkin and John Stoeckle. "Information Control and the Micro-Politics of Health Care: Summary of ongoing research project." Social Science and Medicine, 1976, 10, 263-276.

[14]Ibid. p.13. Haug et al. cites Eliot Freidson. Patient's Views of Medical Practice. New York, Russell Sage Foundation, 1961.

profession's status declines as a result of these factors. The doctor's judgment approach and the consumer theory of health are two models that address the control of information in the medical relationship.

The "doctor's judgment" approach is a traditional perspective that dominated the health-care field. The model assumes that ethically bound physicians should decide what type of information is made available to a patient. The decision is based on the professional's judgment of what is in the patient's best interest. The model rejects the notion that patients have a right to review all information contained in medical or health records since;

> ...complete disclosure might create needless anxiety or upset patient unduly; telling only part of the truth, or withholding information temporarily, may be good medicine in a particular situation, especially when psychosomatic aspects are involved; patients would not be helped if they were to be told the speculative and tentative hypotheses that physicians were considering at a given moment.[15]

This traditional model asserts that a good physician will release information to assist in the patient's care and the decision should ultimately be left to the doctor and not a delegated authority.[16] Proponents of the doctor's judgment approach oppose access to information rights for patients due to the technical language in medical records. Some physicians fear the patient will not understand the terminology and further interpretation would be unnecessarily time-consuming and expensive. One argument espoused is that, "...providing access would inhibit doctors from putting down the speculative and hypothetical comments they now do, to help both themselves and other professionals who may later consult the record, and would lead to highly defensive record-keeping practices..."[17] One further criticism is that the value of the medical record for research, care-review and service payments would be reduced as record-keeping practices changed. A second

---

[15]Alan F. Westin. "Medical Records: Should Patients have Access?" Hastings Centre Report. Vol. 7, No. 6 (December 1977), p.25.

[16]Ibid. p. 25.

[17]Ibid. p. 26.

model of information control, the consumer theory of health care challenges this traditional approach.

The consumer theory of health care model considers the physician an agent of the patient who is hired to exercise professional skills and judgment. The physician is bound by a fiduciary duty to provide complete disclosure of information upon request by the patient. Full disclosure of information to a patient is beneficial for a number of reasons:

> ...it is essential to the patient in making informed decisions about the risks and benefits of proposed treatments and operations; it is essential if the patient is to know whether to authorize release of medical information to third parties; it fosters patient participation in and taking personal responsibility for health care; it would assist patients in making consumer judgments about the acceptability of care being provided by a given doctor or hospital, compared to other available alternatives.[18]

Consumers of health services believe an examination of medical records is essential and provides opportunities for patients to correct any errors and to decide whether to authorize release for non-medical purposes. According to the traditional "doctor judgment" approach, physicians have a high degree of autonomy when determining the types of information to be released to a patient. The "doctor judgment" model rejects a legislated right for patients to access medical and health records. The "consumer" model recognizes the need for full disclosure within certain exceptions. Critics of the consumer model argue that the language used in the records may not be intelligible. Conversely, proponents argue that: "Explanations should either be added to the record or made to the patient orally by health professionals."[19] The five models reflect a diversity of views that exist in the Canadian health-care system. Similar views exist in the United States.

A study conducted by S. O'Gara in 1984 suggests that the traditional perspective that patient access will have negative effects may be invalid. O'Gara's study found that 75 percent of

[18]Ibid. p. 26.

[19]Ibid. p. 26.

physicians did believe patients would suffer harm by examining the health record.[20] The study revealed that physician-patient communication was not disrupted once patients were given access to records. Instead physician-patient communication improved. The concerns about increased numbers of malpractice suits were also unfounded. According to O'Gara "...although 51 percent of physicians surveyed in an attitudinal study believed patient access would increase malpractice litigation, an American Medical Association report found no change in incidence in states permitting patients to have access to their records."[21] The fear and uncertainty that patients experience about the permanency of their health record "...can be quelled if patients are given the opportunity to review the accuracy, completeness, and timeliness of health records information used in making nonmedical decisions about them."[22] In Canada, patient request for information is seldom handled in a uniform manner and is often based on organizational practices.

Given the ad hoc approach in which information requests may be handled in the health field, a legislative guarantee allowing patients to examine personal health records advances the consumer theory of health care. Rozovsky argues that, "The answer for patients who want access is to retain a lawyer who is familiar with the working of the health care field, and particularly with how record keeping takes place."[23] Many Canadians assume that the confidentiality of patient information is protected in a doctor's office or health care institution. As Rozovsky points out, there have not been many court cases in Canada in which patients have sued doctors or hospitals for the release of confidential medical information. "Because of the costs, and the uncertainty of whether there is a

[20]Jo Anne Czecowski Bruce (1988). Privacy and Confidentiality in the Health Care Information. Second edition. Illinois, American Hospital Publishing, Inc. Bruce on p. 163 cites the study by S. O'Gara. "Does Patient Access to Health Records Cause Harm?" Journal of the American Medical Record Association. March 1984, 515(3):20.

[21]Ibid. p.164. Cited S. O'Gara "Does Patient Access to Health Records Cause Harm?" p. 22.

[22]Ibid. p. 3.

[23]Lorne E. Rozovsky (1994). The Canadian Patient's Book of Rights: A Consumer's Guide to Canadian Health Law. p.89.

legal right, it usually is not worth doing."[24]. Recently, the situation has changed as the number of malpractice suits increased in Canada. "This change has taken place during a period when Canadians have placed less importance on peace, order and good government and have become caught up with their "rights and freedoms" as given to them under the constitutional Charter of Rights and Freedoms."[25] As more Canadians challenge the physician's authority, "deprofessionalization", of medicine occurs.

The professional status of physicians has come under scrutiny in the past two decades. C. P. Shah provides two explanations for "deprofessionalization." First, there has been a decreased deference to all forms of authority as a result of the increasing democratization of western societies. Second, "...the great increase in the general level of education, particularly among the large numbers of individuals, employed in other scientific disciplines and the social sciences, has removed the mystique associated with the medical profession."[26] Shah believes that one of the most important deprofessionalizing factor was the establishment of government-sponsored universal medical insurance.[27] The medical profession continues to enjoy some degree of autonomy although members are increasingly held accountable to the public bureaucracy and consumers. Consumerism in medicine and the emergence of new professions are dominant forces that challenge the traditional perspectives of the physician-patient relationship.

---

[24]Ibid. p. 90.

[25]Ibid. p. 181.

[26]C. P. Shah (1994). Public Health and Preventative Medicine in Canada. Third edition. Toronto, University of Toronto Press. p.402.

[27]Ibid. p. 402.

Challenges to Information Control in the Health Field

Consumerism in Medicine and New Professions

The deference to medical authority has undergone significant transformation since the late part of the twentieth century. The rise in health-care consumerism has brought into question the authority of physicians. "Consumerism implies buyer's challenge of seller's claims. It represents an approach of doubt and caution, rather than faith and trust, in any transaction, including the medical."[28] Consumerism in medicine refers to "challenging the physician's ability to make unilateral decisions -- demanding a share in reaching closure on diagnosis and working out treatment plans."[29] Marie Haug and Bebe Lavin explain this phenomenon by suggesting that the increase in the educational level of the general population reduces the information gap between patients and physicians.[30] Educational levels account for the increasing willingness to question medical authority as the social distance between the two parties narrow. Patients have higher expectations concerning rights and benefits. Joan Price Boase points to the adversarial nature of society as contributing to the erosion of professional status.[31] Public awareness programs, health magazines and health information available from various media sources promote an informed public and the efficacy of self-care. Patients will question doctors, engage in greater self-care activities and employ the services of paraprofessionals for some health-care needs.[32]. Haug et al. provide a number of explanations for the rise in patient consumerism. The "...growth of various paraprofessions, new occupations demonstrating that for some conditions and types of care,

[28]Marie Haug and Bebe Lavin (1983). Consumerism in Medicine: Challenging Physician Authority. p.10.

[29]Ibid. pp. 16-17.

[30]Ibid. p. 15.

[31]Joan Price Boase (1994). Shifting Sands: Government-Group Relationships in the Health Care Sector. Montreal and Kingston, McGill-Queen's University Press. p.16.

[32]B. Singh Bolaria and Harley D. Davidson (1994). Health, Illness and Health Care in Canada. p.193.

physicians' services are expendable."[33] Furthermore public and government concern about medical ethics brought into question the physician's authority.[34] Boase identifies a number of factors that contribute to the erosion of professional status. These include: the "...education status of other (aspiring) medical professions and their concomitant rejection of historical hierarchical, superior/subordinate relationships within this field" and technological changes resulting in highly educated groups and physicians who are unable to claim comprehensive knowledge.[35] As new professions emerge in the health field the control over information by physicians diminishes further.

The participation by a host of health care providers fostered the need for detailed documents and shared health information. The primary health record serves a number of purposes including details on patient visits and information for third party payments. Information must be recorded and available for inspection by individuals involved in the treatment process. Consumerism in health care means more patients are visiting a range of specialists and health professionals. The outcome is "the classical doctor-patient relationship is dispersed among a team of medical and para-medical personnel."[36] The medical record is more important as the health care field becomes more specialized. It is not uncommon for a patient to see a variety of health care professionals. The patient in many cases is not cared for exclusively by a personal physician, but by nurses, consulting physicians, technologists, technicians, health personnel and administrative personnel.[37] Referrals to a number of professionals are common trends in the health care system. A major concern associated with a multi-disciplinary approach to health care delivery is the loss of control

[33]Marie Haug and Bebe Lavin (1983). Consumerism in Medicine: Challenging Physician Authority. p.10.

[34]Ibid. p. 22.

[35]Joan Price Boase (1994). Shifting Sands: Government-Group Relationships in the Health Care Sector. p16.

[36]Canada, Task Force established jointly by the Department of Communications/Department of Justice (1972). Privacy and Computers. p.73.

[37]Lorne E. Rozovsky and Fay A. Rozovsky (1984). The Canadian Law of Patient Records. pp.73-74.

over patient information. The doctor is no longer the primary custodian of health information especially in cases where the patient chooses among a variety of health care options. In addition, a number of health care professionals within the hospital setting compile information about the patient. David H. Flaherty points to studies revealing that as many as 75 to 100 individuals view a patient's medical and health information in a clinic or hospital setting.[38] As "...personal information flows from the patient to hundreds of other people so that they can provide the sophisticated type of treatment which patients in Canada now expect" privacy is reduced further.[39] D. Coburn et al. observe: "Physicians are losing ground to planners and even to other health-care workers. What physicians do is now subject to scrutiny and control by hospital administrators, health planners and state bureaucrats."[40] The computerization and centralization of health information are further developments in the health care field that have a significant impact on the control and use of information.

Computerization and Centralization of Health Information

Computerization of medical information accentuates the problem for both the traditionalist and consumers of health care as more detailed patient records become available.[41] Westin states:

> This makes patients more concerned about what is now captured in their records and disseminated efficiently beyond the primary care setting, and makes doctors more worried about their detailed progress notes, formal diagnoses, and observations on emotional and social aspects printed out for patients to take away, and often to show to their lawyers and friends.[42]

---

[38]David H. Flaherty. "Privacy and Data Protection in Health and Medical Information." Notes for Presentation to the 8th World Congress on Medical Informatics. Vancouver, July 27, 1995 (unpublished). p.2.

[39]Lorne E. Rozovsky and Fay A. Rozovsky (1984). The Canadian Law of Patient Records. p. 74.

[40]D. Corburn, Carl D'Arcy, George M. Torrace and Peter Kong-Ming New (1987). Health and Canadian Society: Sociological Perspectives. Second edition. Markham, Fitzhenry & Whiteside. p.364.

[41]Alan F. Westin. "Medical Records: Should Patients have Access?" Hastings Centre Report. p.26.

[42]Ibid. p. 26.

The centralization of health records in hospitals and large institutions reduces the control over patient information by physicians. In modern societies the concern about third party access to information is fostered by the large scale collection and storage of personal data. The debates on the confidentiality of health records and the effect information technology may have on personal privacy are widespread in several western societies. In a 1972 Report by the federal Task Force, *Privacy and Computers*, the authors stated that centralization and computerization of medical records raised concerns about privacy. The Task Force was perturbed by "...the possibility of error and the use of health information by third parties, unknown to either doctor or patient, or perhaps with the knowledge of the doctor only..."[43] Michael Wahn argues that, "Physicians are learning, sometimes less than gracefully, to accept restrictions on their autonomy that follow from tight hospital budgets."[44] The bureaucracy's monitoring of the diagnostic and treatment of patients in hospitals limit the autonomy of physicians. The review of medical insurance claims to determine utilization rates are common practices. Furthermore, the doctor's expertise and autonomy are challenged as computers are used to monitor work practices to compile comparative statistics. The administrative, investigative and statistical tools employed by bureaucracies threaten to undermine the control over health information traditionally enjoyed by the medical profession. The use of identifiable health information from secondary sources creates some tension between researchers and privacy advocates.

Research and Health Information

Howard B. Newcombe, a researcher with the Ontario Cancer Registry describes the resistance to the use of identifiable patient information for research. "Public perception of 'privacy' (not

[43]Canada, Task Force established jointly by the Department of Communications/Department of Justice (1972). Privacy and Computers. p.74.

[44]Michael Wahn (1987). "The Decline of Medical Dominance in Hospitals." Health and Canadian Society: Sociological Perspectives. Edited by D. Corburn et al. p.427.

'confidentiality') pose the major threat to use of named records in cohort studies."[45] Researchers link personal histories in the field of epidemiology for statistical purposes. Large cohort studies are made possible by "...electronic computers; consolidations of personal records into machine-searchable databases; and probabilistic ways of linking together the records of particular individuals."[46] An extensive body of literature has developed since 1959 on the methodology of record linkage and its application to "...patient care, medical data processing, epidemiology, vital statistics, demography, genetics, public health service, genealogy, [and] historical migrations..."[47] Newcombe warns that scientific and social harm will occur by limiting the use of records in the name of privacy. Newcombe is critical of the Canadian Federal Privacy Commissioner and Ontario Information and Privacy Commissioner who wish to impose constraints on data linkage in research. In Ontario, for example, physician reporting of cancer cases is not mandatory. As a result the Cancer Registry is created by linking records from a number of sources, including treatment centers, general hospitals, pathology reports, prescriptions for free drugs and death registrations.[48] Newcombe argues that: "The [Ontario] Information and Privacy Commissioner objects on the basis of a supposed "fundamental principle", i.e., data for research should be collected directly from the individual and secondary use of existing records should be avoided."[49] The researchers' ability to obtain permission from participants in cohort studies may be somewhat limited. Large scale cohort studies on cancer in the Canadian population will "...depend on linkages with a centralized mortality database going back to 1950."[50] As Flaherty puts it: "Privacy advocates are emphatic about the need for informed consent for secondary uses of

[45]Howard B. Newcombe. "Cohorts and Privacy." Cancer Causes and Control, Vol. 5 No. 5, (1994) p.289.

[46]Ibid. p. 287.

[47]Ibid. p. 287.

[48]Ibid. p. 289.

[49]Ibid. p. 289.

[50]Ibid. p. 288.

personal health information, including statistical and research uses."[51] Researchers note that some confusion exists between the administrative and statistical uses of records. The former is used to determine eligibility for a benefit and will directly affect the individual. The purely statistical use will not have a direct impact on the individual nor will the linking of records. A. B. Miller, a researcher at the University of Toronto argues that the use of identifiable information is necessary for researchers in cancer registries and those concerned with vital statistics. Miller states "...we need to identify these individuals and correctly classify the nature of their disease...This requires data on the identification of these individuals at the hospital laboratory, cancer registry and vital statistics registries, both at provincial and national levels."[52] Privacy advocates believe the public should have concerns about the administrative and statistical uses of data. Ann Cavoukian, the Assistant Information and Privacy Commissioner for Ontario responded to criticisms by Newcombe. Cavoukian provides several explanations why the direct collection of personal information from the individual is desirable. These include: "Enhancing the likelihood of the accuracy of the information; ensuring that the information is not used out to context; and ensuring that the individual whose personal information is being collected has been advised of the reasons for collection, the legal authority for the collection, and the intended uses of the information."[53] Cavoukian does suggest some indirect collection may be permissible once personal identifiers are removed. Flaherty observes that: "Despite the fact that it is impossible to anticipate all legitimate future uses of data, ensuring acceptable levels of informed consent is a very sensitive data protection issue."[54] There is a conflict between the risks associated with computer linkage and

[51]David H. Flaherty. "Privacy, Confidentiality, and the Use of Canadian Health Information for Research and Statistics." Canadian Public Administration. Vol. 35, No. 1 (1992), p. 82.

[52]A. B. Miller (1986). "The Researcher's Need for Access." Proceeding of the Workshop on Computerized Record Linkage in Health Research held May 21-23, 1986, Ottawa. Edited by Geoffrey R. Howe and Robert A. Spasoff, University of Toronto Press. p. 64.

[53]Ann Cavoukian. "Comment: Cohorts and Privacy." Cancer Cause and Control, Vol. 5 (1994), p. 292.

[54]David H. Flaherty. "Privacy, Confidentiality, and the Use of Canadian Health Information for Research and Statistics." Canadian Public Administration. p.84.

identifiable patient records, and the public benefits that would follow from research which identifies health hazards. Further restrictions on the researcher's ability to use health information may have a serious impact on public health issues. Governments are major users of health information for administrative and statistical purposes.

Third-Party Payment

The state's involvement in the provision, financing and regulation of medical and hospital care has restructured the relationship between physicians, patients and the government. Third party payments for hospital and medical service have an impact on the physician-patient relationship. Rozovsky argues that: "Privacy was further reduced by the development in Canada in the 1950's and 1960s of government hospital insurance, medicare and other health care insurance programmes."[55] The demand for health information is fueled by claims administration, utilization reviews, public health issues, investigations of fraud and abuse, and cost control measures. Public health insurance authorities analyse how health care is provided to protect standards and to ensure funds are spent within guidelines set by the government. "In order to carry out what is called utilization management, a great deal of information must be collected on the number of procedures performed, the time required for each, [and] the success rate..."[56] Health insurance authorities have developed elaborate systems to gather information. The result is that: "The treatment of every patient by a physician or in a hospital is reported to government health authorities. The name of the patient, the diagnosis, and the treatment are collected."[57] The situation in Canada is not unique. Bruce argues that, "...what technology did not accomplish by way of penetrating confidentiality, big government [in the United States] did in its effort to guarantee availability of

[55]Lorne E. Rozovsky (1994). The Canadian Patient's Book of Rights: A Consumer's Guide to Canadian Health Law. p.74.

[56]Ibid. p. 82.

[57]Lorne E. Rozovsky and Fay A. Rozovsky (1984). The Canadian Law of Patient Records. p.74.

care."[58] The collection, storage and dissemination of information in the Canadian health care system are widespread.

Throughout Canada, rising health care costs has led to a preoccupation with deficit reduction, managing more with less and changing the way governments use information in the health field. To reduce fraud and over-utilization of the system, the collection of information is vital. To curb abuse health authorities use computerized systems to draw physician and patient profiles and are compared to set averages. "The price however, is the loss of privacy for patients who get the benefits of paid services..."[59] Besides hospital and medical services, eligibility for social services and workers' compensation programs will be based on information contained in the primary or secondary patient record. A primary patient record is used by the health care professional to provide patient care and to document observations and treatment. The secondary patient record includes patient-identifiable data such as Social Insurance Number or Personal Health Number that is taken directly from the primary patient record. To cope with burgeoning health care costs, measures to improve efficiency include reviewing expenditures and utilization of services and reducing duplication. Moreover, a number of information technologies described in Chapter IV are employed by provincial Ministries of Health to contain health care costs. The bureaucracy will develop new and effective ways to share information within the health care system. This is not unusual, since a large number of individuals and organizations have an interest in the health record.

Health Records in British Columbia

A review by the Deputy Provincial Health Officer in 1995 indicated that approximately 3.7 million health records existed in the health care system.[60] The review found that, in many cases, the

[58]Jo Anne Czecowski Bruce (1988). Privacy and Confidentiality in the Health Care Information. p.16.

[59]Lorne E. Rozovsky and Fay A. Rozovsky (1984). The Canadian Law of Patient Records. p.75.

[60]Shaun H. S. Peck. Review of the Storage and Disposal of Health Care Records in British Columbia. Report by the Office of the Provincial Health Officer to the B.C. Ministry of Health and Ministry Responsible for Seniors. Victoria, July, 1995. p. 9.

creation of a new record is made each time an individual visits the health care system and there may be more than one record for each illness and injury. This number is not exorbitant considering the large number of agencies, organizations and health care providers maintaining health records in the province. The list includes the Ministries of Health and Social Services, the Attorney General's Office, the Workers' Compensation Board, hospitals, long term care facilities, home care agencies, physicians' offices, offices of other independent professional health care providers, and the offices of unregulated and unfunded health care providers.[61] Health care institutions and professionals collect and store a vast quantity of intimate and sensitive personal information. Health records include medical records, test results, clinical notes and hospital charts. The types of information found most often in a health record include: personal and family information; physical and psychological health test results; and payments made by the health insurance authority. Beyond demographics, diagnostic tests and insurance data; personal information can relate to an individual's race, religion, marital status; their education, criminal or employment history, and their personal views or the views of others about them. An all encompassing definition of a health record is "any health information on an identifiable person recorded in letters, photographs, vouchers, payment vouchers, papers, electronic storage or any other means of storage or recording, including video recording."[62] Today the health record serves a multitude of functions some of which extend beyond the medical relationship. These include: clinical purposes such as treatment and care of patients; teaching; research; gathering of statistics; hospital accreditation; government funding; auditing of standards; discipline of professionals; taxation; fund raising; legal defense of health care providers; and to meet legislative requirements.[63] The health record is indeed a valuable tool and useful to more organizations and individuals than ever before. Throughout

[61]Ibid. p. 9.

[62]Ibid. p.4.

[63]Erin Shaw, John Westwood and Wodell Russell (1994). The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. Prepared for the B.C. Civil Liberties Association and B.C. Freedom of Information and Privacy Association, Vancouver. p. 98.

Canada, provincial medical Electronic Data Processing records serve a number of functions. "...[T]o control the type of medical care being delivered;...to research into epidemic diseases and patterns of health care utilization; and to help enforce legislation."[64] Health information transcends the medical profession and diminishes the physician's control in the medical relationship. The protection of patient information involves a number of important issues such as the confidentiality, privacy, disclosure, privilege, access and ownership of health records. A number of strategies available to safeguard health information in British Columbia include professional codes of ethics; health care guidelines and policies, judicial review and recently access to information and privacy legislation.

The Protection of Health Information

Confidentiality and Disclosure of Health Records

The confidentiality of patient data has been the subject-matter of debates in the field of health-care. The traditional perspective on the fiduciary relationship between the patient and doctor and the protection of information is viewed as a matter of professional ethics and medical secrecy. Ellen Picard observes how: "The requirement of confidentiality arises from the doctor-patient relationship and is older than the common-law."[65]. The disclosing of patient information has special protection under the Oath of Hippocrates which governs the medical profession. The Oath of Hippocrates states that:

> Whatsoever I see or hear in the course of my practice, or outside my practice in social intercourse, that ought never to be published abroad, I will not divulge, but consider such things to be holy secrets.

The disclosure of patient information is strongly discouraged by the Canadian Medical Association's Code of Ethics:

---

[64]Ibid. p. 73.

[65]Ellen I. Picard (1984). Legal Liability of Doctor's and Hospitals in Canada. Second edition. Toronto, Carswell Legal Publications. p.8.

> An ethical physician will keep in confidence information derived from his patient, or from a colleague, regarding a patient and divulge it only with the permission of the patient except where the law requires him to do so.[66]

A physician may be charged with breach of the professional code of ethics and suspended for professional misconduct. The confidentiality of health information is no longer left up to the discretion of physicians but is increasingly seen as a patient right. Socio-cultural developments such as consumerism and the rise in the patient rights movement in North America help to explain this trend. There is a growing recognition to "regard confidentiality...as an instrument to protect individual privacy."[67] The confidentiality of health information has some protection in the health care system.

Health care associations and facilities in British Columbia have guidelines and policies to protect the confidentiality of health records. The British Columbia Health Association (BCHA) whose membership includes all acute care and extended care facilities and some intermediate care facilities encourage members to have written policies to promote the patient's right to confidentiality and procedures to allow patients to see personal health records.[68] The guidelines are entirely voluntary for members of the BCHA. The Canadian Health Record Association and the Canadian College of Health Record Administrators have the *Code of Practice for Safeguarding Health Information* that stipulates individuals or institutions handling health information should have written policies to address access issues and confidentiality of information. The Code recommends that employees receive some training on the issues and sign a pledge of confidentiality.[69] The BCHA Guidelines and the Code help to strengthen the right to

---

[66]Ibid. p. 8.

[67]J. K. M. Gevers. "Issues in the Accessibility and Confidentiality of Patient Records." Social Science Medicine. Vol. 17, No. 16, (1983). p.1183.

[68]Erin Shaw, John Westwood and Wodell Russell (1994). The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. p. 100.

[69]Ibid. p. 101.

confidentiality and provide standards, although both are not binding on health care facilities or caregivers. One health care facility in British Columbia, the Greater Victoria Hospital Society has the following guidelines: "...health information will be released only to health care professionals caring for the patient; in compliance with provincial and federal laws or a court order; with the written authorization of the patient or the direction of the President."[70]. Hospitals and physicians must maintain records under the Hospital Act and The Medical Practitioners Act of British Columbia. Statutory protection of patient information exists for specific cases. The Health Act Communicable Disease Regulation and the Venereal Disease Act, for example, deal with communicable diseases and prohibit the disclosure of patient information. The two pieces of legislation protect patient information from unauthorized disclosure. Other guidelines include ensuring a secure location for health records, permitting only authorized individuals to view records and requiring confidential security codes and passwords for computerized information.

The disclosure of professional secrets given to a practitioner is protected by common law. Canadian common law courts recognize the physician's duty not to disclose information to third parties. Patients can sue a physician or health care provider that releases information for breach of confidence, breach of contract or negligence. Erin Shaw et al. point to a number of difficulties in enforcement. First, an application to the court is both costly and time-consuming. Second, "the bases for such legal claims [have] been uncertain" as "the common law has upheld the right of a doctor to disclose patient information to a third party when the third party is at risk."[71] The problem of enforcing the common law right to confidentiality of health care records was identified by the Ontario Krever Commission. The Krever Commission's recommendation for "...a statutory provision creating a right to sue a health care provider who has unjustifiably disclosed health

[70]Ibid. p. 101.

[71]Ibid. p. 102.

information to a third party" was never adopted.[72] Justice Horace Krever, the Commissioner whose Report consisted of three volumes of submissions detailing abuses of health information stated quite clearly:

> The reader will now know that unauthorized disclosure of health information to third parties by individual and institutional health-care providers has occurred frequently in Ontario in spite of the existence of many ethical canons and legislative pronouncements relating to confidentiality of health information, and of prohibitions against its disclosure without the consent of the patient.[73]

In 1992, a report prepared for the B.C. Freedom of Information and Privacy Association examined access to and confidentiality of health records in the province. The researchers found that a similar situation existed in British Columbia that required legislative action in the province.[74] A number of cases described in the report suggest confidentiality of health information was being undermined. Moreover, Shaw et al. point to a number of examples in which physicians and health care providers in British Columbia must release confidential health information to agencies of the state: "...patients who are judged unfit to drive (to the Motor Vehicle Branch); births, deaths and stillbirths (to Vital Statistics); suspected child abuse (to child protection authorities; failure to do so is an offense); and certain communicable diseases (to a public health official)."[75] The examples illustrate how societal interests outweigh the individual's right to limit disclosure of personal health information. The erosion of patient confidentiality is exemplified further by the disclosure requirements in common law.

---

[72]Horace Krever (Commissioner). Report of the Commission of Inquiry into the Confidentiality of Health Information. Volumes I, II and III. Royal Commission Report, Toronto, Queen's Printer for Ontario, 1989.

[73]Ibid. p. 1 of Volume III.

[74]Bill Trott, Judith Ashbourne and Richard Gareau. Access to and Confidentiality of Health Care Records in British Columbia. Prepared for the B.C. Freedom of Information and Privacy Association by the Community Legal Assistance Society, Vancouver., 1992.

[75]Erin Shaw, John Westwood and Wodell Russell (1994). The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. p. 103.

Privilege and Disclosure

Despite popular belief, the physician-patient relationship is confidential, but not privileged. In Canada a common-law medical privilege has not developed in the nine common law provinces. The legislatures of the provinces have not followed the United States example, in which forty states have some form of privilege protection.[76] The Code of Civil Procedure of Quebec 1965 offers a professional privilege to physicians and dentists.[77] Privilege is a term that describes the right to refuse disclosure or access to certain types of information. A privilege would limit the flow of information. A doctor may be compelled by a court to violate standards of confidentiality set by the medical professional body and to disseminate any information or communication given by a patient. A physician or health care provider subpoenaed must provide the information requested or face contempt of court charges. A discretionary privilege is granted in a few exceptional cases.[78] Physicians may disclose information with the consent of patients or as required by law. Disclosure of information in a medical record to third parties requires the patient's written consent or a court order. Third parties refer to "...physician-to-physician transfer for administrative purposes, lawyers and insurance adjusters..."[79] The disclosure of unauthorized medical information may result in common law actions of defamation, breach of contract, breach of confidence and negligence.[80] The common law courts have also examined the issues of access and ownership of health records.

---

[76]Jean V. McHale (1993). Medical Confidentiality and Legal Privilege. New York, Routledge. p. 28.

[77]Jack R. London (1980). "Privacy in the Medical Context." In Aspects of Privacy Law: Essays in Honour of John M. Sharp. Edited by Dale Gibson. Toronto, Butterworths and Co. (Canada), Ltd. pp. 281-297. London writes: "With the exception of matters arising within the legislative jurisdiction of the Province of Quebec, the physician-patient relationship or health care personnel-patient relationship is not protected in court. Such persons may not thereby refuse to give testimony relevant to the litigation." p. 291. Also refer to Jean V. McHale. Medical Confidentiality and Legal Privilege. p. 29.

[78]Ibid. p.291.

[79]McInerney v. MacDonald [1992] 2 S.C.R. 138

[80]Bill Trott, Judith Ashbourne and Richard Gareau (1992). Access to and Confidentiality of Health Care Records in British Columbia. p. 4.

Access and Ownership of Health Records

Under common law, the ownership of patient records remains with the physician. The Canadian Medical Association (CMA) considers medical records confidential documents. The ownership of these documents remains with the physician, institution or clinic responsible for its compilation. The CMA believes patients have a right to medical information in their personal records but not to the documents themselves.[81] In recent years the patient's interest in examining personal health records has grown in importance. The results have been a "...trend away from the long lasting and paternalistic doctor-patient relationship...[and] providers and institutions are becoming increasingly responsive to patient demands for access."[82] The general right to examine health care records did not exist in British Columbia before the FOIPP Act. Justice Horace Krever stated in the Krever Commission Report: "If the patient asks to see his or her report, is informed by the physician of any risks and harmful consequences of doing so and is nevertheless willing to run the risk, no amount of paternalism should stand in the way of the 'right to access'."[83] The McInerney v. MacDonald 1992 court decision provides patients with a legal right to examine and copy information in the health record. The Supreme Court of Canada's ruling highlights the increasing support for patient rights. It also points to increasing judicial activity in the health policy field. The Court decided that physicians "have exclusive right to physical possession of the record" and "patients have a legal interest in the information and a right to inspect and copy information."[84] The Court concluded that although the physician owned the physical record, the patient has an interest in the information. According to this court ruling, the physician must provide access to

[81]McInerney v. MacDonald [1992] 2 S.C.R. 138

[82]Erin Shaw, John Westwood and Wodell Russell (1994). The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. p. 104.

[83]Horace Krever (Commissioner). Report of the Commission of Inquiry into the Confidentiality of Health Information. Volume II, p. 470.

[84]McInerney v. MacDonald [1992] 2 S.C.R. 138

personal medical information when a request is made by a patient, unless disclosure would adversely affect the physical, mental or emotional health of the patient or cause harm to a third party. Some degree of paternalism continues to prevail in the health care system. Under the British Columbia Hospital Act, hospitals have an exclusive right to the physical possession of patient records. The Court decision did not apply to health records held by hospitals or other health care facilities; only physicians' records. Physicians practicing in provinces lacking adequate access legislation must abide by the McInerney v. MacDonald decision. The Court did not address privacy issues in the case. In British Columbia, and elsewhere, such as the United States, governments have legislated in favour of the patient's right to access health records and the privacy of the information.

Legislating Access to and Privacy of Health Records

The United States

In the 1970s, Americans became increasingly perturbed by the sharing of information. Carol Levine suggests the Watergate break-in at a psychiatrist's office to obtain the medical records of Daniel Ellsberg did arouse interest in the privacy of health information.

> The main worry is that health records, which are growing more complex and complete, will find their way into agencies - credit bureaus, law enforcement offices, welfare agencies, personnel departments - that do not have a right to them and that will use the information to deprive an individual of some benefit or chance for advancement.[85]

One additional concern is that patient authorization to release information still pose threats to privacy. The abuses to confidentiality will continue if the patient lacks prior knowledge of the types of information held in the personal health record and the individuals and organizations that can examine the record. Patients may unwittingly authorize disclosure of information for reimbursement of medical bills, employment or to receive a government benefit. The movement in the United States to give patients a legal right to examine personal medical records was similar to

[85]Carol Levine. "Sharing Secrets: Health Records and Health Hazards." Hastings Centre Report, Vol. 7, No. 6 (December 1977), p. 14.

the attempts made by parents and students to gain access to school records and consumers to access credit bureau records. Westin states these attempts are part of "...a growing citizens' movement to affirm individual self-determination and place limits on the power of institutions to determine important aspects of people's lives without due-process-oriented procedures."[86] Due to the prevalence of litigation in the United States, consumers suggested access rights would reduce the need to file malpractice suits to inspect a medical record.[87]

The US Federal Privacy Act of 1974 did permit data subjects to access personal records and correct inaccuracies. American federal agencies adopted procedures to allow patients to view their health records under the access requirements of the Privacy Act. The Act requires written consent for the release of any medical information. The US Freedom of Information Act (FOIA), allows patients in federal hospitals to request access to personal records. Patients must state the purpose for the request and outline how the record will be used on the request form. The Act specifies time frames for compliance and allowable charges for copies. Under the FOIA patients can request an amendment to the record. A number of American states have laws that permit access to medical records. State policies are not uniform and the rules vary considerably. British Columbia's inclusion of health records in the Freedom of Information and Protection of Privacy (FOIPP) Act promises to give patients more control over the health record.

British Columbia

Barry Jones, a key promoter for privacy and access to information rights for British Columbians believed health care information should be included in the FOIPP Act. Jones noted that: "Given its sensitivity, health care information is perhaps the best example, of personal information that

[86]Alan F. Westin. "Medical Records: Should Patients have Access?" Hastings Centre Report, Vol. 7, No. 6 (December 1977). p.23.

[87]Ibid. p. 26.

demands strong access and privacy safeguards."[88] The first tier of the legislation, effective on November 1, 1993, applied to health care records in the custody or under the control of the Ministry of Health or provincially operated health care facilities. The Act covers the health records of provincial health units, residential care facilities, mental health centres, mental health hospitals, alcohol and drug treatment centres. The health care records in the custody or control of the Ministry of Social Services and provincial correctional facilities are subject to the legislation. The second tier of the legislation on November 1, 1994, included hospitals and health care facilities that are publicly funded and exist under provincial enabling legislation. On November 1, 1995, self-governing professional bodies came under the second tier of the Act and included organizations such as the College of Physicians and Surgeons and the College of Pharmacists. The FOIPP Act does not apply to health records held by physicians in private practice. The legislation is nevertheless far reaching.

On November 1, 1994, one hundred provincial hospitals were regulated by the FOIPP Act. The Act introduced far reaching public access to information and privacy rights. The legislation emerged in a period marked by increasing attention on the dangers of unprotected health information. The inclusion of hospitals, health-care agencies and, in 1995, self-governing professional bodies also highlight the movement towards increasing regulation of the health sector. The scope of this new piece of legislation is wide, few, if any public bodies that receive some form of public funding are excluded. The legislation allows anyone to make an information request and all records can be examined unless exempted to protect sensitive economic, financial, negotiation, personal or security matters (refer to Appendices A and B). The exemptions in the Act are subject to review if the public interest would be better served by the release of the information. Individuals can make a request to correct personal information under the custody or control of a public body (refer to Appendix C). The Act prohibits organizations from charging a fee to individuals who

[88]Barry Jones (1993). Barry Jones Report: The Extension of Citizens' Information and Privacy Rights to all Public Bodies in British Columbia. p.49.

request access to personal information. The patient's right to have access to personal health information is not absolute.

An access request may be denied if the information could potentially cause: "Grave harm to the safety or mental or physical health of the patient, another person's safety or will reveal another person's personal information."[89] This provision conforms with the McInerney v. MacDonald (1992) court ruling. The FOIPP Act requires a compelling reason for denying an individual access to personal health care information. The legislation provides a system of appeal to the Information and Privacy Commissioner of British Columbia at no cost to the appellant. The Commissioner will decide whether to order the disclosure of the record to the patient. The Information and Privacy Commissioner, David Flaherty notes that concern for privacy and confidentiality in the health field is a matter of fundamental human rights.[90] Flaherty recently suggested that the protection of privacy or fair information practices is often ignored by operators of information systems in hospitals and physicians.[91] To avoid any unreasonable invasion of privacy, the Act states disclosure of medical information to a third party will require the patient's consent. Under Section 22 the patient's consent may not be necessary if the head of a public body refuses to disclose personal information that would be an unreasonable invasion of a third party's personal privacy. Section 33 specifies under what conditions a public body may disclose personal information (refer to Appendix D). The Commissioner is responsible for ensuring adequate safeguards are available to protect the collection, use, disclosure and security of health care information. The inclusion of hospital and health agency records in the Act will provide additional protection to patients. A patient may examine the accuracy of the health record, make corrections, and determine the extent

[89]Ibid. p. 51.

[90]David H. Flaherty. "Privacy and Data Protection in Health and Medical Information." Notes for Presentation to the 8th World Congress on Medical Informatics. Vancouver, (unpublished), July 27, 1995, p1.

[91]Ibid. p.1.

to which personal information is disclosed to others through informed consent. The enactment of the FOIPP Act and the state's involvement in the regulation of health information reflect increasing intervention in the health policy field and the emerging patient rights movement in Canada. The policy literature, in particular the Krever Commission Report and recent events in British Columbia suggest patients are often unaware that their expectation of confidentiality is being eroded.

A number of privacy disasters that occurred during the past two years in the province's health care sector heightened concerns about the protection of medical and health information.[92] The examples are numerous. They include, the Bella Bella Beach Bonfire of August 8, 1994 involving inadequate disposal of hospital records; the gynecological and obstetrician records of more than three thousand British Columbian women recovered in the basement and backyard of an abandoned home of a Vancouver gynecologist in April 1995; the discovery of health records, birth notices and post-natal notes in a filing cabinet that was available for sale to the general public in Prince George; and the unsuspecting purchase of computer disks containing medical information from the Value Village Stores Ltd., in Langley. Each of the events involved some degree of human error and mismanagement of patient files. The inadequate protection afforded these medical records suggest an ad hoc approach exists for the storage and disposal of confidential information in the health sector. A number of provincial legislation applies to the storage and disposal of health care records.[93] In response to these events a review was conducted by the Deputy Provincial Health

[92]See "Privacy chief wants access to data bases tightened", The Vancouver Sun, January 10, 1995, A1.
"Women's medical records strewn on lawn", The Vancouver Sun, April 4, 1995, A1, A2.
"Shredding of files quick as $65 call", The Vancouver Sun, April 5, 1995, A1, A2.
"Invasion of privacy near 'crisis'", The Vancouver Sun, March 2, 1995, C17.
Summary of events highlighted by David H. Flaherty in "Privacy and Data Protection in Health and Medical Information." Notes for Presentation to the 8th World Congress on Medical Informatics. Vancouver, (unpublished), July 27, 1995.

[93]The legislation applicable to health care records include: The Document Disposal Act, The Interpretation Act, The Hospital Act Regulations, the FOIPP Act, the Continuing Care Act, the Adult Care Act Regulations, Community Care Facilities Licensing Act, the Health Professions Act, acts that govern individual health professionals and the Workers' Compensation Board Act. See Shaun H. S. Peck. Review of the Storage and Disposal of Health Care Records in British Columbia. Report to the

Officer for the Ministry of Health and Ministry Responsible for Seniors. The Deputy Provincial Health Officer made several recommendations on how to improve the storage and disposal of health care records. The principle recommendation endorsed by the Deputy Provincial Health Officer was the adoption of a *Code of Practice for Ensuring the Confidentiality and Security of Health Records in British Columbia.*[94] Health care organizations are encouraged to adopt the Code and to develop policies for the storage and disposal of health care records. The response and public concern evoked by these events reveal a growing apprehension about the safety and protection of health information.

The arguments for the legislative protection of health information are compelling as well as the notion that the public interest is at stake. The agencies of the government must now balance the issues to ensure access demands do not compromise the privacy of patients. Hospitals, health care institutions and the self-governing professional bodies will have to be more vigilant in their information practices and will be held accountable to the Information and Privacy Commissioner's Office and the public at large. The public interest will be advanced in the province if the legislation fulfills expectations for increased accountability and openness for public bodies. The FOIPP Act does not include the records held by physicians in private practice, although the McInerney v. McDonald decision clearly allows patients to access these health records. In these cases, individuals must seek redress through the courts when dealing with issues of unauthorized disclosure of private records or rely on the professional body to intervene. A few of the privacy disasters that involved the health records of physicians in private practice suggest the legislation may not have gone far enough to protect health information in the province. The bureaucratic use of information technology to monitor the health care system presents further challenges to the protection of health information.

Minister of Health and Minister Responsible for Seniors. Victoria, Office of the Provincial Health Officer, July 1995. p.10.

[94]Ibid. p. 2 provides a complete summary of recommendations made by Shaun Peck to the MOH.

Chapter IV - The Bureaucratic Response: Public Administration, Information Technology and The Citizen

The challenges posed by public management of health care information and the regulatory responses to privacy issues were highlighted in Chapter III. In response to the growing complexities of the health care system, the bureaucracy uses a variety of technological tools to meet fiscal challenges; implement and monitor programs and to regulate in a number of policy areas. The Canadian health care system faces a variety of challenges in the coming years. The most significant is perhaps, the economic pressures on the system to reduce costs and to manage the available resources. Health information management is one response to the growing crisis. Provincial governments across Canada are looking at ways to effectively manage the public health care system. To some extent, this may involve the use of computerized drug information networks or a variety of card technologies. The proliferation of information in the health sector and the opportunities available to share information among users, pose some challenges to privacy. This chapter provides a brief summary of the fiscal challenges in the health sector and the bureaucratic responses to the problems. A review of specific information technologies used by the bureaucracy to regulate and monitor the health care system will illustrate how individual privacy may be undermined. The potential benefits and privacy implications for each type of technology are given equal consideration throughout this chapter. The presumed dangers and potential privacy violations discussed reflect concerns raised by policy-makers, consumers, interest groups and advocates. The primary focus is on British Columbia, although some experiences are drawn from other jurisdictions for comparative purposes.

Health Care Costs

In 1993, Canada spent over $72 billion on health care or approximately 10% of Gross Domestic Product (GDP).[1] The only country to spend more per capita and a larger amount of the GDP on health care is the United States. In the health literature three distinct phases of health expenditures are identified between the period of 1960 to 1991. The 1960s to 1970s health care costs as a percentage of GDP increased from 5.5 to 7.1% as public coverage of hospitals and medical services expanded.[2] In the 1970s, health care costs as a percentage of GDP was stabilized as a result of provincial cost constraints and national price and wage controls. From 1980 to 1993, health care costs rose from 7.3 to 10.1% of GDP. The public share of health care funding from 1960 to 1970 increased from 43 to 70% and to 75% in 1980. In the early 1990s the public share has decreased to approximately 73%.[3] The current health care system is in a state of turmoil. The escalation of health expenditures and costs coupled with the problem of shrinking provincial revenues due to restrictions on the growth of Established Program Financing cash transfers provides much evidence. In response, provincial governments must examine new ways to manage the system. Douglas E. Angus, Ludwig Auer, J. Eden Cloutier and Terry Albert describe four options available to governments. These include: "...raise taxes, run large deficits, cut back spending in other areas such as education, or begin in earnest to control health care costs."[4] A number of provincial royal commissions and other studies on health care costs did emerge in the 1980s although "...strong cost control measures did not emerge until the recession hit in 1990-91."[5] Provincial governments are implementing reforms and monitoring the health care system

[1]Douglas E. Angus, Ludwig, Auer, J. Eden Cloutier and Terry Albert. Sustainable Health Care for Canada: Synthesis Report. Queen's-University of Ottawa Economic Projects, Ottawa: University of Ottawa. 1995. p.9.

[2]Ibid. p. 9.

[3]Ibid. p. 9.

[4]Ibid. p. 14.

[5]Ibid. p. 14.

more closely. One way in which the government is managing the system is by examining the utilization of pharmaceuticals. Pharmaceuticals represent the third largest expenditure in total (public and private) health care costs.[6] During 1960 to 1993, the annual cost of pharmaceuticals rose from under $300 million to $11 billion.[7] A ten percent increase in the consumption of prescription drugs was contributed to the growth and aging of the population. Moreover, twenty-five percent of the increase was due to more prescription drug purchases per patient.[8] A 1994 study by John N. Lavis and Geoffrey M. Anderson found prescription drug expenditures among elderly British Columbians during the 1980s "...were primarily caused by increases in the quantity of (new and existing) drugs being purchased per capita."[9] The researchers studied the number of different drug exposures among the elderly in Ontario and British Columbia and concluded that, "...multiple drug exposures can have significant impact on both quality of care and on the level of expenditures."[10] Perhaps more startling is that: "Almost 48 percent of individuals exposed to six or more different drugs received their prescriptions from three or more different physicians."[11] The impact of drug interactions on the health care system is far reaching. Furthermore, the "percentage of hospital discharges attributable to negative drug events was highest for those aged 75-84 years."[12] The strategies employed by provincial governments to address rising health care costs varies considerably. Pharmanet a computerized drug information network and card technology represent two approaches to manage information in the system and to reduce costs.

[6]Ibid. p. 105.

[7]Ibid. p. 40.

[8]Ibid. p. 40.

[9]Ibid. p. 106. Angus cites this study by John N. Lavis and Geoffrey M. Anderson (1994). "Prescription drug Use in the Elderly. Expenditures and Patterns of use under Ontario and British Columbia Provincial Drug Benefit Programs." Queen's-University of Ottawa Economic Projects, Working Paper No. 94-02. Ottawa, University of Ottawa.

[10]Ibid. p. 106. Angus cites the study by Lavis et al.

[11]Ibid. p. 109.

[12]Ibid. p. 109.

David H. Flaherty writes that: "The issue of accountability is critical, because civil servants seek data on individuals, to design and evaluate programs, to augment their prestige/power, and, as a product of a supposed technological imperative, to enable them to use the latest hardware and software programs."[13] Bureaucracies continually strive for new ways to use information to regulate and control programs.

Bureaucracy and the Requirements for Personal Information

The rise of the welfare state in the twentieth century led to increased interaction between individuals and public bureaucracies as the state demanded more detailed personal information. Eva Etzioni-Halevy notes that bureaucratic power grew as the state intervened in response to the public's rising expectation for public welfare.[14] To implement public policies in society, governments are demanding ever-increasing quantities of information about the individual citizen. The collection, use and storage of information by bureaucracies can conflict with privacy. Canadians have a growing interest in the accuracy, completeness and relevance of records that are held by government agencies. Critics suggest that to protect privacy interests the activities by governments must be limited and challenged.[15] One author describes how the use of individual files to determine eligibility for benefits and services and to check against other files "...permits the government to implement its will within society."[16] David Sadofsky argues that: "To interact with the bureaucracy, the individual must be willing to release information demanded by the form. To fail to release information is cause for the bureaucratic machine to reject the applications."[17] In

[13]Flaherty, David H. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." Science, Technology, & Human Values, Vol. 11, Issue 1 (Winter 1986), p.8.

[14]Eva Etzioni-Halevy (1983). Bureaucracy and Democracy: A Political Dilemma. London, Routledge & Kegan Paul. p. 2.

[15]David Sadofsky (1990). Knowledge as Power: Political and Legal Control of Information. New York, Praeger Publishers. p. 9.

[16]Ibid. p. 15.

[17]Ibid. p. 19.

many cases the individual may not be able to question why certain types of information are collected or "whether personal privacy truly outweigh[s] the agency's information requirements."[18] In recent years governments have used an efficiency argument to promote the sharing of information among departments, ministries and agencies. Sadofsky warns of the dangers associated with cross-referencing data to other agencies as: "The value of efficiency and the inapplicability of the value of privacy allow bureaucracies to utilize information as an organizational resource."[19] Two American examples illustrate problems from the multiple use of information by government agencies.

In the United States, the New York Controlled Substance Act permitted a state agency to require doctors and pharmacists to report the prescription of Schedule II drugs such as cocaine, methadone, amphetamines. These drugs help to ameliorate pain in the treatment of various illnesses.[20] Each month approximately 100,000 Schedule II prescription forms were submitted to the New York State Department of Health. The purpose of the collection by the agency was to identify criminal abuse by monitoring the legal use of controlled drugs. During the first twenty months of operation, Sadofsky notes that only two cases had sufficient cause for investigation. An Appellate Court in the United States ruled that the Department's practice interfered with constitutionally protected 'zones of privacy' that, "...includes one's own body and one's professional relationship with a personal physician."[21] A second example is the US Health and Human Services' decision to "equip pharmacies with computers to keep track of medicine dispensed to 32 million recipients of Medicare [and] another tabulation by that agency of disciplinary actions taken against licensed health practitioners..."[22] Given the serious implications to personal privacy

[18]Ibid. p. 19.

[19]Ibid. p. 20.

[20]Ibid. p. 53.

[21]Ibid. p. 54.

[22]Ibid. p. 16.

illustrated in the two examples, the concerns voiced by privacy advocates on the potential misuse of a computerized drug network may not be overstated in British Columbia. One of the primary concerns is the new opportunity available to the bureaucracy to monitor the entire population or to assist in law enforcement.

Government agencies will collect information about citizens and expertly use this information for decision-making. Three issues of particular importance are the accuracy of agency records; the use of records for other purposes beyond the original collection and the release of personal information. By legislating the right to access personal information, the individual has the opportunity to discover inaccurate or incomplete records that may create obstacles for future benefits. It also places some responsibility on the agency to update and verify records. A legislated right to privacy allows individuals to limit disclosure and monitor the use of personal information by agencies. The content of agency files and the rationale for decisions are beyond the reach of the individual without adequate legislative safeguards. The statutory protection of access and privacy rights may help individuals in challenging agency authority and scrutinizing bureaucratic activities. Information technology presents new opportunities to control and regulate government programs and alters the relationship between the citizen and the state.

Information Technology and the Control of Government Programs

The expansion of government programs and the introduction of computer technology in government operations have changed the relationship between the citizen and state. A number of large-scale information systems permit less individualized response to citizens as the provision of some services becomes impersonal.[23] Sadofsky makes a similar comparison "...instead of dealing with the whole person, the bureaucracy reduces decisions regarding individuals to the contents of

[23]David F. Andersen and Sharon S. Dawes (1991). Government Information Management: A Primer and Casebook. New Jersey, Prentice-Hall, Inc. p. 118.

predefined forms. The individual cannot introduce any factors unrecognizable by the form."[24] David F. Andersen and Sharon S. Dawes suggest the expansion of the psychic, geographic and social distance between citizens and state increase from data collection and intervention. They argue that, "...the possibility for fraud and abuse of removed, complex government programs has led to a widespread and politically popular call for increased accountability and auditability of government records."[25] The Canadian Medicare System is one example of a government program facing increasing calls for accountability.

The provincial Ministries of Health represent one government agency responsible and accountable for the administration of Medicare and health programs to the public: "To achieve public accountability, information must be collected, stored, and verified against other sources (some of which are databases maintained elsewhere by the government)."[26] Technology alters the processes of government operations as: "The interaction between what is technically possible and what is politically viable offers a constantly changing set of programmatic initiatives and policy choices."[27] An agency will use various sources of information to achieve accountability for its program. B. C. Smith suggests that: "The evil is not bureaucracy as such, but the expansion of the sphere in which bureaucratic management is applied."[28] Information technology presents new opportunities to delve more persistently into private affairs. A number of technological tools are "...used to cross-check among various programs to prevent fraud and abuse and, as a result, cut the size and cost of government."[29] Technocrats will have greater responsibility with the large scale

[24]David Sadofsky (1990). Knowledge as Power: Political and Legal Control of Information. p.19.

[25]David F. Andersen and Sharon S. Dawes (1991). Government Information Management: A Primer and Casebook. p. 118.

[26]Ibid. p. 78.

[27]Ibid. p. 79.

[28]B. C. Smith (1988). Bureaucracy and Political Power. New York, St. Martin's Press, Inc. p. 26.

[29]David F. Andersen and Sharon S. Dawes (1991). Government Information Management: A Primer and Casebook. p. 78.

information systems that guide and control government programs. The impact is some degree of public intrusion into the lives of private citizens. The information generated by agencies of the government will be useful to the public.

The government is a source of public knowledge. Information technology facilitates this function. "Some contend that information is a right of citizenship...others see government's responsibility fulfilled by the collection, storage, and preservation of data..."[30] Public and private organizations, including businesses; students and researchers from the academic community use information collected by public institutions. The statistical reports generated by Statistics Canada and Health and Welfare Canada represent two examples of well-known and highly respected sources of information originating from public institutions. The bureaucracy's responsibility to protect and secure the records under its control increases as the value and quantity of information grows.

Information technologies place new demands on agency operations. Governments adopt the role of trustee and manager of public information.[31] Government agencies are responsible for ensuring the physical security of information used for public programs, the maintenance of past records and make decisions on "...how and when to archive electronic data, who should have access to what information at what cost, and in how timely a fashion."[32] Managers of public information face a number of competing responsibilities. "...[T]hey manage one of the most important assets of democratic government - information about what government does and how it does it...on the other hand, they must handle sensitive personal data that deserves special protection from disclosure."[33] Government agencies are managers of large quantities of information and increasingly are held

[30]Ibid. p. 81.

[31]Ibid. p. 81.

[32]Ibid. p. 81.

[33]Ibid. p. 111.

responsible and accountable for the protection of personal information in their possession. This is very important as individuals applying for government benefits and services provide very intimate details about themselves and often forfeit their right to privacy in the relationship.

Information technology, according to critics, creates a fundamental change in the relationship between the citizen and the state.[34] Individual rights or claims may not counterbalance the collection practices of large bureaucratic institutions. New technological tools that can enhance efficiency in government administration raise fundamental questions about individual rights. Questions concerning how far government agencies may pursue efficiency before they begin to infringe on personal privacy occupies the attention of privacy advocates, civil libertarians, and the public. Recent developments in the area of health information management in British Columbia provide an opportunity to explore some of these questions.

Health Information Management in British Columbia

Modern computer systems enhance the administrative abilities of agencies to provide benefits, services and to satisfy public expectations for fast service provision. Recent attention by the provincial government focuses on using health information management to improve the entire health care system. The British Columbia Ministry of Health and Ministry Responsible for Seniors (MOH) in one report stated: "The vision for Health Information Management in British Columbia is to effectively and efficiently manage information so as to support the health system."[35] The province spends approximately $60 to $100 million on health information systems activities and the annual cost for capital expenditures is $8 to $15 million.[36] In response to rising health care costs and budget cuts, agencies seek new ways to manage information.

---

[34]Ibid. p. 113.

[35]British Columbia, Ministry of Health and Ministry Responsible for Seniors (1995). Vision for Health Information Management in British Columbia. Health Information Management Project, Victoria, May. p .2.

[36]Ibid. p. 10.

A 1991 provincial report *Closer to Home: The Report of the Royal Commission on Health Care and Costs* identified a number of factors that will lead to a more cost effective health system. These include: better health; greater public participation and responsibility; bringing health closer to home; respecting the care giver; and effective management of the health system. The Royal Commission pointed to inter-sectoral sharing of health information as an important component of an integrated health system.[37] "Integration implies an efficient and effective flow of information to minimize the boundaries between organizations, and promote a continuity of care; to build a partnership among all elements of the health system."[38] The MOH believes that the five directions advanced in the Report will be achieved by information management. The goals for health information management set out by the MOH are as follows:

> Clearly identify and gather uniformly defined information necessary to plan, manage, operate and evaluate the health system; ensure information accuracy, consistency and integrity; ensure appropriate access to consistent information; integrate information across service delivery, functional, geographic and jurisdictional boundaries as required; minimize capital and operational information systems costs and continually evaluate information systems in relation to benefits produced; and ensure compliance with freedom of information and protection of privacy law.[39]

To achieve these goals a number of key principles for information management were recommended. One of the most important principle is to use "person-based systems [that] will hold a health record for each individual that can be referenced to that person's Personal Health Number (PHN)."[40] In addition, information would become available in whole or part to other designated health systems through linkage of systems and information entered on a computer. Health professionals will obtain the information from the operational systems at work sites. Once

---

[37]Jenny Karim. Sharing Health Information: The B.C. Scenario. Prepared for the Provincial Health Information Management Steering Committee and the Ministry of Health, Victoria, April 1993. p. 1.

[38]Ibid. p.1

[39]British Columbia, Ministry of Health and Ministry Responsible for Seniors. Vision for Health Information Management in British Columbia. p. 3.

[40]Ibid. p. 4.

common standards and health system-wide networking are developed information will be shared across the system. Only information necessary to make decisions will be collected and must be timely, accurate, reliable and have integrity. The security and confidentiality of data are essential principles. Authorized individuals will receive information on a need to know basis. The MOH envisions for the future a province-wide health information sharing network, called HealthNet/BC, that would allow access to information in two ways.

First, an information sharing facility allows databases to be shared between communities, regions, hospitals, individual providers and the MOH. Second, an open Data Network provides access to multiple computer systems and databases in the health system. The network would enable local area networks and a provincial health information network to be interconnected.[41] To achieve the overall goal of information management, a number of components are necessary. First, the Personal Health Number (PHN) must be adopted as a province-wide unique identifier for all British Columbians in the health system. Second, electronic patient records or longitudinal health records will have to be used by all service providers to facilitate service integration and to capture operation information. Third, the confidentiality and privacy principles in privacy legislation must be followed so that only information required is collected and appropriate access is given. The MOH considers information sharing an important component for a cost effective health system.

In British Columbia information exchange activities involve many segments of the health system including hospitals, public health units, the private sector, health affiliated organizations, and the MOH.[42] A 1993 study commissioned by the British Columbia Provincial Health Information Management Steering Committee and the MOH revealed the level of health information sharing activity in the province.[43] Questionnaires were mailed to five health sectors. These include:

[41]Ibid. p. 6.

[42]Jenny Karim. Sharing Health Information: The B.C. Scenario. p. 15.

[43]Ibid. p. i.

hospitals, public health units, MOH offices, private sector and health affiliated organizations. The response to the survey by 101 hospitals, 47 public health units, 79 MOH offices and headquarters, 47 private sector, and 77 health affiliated organizations indicated that 173 clinical and administrative systems exist in the health system.[44] The 173 systems include province-wide, community based and institution based systems. The medium of exchange identified were 106 electronic, 30 manual and 37 using both types. Out of the 173 projects, 69 share client specific information for prevention and treatment; 23 involve sharing of non-identifiable client information for administrative, research, planning and evaluation; and 81 projects involved client specific and non-specific information exchanges.[45] The extensive nature of information sharing activities in the province led the researchers to formulate some important questions related to the protection of health information. These include:

> Should all of a patient's health information be able to be linked? If not, to what extent do we need linkage? Who should such a record belong to? Are health providers willing to share patient information? What are the legal ramifications of sharing patient information? To what extent is there a need for a mechanism/structure to allow the linkage of all patient information so a complete profile can be constructed?[46]

An attempt to answer any one of these questions will require careful consideration of the threats to confidentiality and privacy of patient records from record linkage. A study by the Science Council of British Columbia highlights the growing popularity of health information sharing activities among several countries.

In 1992, SPARK Health Sector of the Science Council of British Columbia investigated health information sharing initiatives in Canada, the United States, the United Kingdom, Sweden, Norway, Netherlands, France, Germany and Singapore. Among the fifty information systems examined four types of technologies were used: card technology; electronic data interchange (EDI)

---

[44]Ibid. p. i.

[45]Ibid. p. 5.

[46]Ibid. p. 10.

and electronic mail (E-Mail); database and telehealth.[47] The SPARK Report noted that the concept of sharing health information is gaining momentum as a cost containment strategy and is defined as "...the concept of creating and/or improving the accessibility and/or distribution of health information."[48] The Report noted that: "Sharing information between health care providers can assist with increasing the quality of patient care and cost containment. These two goals can be achieved by decreasing duplication and errors, preventing harmful interactions of drug-drug, drug-disease and drug-test, and increasing efficient resource utilization."[49] The four types of technology identified in the SPARK Report are presently in use in the British Columbia health system. Database and card technologies have considerable support from the government of British Columbia. First, the MOH which is responsible for Pharmacare a provincial drug plan recently implemented a computerized drug network system. The Pharmanet System's goals are to assist pharmacists in identifying potential drug interactions; potentially reduce hospital admissions; discourage multi-doctoring; and prevent abuse of prescription drugs and fraud. Second, the MOH issues personal health cards and discussions on the development of provincial identity cards or multi-purpose identity cards are underway in the province.

Pharmacare and Pharmanet

In 1974, Pharmacare was first established to assist in the payment of prescription drugs and some medical supplies for seniors.[50] Before Pharmacare, the provincial government reimbursed the prescription costs for recipients of social assistance. In 1977, families in British Columbia became eligible for coverage under a separate plan. By 1987, seniors were paying a portion of their

[47]Science Council of British Columbia. Sharing Health Information: An Overview of Fifty Projects. SPARK Report Strategic Planning for Applied Research and Knowledge. Prepared for SPARK Health Sector: Health Informatics Working Group, Burnaby, January, 1992. p. 1.

[48]Ibid. p. 3.

[49]Ibid. p. 4.

[50]British Columbia, Ministry of Health and Ministry Responsible for Seniors. Shaping the Future of Pharmacare. Victoria, May, 1993.

prescription costs. All provinces have a drug plan that exists outside of the medicare system and provides coverage to seniors and individuals receiving income assistance. Medicare only pays for the cost of doctors and hospital care. In British Columbia residents are automatically eligible for Pharmacare by registering with the Medical Services Plan. Six separate plans presently exist in the system. Pharmacare coverage varies with age, although it is not dependent on one's ability to pay. A senior with low or high income will pay the same. A working family with low or high income will pay the same premiums. The overall cost of Pharmacare is significant.

The annual cost of the program has been doubling in the last five years. During 1987/88 to 1992/93 expenditures have risen from $160 million to $346.7 million.[51] "That's the equivalent of 28 cents for every dollar...spent on the services of doctors, or 13 cents for each dollar...spent on hospitals."[52] The program budget exceeded claims in 1989/90 by $19 million and in 1992/93 by $32 million.[53] Each taxpayer in British Columbia contributes over $100 from total taxes to support Pharmacare. Less than 2% of the budget pays for administrative costs. Pharmacare reimburses over ten million prescriptions and represents a major expenditure for the MOH. In response to shrinking provincial health budgets and the rising cost of Pharmacare, the MOH introduced Pharmanet a province wide computer network that will record the drug history of the entire population.

One recommendation by the British Columbia Royal Commission on Health Care and Costs was the implementation of a province-wide pharmacy network. In particular, the Commission recommended:

---

[51]Ibid. p. 6.

[52]Ibid. p. 3.

[53]Ibid. p. 6.

> Pharmacare foster the development of an electronic network linking all physicians, pharmacies, hospitals, and intermediate care facilities so that physicians and pharmacists have access to: the diagnosis, medication profile, and allergy status of a patient; information regarding potential drug/drug and drug/disease interactions; prescribing guidelines compiled by the Drug Usage Review; [and] information available through the Drug and Poison Information Centre.[54]

The idea for a network was under consideration for several years before the Royal Commission's Report. The College of Pharmacists of B.C., the B.C. Pharmacy Association, the government, the provincial Coroner's office and various health care professionals were in support of the system.[55] Pharmanet is the MOH's new computerized pharmacy network and benefits to the public include:

> Protecting citizens form dangerous drug interactions and overuse of prescription medications; providing current drug monograph information to allow more informed consumption of prescription medications; providing electronic claims coverage at point of sale, thus eliminating the time consuming wait for Pharmacare coverage reimbursement.[56]

The MOH built the system and the College of Pharmacists and the British Columbia Pharmacy Association are equal partners. In the summer of 1995 connection to the system was a requirement for all community pharmacies. Pharmanet consists of a telecommunication link to each pharmacy and a set of central data systems that administer drug usage and Pharmacare benefits. Pharmanet receives the details of each prescription being dispensed at individual pharmacies through electronic transmission. The central system determines the portion of the cost that is eligible for Pharmacare reimbursement. All patients require a Ministry of Health Personal Health Number (PHN) to fill a prescription. Payments to pharmacists by Pharmacare are automatic and save on administrative paperwork. In addition, the performances of drug utilization evaluations (DUE), permit assessment of the prescription profile of patients in the previous fourteen months. Pharmanet will provide the following information to the pharmacist.

> Confirmation of the prescription costs to be covered by Pharmacare; any warning messages from the DUE checking, including drug-to-drug interactions, and over

---

[54]British Columbia. Closer to Home: Royal Commission on Health Care and Costs. Victoria, 1991.

[55]British Columbia, Ministry of Health and Ministry Responsible for Seniors. PharmaNet - The Basics. Victoria, (unpublished) no date.

[56]Ibid.

> medication warnings; a full "profile" of all medications previously dispensed to the patient during the previous fourteen months; the profile will also contain any reported adverse drug reactions or clinical conditions (e.g., diabetic, etc.).[57]

The system will assist pharmacists in identifying and preventing a number of serious prescription problems that were identified in a study.

In 1992, a study conducted by the B.C. College of Pharmacists during a six month period identified a number of prescription problems in the province.[58] The forty-eight participating pharmacists reported 1,450 prescription problems including the wrong dosage (25.3%); the wrong strength (21.7%); a patient history of allergy (19%); the ordering of the wrong drug (15.5%); or inappropriate drug (2.2%); adverse drug reaction (3.0%) and other (11.9%).[59] Jenny Karim writes that: "In British Columbia, Ministry of Health statistics report over 7000 hospitalizations due to drugs causing adverse effects in therapeutic use in 1992/93."[60] The benefits to the provincial government include a reduction in administrative costs associated with the Pharmacare program, a decline in fraud and overcomsumption of prescription medications and the ability to implement changes to Pharmacare benefits and plans with minimal disruption. A number of security measures are in place to protect the privacy of prescription information.

The pharmacy manager is ultimately responsible for the security of the system and must play an active role in training his/her staff. The pharmacist or a designated support person who is under the supervision of a pharmacist can check the Pharmanet database.[61] The pharmacy workstation

---

[57]Ibid.

[58]Karim, Jenny. Clinical Data Supporting the Need for a Pharmacy Network. Prepared for Ministry of Health and Ministry Responsible for Seniors. Victoria, February, 14, 1994, unpublished, p.4. Karim describes a study conducted by S. Eng-Kerr and T. Stratton. "Prescription Intervention by British Columbia Community Pharmacists." B.C. College of Pharmacy Study, 1993.

[59]Ibid. p. 4.

[60]Ibid. p. 3.

[61]Personal interview with Linda J. Lytle, Registrar, College of Pharmacists of British Columbia. Refer to Chapter V.

will be de-activated if it sits idle for some time. To access Pharmanet operators must identify themselves and only pharmacies with authorization can use the system. Pharmanet prohibits dial-in access. The transmission of personal data from each pharmacy to Pharmanet has the protection of encryption. The system will detect browsing by logging each access to a patient's file and recording the information on a medication profile. A patient may obtain a print out of this profile from the College of Pharmacists. The B.C. College of Pharmacists' Registrar states; "Only patients or their agents may write to the College to request a printout of their prescription records since a pharmacist cannot provide or request a patient record."[62] The College will be able to monitor requests made by users of the system to view patient profiles. Bylaw B20 of the Pharmacists, Pharmacy Operations and Drug Scheduling Act imposes penalties on pharmacists contravening the Act. Patients also have the option to select a keyword to restrict access to their medication profile. Only the College of Pharmacists and the College of Physicians and Surgeons can bypass the keyword to see a medication profile.[63] A number of privacy issues were raised by the Provincial Information and Privacy Commissioner, a public interest association and civil libertarians during the implementation of the Pharmanet system.

Much of the opposition to the MOH's Pharmanet system was voiced by David F. Flaherty, the Information and Privacy Commissioner. Flaherty argued that,

> Pharmanet represents a kind of sad search for a technological fix to the social and economic problems of our society. The hope for such a technological fix is an enduring trait of the late twentieth century. Pharmanet is indeed a technology in search of an application. We are going to automate and link prescription forms on a province-wide basis, because we can do it and because we think it can solve some problems.[64]

---

[62]Ibid.

[63]British Columbia, Ministry of Health and Ministry Responsible for Seniors. PharmaNet - The Basics. Victoria, (unpublished) no date.

[64]David H. Flaherty. Pharmanet and Personal Privacy. Vancouver, Information and Privacy Commissioner, March 17, 1994. p.2.

One serious criticism of the Pharmanet program was the lack of public consultation in the province. According to critics, policy guidelines did not readily follow the technological developments. The technology was guiding the policy making process. Flaherty asserts,

> Despite the spirit of greater openness and accountability explicitly adopted by an unanimous-legislature in creating the Freedom of Information and Protection of Privacy Act, I regret a system of policy making that waits to the very last minute for public consultations on such an important matter. That is why I totally reject any argument that Pharmanet must go forward because money has already been spent on it.[65]

Darrell Evans, Executive Director of FIPA notes that the public consultation promised by the MOH turned out to be public information sessions. Public consultation and debate were minimal.[66] The College of Physicians and Surgeons was consulted briefly on Pharmanet just before implementation.[67] Among the many arguments opposing the Pharmanet system, there are two major concerns.

First, the Information and Privacy Commissioner, FIPA and the BCCLA consider the compulsory nature of the Pharmanet program one of its fundamental weaknesses. Flaherty argues that the "...notion of voluntarism is at the heart of the fundamental concept of information self-determination."[68] Evans argues that: "Bureaucrats lean more favourably towards universal and comprehensive programs, with little exception."[69] Flaherty warns "...it will be mandatory for anyone in the province seeking a prescription, and there are no provisions that forbid an employer

[65]Ibid. p. 1.

[66]Personal interview with Darrell Evans, Executive Director of the Freedom of Information and Privacy Association (FIPA). Refer to Chapter V.

[67]Personal interview with Dr. M. Vanandel, Deputy Registrar, College of Physicians and Surgeons of British Columbia. Refer to Chapter V.

[68]Flaherty, David H. Provincial Identity Cards: A Privacy-Impact Assessment. Notes for a Presentation on September 26, 1995. Victoria ,unpublished. p. 2.

[69]Personal interview with Darrell Evans, Executive Director of the Freedom of Information and Privacy Association (FIPA).. Refer to Chapter V

or other third party from requiring you or me to produce a printout from the system for review."[70] Conversely, proponents note that a mandatory system involving all pharmacies would help to eradicate abuse of prescription drugs and prevent patients from visiting a pharmacy that is not connected to the network.[71] Second, critics suggest Pharmanet will function as a surveillance system over the entire population. The information compiled may serve multiple purposes beyond its original intent. Flaherty points to police, law enforcers and the Motor Vehicle Bureau who may want to have access to the system to locate a suspect or determine eligibility for a driver's license.[72] Job applicants may face challenges to provide a medical profile of their drug use. These scenarios may never be realized. Nevertheless, the potential exists for agencies of the state to use a system that contains the drug history of an entire population to achieve other administrative goals. The proposals for advanced card technology such as a provincial identity card has also raised concerns about the potential surveillance by the state over the entire population. Patients currently use a variety of card technologies to access services in the Canadian health care system. With the advancement of universal cards serving multiple functions the need for information self-determination may become more pervasive.

Card Technology

The development of card technology permits the storage of vast quantities of information on plastic wallet-sized cards. In the health care sector, applications of this technology involve collection, retention, use and disclosure of personal information. The types of card technology available to collect and share information include embossed circuit cards (memory chip cards and smart cards),

---

[70]Flaherty, David H. Pharmanet. Excerpt from a speech presented to University of Victoria, School of Law, British Columbia, February, 7, 1995.

[71]Personal interview with Linda J. Lytle, Registrar, College of Pharmacists of British Columbia. Refer to Chapter V.

[72]David H. Flaherty. Pharmanet and Personal Privacy. Vancouver, Information and Privacy Commissioner, March 17, 1994. p. 2.

and optical storage cards.[73] The application of each type of card will vary. The first advanced card was the embossed plastic card that was introduced in the late 1940s and achieved wide acceptance by the 1960s and 1970s. Canadians use embossed plastic cards such as Social Insurance Number cards, hospital identification cards, library and membership cards. The embossed lettering can hold the name of the card holder, account number and may contain a signature stripe on the back. In the late 1970s, major credit card companies began to use magnetic stripe cards that consist of a thin stripe of magnetic material on the surface. A code represents the data stored on the stripe. The magnetic stripe card stores up to 240 characters of information and can be updated. The cards are presently used for credit and debit transactions, for automated banking machines, health cards and club memberships. The card does not store sensitive data although small amounts of information can be encrypted. Moreover the cards can be damaged, counterfeited and are usually limited to one application. Three provinces use one type of magnetic stripe card, the personal health card.

Personal Health Card

Magnetic stripe cards are used as personal health cards in Saskatchewan, British Columbia and Ontario. British Columbia, beginning in 1989, issued health cards. The Care Card is a magnetic stripe card that includes the following information: personal health number, identity number, and dependent number (linking the individual to his/her family), unit type (i.e., type of health insurance program to which the individual belongs), card issue and expiry date, date of birth, and full name.[74] At present, British Columbians use the personal health card to obtain health services. Future use may include linkage of cards to a central database.[75]

---

[73]Tom Wright. Health Card Technology: A Privacy Perspective. Toronto, Information and Privacy Commissioner/Ontario. October 1992. p.i.

[74]Ibid. p. 9.

[75]Ibid. p.9.

One trend in the health sector is promoting the personal health card as a tool for increasing the quality of health care and reducing costs. The card can serve a number of purposes. These include, providing identification and access to health services, facilitating benefits and claims processing, storing pharmacy and clinical records, gathering data on the utilization of health care services and facilities, patient monitoring, controlling access to health information, and as a marketing and public relations device.[76] The inclusion of benefits and claims data would enable the identification, access and reimbursement of health services. Proponents believe it may prevent overuse or deliberate misuse of pharmaceuticals and mixing of drugs by the elderly. It may also reduce the incidence of multi-doctoring by individuals addicted to narcotic prescriptions. The personal health card has the capacity to carry clinical records and information such as family medical history, immunization information, diagnoses, visits, test results, physician notes and referrals.[77] Several advantages exist for the use of full records. First, the card would assist in tracking services and facilities by gathering data. "This would allow insurers, providers, and health care policy makers to track and analyze disease trends, pharmacy costs, patient use of their services and other factors that may have an effect on planning."[78] Second, proponents view the widespread use of card technology as a valuable tool for administering government programs. The card may be useful for gathering information for health care planning. One major benefit envisioned by the health service industry is the potential to monitor the entire health care system. Critics suggest the risks to individual privacy may be too high.

The widespread implementation of advanced card technology in the health sector raises issues about the protection of personal information. Technologies that facilitate the collection, storage and disclosure of health information challenge the individual's ability to maintain control over the

[76]Ibid. p. i.

[77]Ibid. p. 6.

[78]Ibid. p. 6.

data. Privacy advocates such as the Information and Privacy Commissioner of Ontario argue that, "... it will be difficult for health care providers to resist copying this information, for their own records or for sharing with others for planning and research purposes."[79] The proliferation of databases containing vast quantities of medical information and the possibilities for linkage pose threats to privacy. The ability to exercise control and limit the use of health information may be increasingly difficult as computer and telecommunication technologies expand. Proponents of the smart card believe it will alleviate some concerns on the misuse of health information due to its portability and independence.

Smart Card

The smart card represents one type of computer readable card technology. Smart cards are "...credit-card-sized plastic devices that contain microscopic integrated electronic circuits, [that] can provide the user with both a secure method of storing and carrying personal information with a way to access resources in a network of computers."[80] The card can store up to sixty-four kilobytes of information and may be erasable or nonearsable. At present, there are three types of applications for the smart card: a portable medical record; an electronic chart; and for securing access to confidential databases.[81] The primary goal of the smart card is to provide better information for health management and planning. In addition, the card would empower individuals by providing more information about personal health and health care. The health care system can use the smart card to manage and communicate health information. As a portable patient record, the information on the card may include, the individual's health history such as illnesses, chronic conditions, operations, preventive health information, blood type, drug sensitivities and current

[79]Ibid. p. 12.

[80]Christel A. Woodward and Lynn Curry (1992). "The Health Encounter Card Pilot Project: An Innovation in Health Care." Health Care Innovation, Impact and Challenge. Edited by S. Mathwin Davis. Kingston, School of Public Administration, Queen's University. p. 53.

[81]Science Council of British Columbia. Sharing Health Information: An Overview of Fifty Projects. SPARK Report Strategic Planning for Applied Research and Knowledge. Prepared for SPARK Health Sector: Health Informatics Working Group, Burnaby, January, 1992. p. 6.

medications.[82] Health professionals attending to a patient would be able to read the card on a need-to-know basis and update the information after each health care encounter. To read a smart card, health care providers in Canada for example, may require an access card, a personal identification number and registration with the MOH. The use of smart card technology does offer some advantages to consumers, health care providers, the MOH, professional licensing bodies and health researchers.

From the perspective of consumers, the smart card will increase the individual's role in personal health care. The card would allow consumers to communicate more effectively with health care providers. The Ontario MOH envisions a number of additional benefits to the patient. "Many consumers have a less than complete awareness of the health care that they have received (types of medication prescribed, diagnostic tests done, purpose(s) of encounters, dietary or exercise instructions' referrals made, etc)."[83] During emergencies, health providers would be able to respond appropriately to patient needs by accessing medical information stored on a card. Providers and agencies of health care will benefit by having accessible information on a card in emergency cases. The recording of a patient's medical history, health conditions, treatment and medication profile will assist the health care provider. The card will facilitate communication among providers of health care especially for treatments that require the services of various practitioners in the field. Physician review of prescription renewal information would help to identify medication problems, duplication of services and problems of patient compliance.

---

[82]Christel A.Woodward and Lynn Curry. "The Health Encounter Card Pilot Project: An Innovation in Health Care." Health Care Innovation, Impact and Challenge. p. 53. Woodward et al. also describe the types of data elements included on a smart card used as a portable patient record in The Encounter Card pilot project in Ontario. These include, biographic data (health number, name, address, birthdate, sex, official and spoken language), emergency contact information, vital medical history (drug sensitivities and other allergies, immunization record), personal and private information (medical/health problems, chronic conditions, significant test results, family history, provider notes), service encounter history (current medications, expired medications, medical service encounters, hospital service encounters, radiology encounters, laboratory encounters and allied health-care encounters). p. 62.

[83]Ibid. p. 56.

At each health encounter the updating of the smart card provides timely information to the MOH. The identification of specific health problems may lead to improvements in planning for health care needs. The MOH would have information on the types of services used to treat conditions. The information would facilitate planning for health care needs and help to identify services authorized for specific conditions. Public Health Units can use the information to determine the immunization status of children. The inclusion of prescription drug information and diagnosis will permit drug utilization reviews. The new technology may track behaviours and result in policies to prevent abuses such as drug interaction and multi-doctoring. The elderly represent one segment of the population that will benefit from the card due to the large number of visits to hospitals as a result of drug interactions. Doctors are often not aware of the complete prescription history of a patient.

The benefits to professional bodies may include monitoring members' standard of care, developing new standards or guidelines and providing continuing education. Christel A. Woodward and Lynn Curry describe how "...easily retrieved, uniform, patient based information is not available about health-care activities of providers and the patterns of care sought out by consumers."[84] The card may be useful in monitoring the practices of health care providers and pharmacists. From the perspective of health care researchers, the smart card will permit higher quality research by generating new types of information. "Health-care researchers are often interested in describing patterns of care and factors that appear to influence those patterns and in examining the relative effectiveness or efficiency of various health-care services and delivery systems."[85] Proponents of smart card technology envision substantial benefits for the health care sector. A number of projects and experiments with smart cards have been initiated in several jurisdictions.

---

[84]Ibid. p. 59.

[85]Ibid. p. 59.

In the province of Ontario, the Ministry of Health (MOH) initiated The Encounter Card Pilot Project between July 1, 1992, and February 25, 1993, to examine the feasibility of using smart card technology as a personal health card.[86] The impetus for the project was the result of numerous reports by the MOH espousing "...a stronger role by individual consumers in health and health-care matters, greater integration of health-care delivery systems and a more active management of health-care system in partnership between the MOH and the health professionals."[87] The information system designed in the 1970s to administer the universal health insurance plan no longer met the changing needs and goals of health care. The project in Fort Frances included 2,193 smart cards that were issued to volunteers and involved 14 physicians and 66 nurses, pharmacists and hospital staff in two local hospitals. The study found that the public did not have any serious confidentiality concerns with the use of a smart card. One of the drawbacks to the project was the physician's resistance to the additional time required to input the data. Robert M. MacIntosh describes how "...the biggest single obstacle to the smart card is the cost and the methodology of transferring information from doctor's sometimes hodgepodge personal files to a database requiring very disciplined input."[88] In addition the individual entering the data must respect the confidentiality of the patient's files. The use of smart cards does raise some troubling questions:

> How will the patient be assured that only relevant information is assessed by appropriate individuals and organizations? Will the information on the card always be accurate and reliable? Who is ultimately responsible for the integrity of the card, the vendor, the individual, or the health care professional? Will the information on the card be used only for the patient's care or will it also be used for purposes such as employment and insurance screening? What information will be stored on the card? Will failure to present a card result in refusal of service?[89]

---

[86]Robert M. MacIntosh. Information Technology for Health Care in Ontario. Backgrounder. Toronto, C.D. Howe Institute, January 12, 1995. p.4

[87]Christel A.Woodward and Lynn Curry. "The Health Encounter Card Pilot Project: An Innovation in Health Care." Health Care Innovation, Impact and Challenge. p. 54.

[88]Robert M. MacIntosh. Information Technology for Health Care in Ontario. p. 4.

[89]Science Council of British Columbia. Sharing Health Information: An Overview of Fifty Projects. p. 13.

The questions represent some underlying concerns that have emerged in the health policy literature. Confidentiality and privacy within the medical context are important issues since each can affect employment, insurance and social status. The collection and storage of data among a large number of institutions or providers increase the probability of misuse. The governments of Ontario, Saskatchewan, Manitoba and Alberta are experimenting with smart card projects. Several problems involving the use of smart cards are described in the health literature including concerns about privacy.

Critics suggest a number of problems exist with the use of a portable patient record. First, the loss of a card will cause problems in service provision. Second, updating information may pose some problems if patients fail to carry cards to hospitals or physician offices. Third, from an administrative perspective, the distribution of cards may be difficult as the population moves. The President of the Confederation of General Practitioners in Quebec argues that the violation of professional secrecy will occur.[90] Disastrous results would occur if insurers and employers access the files. Donald A. Jardine observes that the use of smart cards entails a tradeoff between public interest and privacy. A number of policy problems will arise from "...a shared record with shared usage...[since]...it is no longer a private one-on-one relationship between the patient and the hospital or doctor."[91] Dependency on the technology may further exemplify the problem. Jardine provides one frightening example. "A young man from Montreal was refused admission at the border to go to his summer home in the United States because the computer system had recorded that he was taking AZT."[92] The development of standards allowing cards to be read from a variety of environments and jurisdictions, by different doctors using a range of computer systems is

[90]Donald A. Jardine (1990). "Health Care Information Technology." Healthy Populace, Health Policy: Medicare Toward the Year 2000. Edited by S. Mathwin Davis. Kingston, School of Policy Studies/School of Public Administration, Queen's University. pp 186-193.

[91]Ibid. p. 192.

[92]Ibid. p. 102.

crucial. Jardine warns the information conveyed must be in a similar manner in which the original writer intended. The province of Ontario has examined the use of universal identification cards and recently announced discussions on the possible implementation of a smart card. This would allow individuals to access a wide variety of services with the use of one card.

In 1994 the Ontario provincial ministries began to examine the feasibility of using a 'Universal ID Card.' MacIntosh opposes the concept of a universal identification card. "Certainly it is technically feasible, because the card can build in passwords for different kinds of access. But it would seem to be getting too close to a 'surveillance card,' which could be very threatening in the hands of a misguided government."[93] McIntosh refers to the BCCLA's response to Pharmanet and warns of the political danger of universality since it would attract opposition from civil libertarians. Recent discussions in Ontario focus on a single smart card to replace "the papers, licenses and certificates residents need to go to the doctor, drive a car, fish, hunt, collect welfare and maybe even vote."[94] The proposal has evoked some debate in the province. The Ontario MOH under the Conservative Government of Mike Harris would like to connect medical databases to allow doctors to obtain a patient's complete history and to investigate fraud. The Federal Privacy Commissioner, Bruce Phillips has reservations about using a smart card and the problems of trying to segregate the various databases. Phillips in response to the Ontario MOH's proposal posed some questions. "Are we trying to make our lives fit technology or make technology fit our lives? What are the rights of the individual in deciding what goes on that card? How democratic is that process going to be?"[95] Earlier the Ontario Information and Privacy Commissioner, Tom Wright issued two reports *Smart Cards* and *Health Card Technology: A Privacy Perspective* that outline some concerns about the use of card technology. In one report Wright recommends that:

---

[93]Robert M. MacIntosh. Information Technology for Health Care in Ontario. p. 4.

[94]"Ontario's move to smart card poses questions about privacy", The Vancouver Sun, March 26, 1996, A9.

[95]Ibid.

> From a privacy perspective, it is preferable to utilize card technology that incorporates the most advanced security features currently available for safeguarding information. Specifically, preference should be given to card technology that incorporates the use of PINs, has the capacity to encrypt information that is transmitted, allows graded levels of access to information on the part of health care professionals, and is not vulnerable to unauthorized reading, alteration, and counterfeiting.[96]

The security features described by Wright are not available on all types of advanced card technology. The smart card offers important security features and has the capacity to encrypt information. One concern voiced by Wright is the possibility that health care professionals may copy the information from the card to a database. The card holder would lose control over the disclosure and use of the personal information. The public and health care professionals have expressed concerns about smart cards.

In 1989, a radio information campaign on health-care issues was conducted by the Ontario Medical Association (OMA). The smart card was a popular issue for discussion among the public and concerns were raised about the confidentiality of patient records. A survey of OMA members revealed two-thirds of physicians support a patient identity card although some were perturbed by the danger to civil liberties. The issues discussed the most included, "...the potential for further deterioration in patient confidentiality, increased opportunity for monitoring of activities, the potential to abuse any information system, the possibility that patient records could fall into the wrong hands, and the potential violation of professional secrecy."[97] The health care professionals and the general public would most likely accept the technology if appropriate safeguards and security features are in place. Wright suggests the essential requirements needed to balance the sharing of information and to protect individual privacy include policies, procedures and legislation. The Information and Privacy Commissioner of British Columbia, David Flaherty, in response to the government's proposal for universal identity cards recommended the use of smart

---

[96]Tom Wright, (Commissioner). Health Care Technology: A Privacy Perspective. Toronto: Information and Privacy Commissioner of Ontario, October, 1992. p. 21.

[97]Ibid. p. 28.

cards with digitized photographs.[98] The government of British Columbia has shifted attention away from the smart card to the universal provincial identity card.

Provincial Identity Cards/Multi-Purpose Identity Cards

In British Columbia the Ministries of Social Service and Health, and the Motor Vehicle Branch of the Ministry of Transportation are examining the potential application of provincial identity cards.[99] Flaherty argues that, "...the prospect of multi-purpose identity cards is the most fundamental privacy issue at the moment in Canada and this province."[100] The inclusion of a unique personal identifier (PIN) in the card would be a "key to a surveillance society." Flaherty questions whether ID cards are "...being imposed on us because of the modern-day urge to worship new and better technology."[101] Flaherty is referring to the widespread use of the Social Insurance Numbers when he states that, "...novel and multiple uses of ID cards will clearly emerge, because of the pressures in our society for efficiency and to prevent fraud, to ensure convenience, and the insensitivity on the part of many to invading the privacy of others."[102] A number of values are at stake with the use of ID cards. These include:

> The right of information self-determination (i.e., to control information about oneself); the right to control disclosure of one's own identity; the right to individual autonomy; the right to be left alone; the right to limit accessibility; the right to exclusive control of access to private realms; the right to minimize intrusiveness; the right to enjoy solitude; and the right to enjoy anonymity.[103]

---

[98]For a complete discussion see David H. Flaherty Provincial Identity Cards: A Privacy-Impact Assessment. Notes for a Presentation on September 26, 1995. Victoria, unpublished.

[99]Ibid.

[100]Ibid. p. 1.

[101]Ibid. p. 3.

[102]Ibid. p. 4.

[103]Ibid. p. 5.

Flaherty believes a smart card would be more secure by giving the individual direct control over the disclosure of personal information.[104] The smart card would make it increasingly difficult for unauthorized individuals to view personal information without consent. Conversely, the Federal Privacy Commissioner, Bruce Phillips and the Ontario Information and Privacy Commissioner, Tom Wright are not convinced the smart card technology systems are fully secure. The types of information technology available to the MOH for health information management in Canada are extensive. Each technological tool presents a further challenge to privacy. Despite reassurances by proponents and the stringent safeguards available, concerns still exist among advocates, civil libertarians and the public.

The decisions made by the British Columbia government to implement Pharmanet and recent discussions on the use of provincial identity cards, according to critics, represent a move towards a surveillance society. This chapter illustrated how the bureaucracy uses information technology to manage health information and achieve administrative goals. In British Columbia there is a growing political will among advocates, public interest groups and the citizenry to safeguard health information and to challenge the methods used by public bodies to collect data. Diverse members of the policy community in British Columbia are striving to hold government and the broad public sector accountable and responsive to privacy issues.

---

[104]"Ontario's move to smart card poses questions about privacy", The Vancouver Sun, March 26, 1996, A9.

Chapter V - Political Agenda Setters: Legislating Access and Privacy Rights

The previous chapters demonstrated a number of important trends in Canada. The most notable is the legislative and judicial recognition of privacy rights, societal claims for information self-determination and the public administrators' growing dependence on information technology to monitor and control government programs. Chapter V focuses on the discussions and debates on access to information and privacy legislation in British Columbia and the role played by members of the policy community. Paul Pross refers to the term 'policy communities' as the relations of pressure groups in a given policy field and government in Canada.[1] Government and elected officials, public interest associations, advocates, academics and the media were instrumental in defining the issues and shaping the legislation on access to information and privacy. The government's decision to amend the FOIPP Act (Bill 50) and include a second tier of organizations using Bill 62 was the result of recommendations within the policy community. During consultation with the broader public sector, some resistance to amendments in the legislation was evident. Personal interviews with staff members from organizations such as hospitals and self-governing professional bodies illustrate some challenges and issues that have emerged with the legislation. Moreover, information practices have improved. In the democratic political process, a number of interests will compete to be heard. Similar to other laws, access to information and privacy legislation may not be responsive to the needs of all interested groups. A variety of interests were influential in shaping access to information and privacy legislation in British Columbia.

The submissions presented by various second tier organizations and associations during public consultation on Bill 62 reflected a divergence of views in the policy community. Public interest associations and patient advocacy groups believed the legislation could have gone further by including records of physicians in private practice. Conversely, some health sector organizations affected by the new regulations argued that it was unnecessary, due to existing guidelines and

[1] A. Paul Pross (1986). Group Politics and Public Policy. Toronto, Oxford University Press.

codes that provided adequate protection to patients. In addition, reference was made to the McInerney v. MacDonald Supreme Court of Canada decision that gave patients the opportunity to examine personal records. It is important to stress that the McInerney v. MacDonald ruling did not apply directly to health records held by hospitals or other health facilities. A significant concern among local public bodies and self-governing professional bodies was the additional resources required to implement the Act. The submissions indicate that cost factors were significant concerns. A number of self-governing professional bodies were perplexed by their inclusion in the legislation for various reasons and adopted a "why me" approach.[2] In comparison to other jurisdictions the legislation is far reaching since it is the only Act of its kind in North America to include self-governing professional bodies. The FOIPP Act represents a compromise among a host of competing factors in the political process. In attempting to balance the various interests, policy-makers were constantly redefining and rewriting the provisions of Bill 50 and Bill 62. The final document as it stands today has undergone changes since its inception, largely as a result of input from different members of the policy community.

Policy Community and Agenda-Setting

Leslie Pal writes that policy community defined broadly will include "...all the relevant actors, as well as the attentive public, who have interests in and influence over policies produced or debated in the sector."[3] The policy sector consists of three categories of policy actors; government; associational and the "attentive public" that make up the community.[4] Executive agencies or ministries, legislative committees, municipalities, commissions and agencies are government actors. Associational actors vary from peak organizations, umbrella groups, unions, professional associations, single issue groups to ad hoc groups. The "attentive public" is represented by

[2]Barry Jones. Appendices to Barry Jones' Report Extending Freedom of Information and Privacy Rights in British Columbia. Victoria, Queen's Printer for British Columbia, 1993.

[3]Leslie A. Pal (1992). Public Policy Analysis: An Introduction. Second edition. Scarborough, Nelson Canada. p. 109.

[4]Ibid. p. 109

academics, journalists, foreign observers and other governments.[5] The actors according to Pal are defined by their commitment, expertise and interest in the policy area. Pross states the policy community because of its functional responsibilities, vested interests and specialized knowledge can acquire a dominant voice in the government's decision-making in a specific public policy area.[6] Pross believes this is permitted by society and accepted by public authorities. In British Columbia a policy community emerged that was concerned with the development of access to information and privacy legislation.

Since the early 1970s a number of Freedom of Information and Privacy Bills was introduced in the provincial Legislature. Access to information and privacy issues were not new to the province. The public although increasingly concerned about privacy was not mobilized to take political action to demand privacy or access rights. During this period the media was a vocal critic of the government's policy or lack of policy on the release of information. By the 1990s political support was growing. A number of individuals and organizations helped to mobilize support and to keep the access and privacy issues high on the political agenda. On August 15, 1990, one public interest group was established called the Freedom of Information and Privacy Association (FIPA). FIPA was formed "...in response to British Columbia's lack of effective public policy and legislation in the information area, and an apparent lack of willingness on the part of government to share public information considered vital to concerned groups."[7] FIPA a non-profit organization proved instrumental in drawing support for a public policy that would provide information rights for British Columbians. Another policy actor, the Ombudsman of British Columbia in 1991, recommended a government policy on fair administrative practices to promote access to information and the protection of privacy. One member from the academic community, Murray

---

[5]Ibid. p. 109

[6]A. Paul Pross (1986). Group Politics and Public Policy.

[7]Evans & Hay Freedom of Information Bulletin: "News Groups Advocates Freedom of Information Law for B.C." News Release August 7, 1990.

Rankin advocated the implementation of legislation and later offered critical evaluation of the governments' draft proposal of Bill 50. The policy field captured the attention of government and associational actors, and the attentive public.

Government Actors

The New Democratic Party during the election campaign promised voters a freedom of information legislation. Pal writes that: "In liberal democracies, political parties compete for power on the basis of programs and platforms consisting of policies. Once in power, they are expected to refine and amend these proposals, implement them, and respond to new public problems..."[8] The Government had to respond quickly since the window of opportunity available to enact this type of legislation was small. Gregory J. Levine notes that the "...legislation is so important to this Government is indicative of provincial history and trends in western liberal democracies."[9] It was the Member of the Legislative Assembly for Burnaby North, Barry Jones whose private member's bill introduced beginning in 1987 that eventually led to the adoption of the FOIPP Act in 1992. The Liberal Party, the official opposition supported the introduction of Bill 50 and in previous years had introduced freedom of information legislation. One member of the legislative assembly, K. Jones felt the scope of Bill 50 should be wider and include local bodies such as school boards, municipalities, health boards and hospital boards without any delay.[10] Moreover, the Ombudsman for British Columbia, was an advocate for fair administrative practices and privacy of information for several years.

---

[8]Leslie A. Pal (1992). Public Policy Analysis: An Introduction. p.13

[9]Gregory J. Levine. "Freedom of Information and Protection of Privacy: B.C.'s New Legislation." The Advocate, Vol. 51, Part 3 (May 1993). p. 381.

[10]British Columbia. Official Report of Debates of the Legislative Assembly. 1st Session, 35 th Parliament. Vol. 4, No. 20. 2737 (June 18, 1992, morning sitting). Victoria: Queen's Printer for British Columbia, 1992.

Before the enactment of the FOIPP Act (Bill 50) the Ombudsman's office dealt with complaints on privacy and access to information issues. The Office was responsible for reviewing the administrative practices of the provincial government. The Ombudsman, Stephen Owen in March of 1991, before the defeat of the Social Credit Government, urged the province to enact policies to address access to information and privacy concerns. In a public report titled *Access to Information and Privacy*, Owen stated that: "A well written policy, [on access and privacy] carefully implemented, could support an effective and non-threatening progression to the introduction of legislation in this area."[11] A policy on public access to government information and privacy was recommended in the Report. Owen noted: "Whether this policy is enshrined in legislation is a matter of public policy to be decided at the political level; that decision is outside the jurisdiction of the Ombudsman's office."[12] Owen felt the Ombudsman's office could effectively implement such a policy. Other Canadian jurisdictions have given the Ombudsman the duties to monitor access and privacy legislation. In March of 1991, the Ombudsman emphasized the need for a policy while speaking at the B.C. Information Rights Conference in Vancouver that was organized by FIPA and Murray Rankin.[13] Other commentators in the province have expressed specific concerns about patient access to personal health care information. The 1991 Royal Commission on Health Care and Costs found that individuals were denied access to personal medical records. Paul Williamson, counsel to the Royal Commission wrote: "I can state that as the commissioners traveled the province they repeatedly heard stories of access-denied individuals."[14] In its final report the Royal Commission concluded that: "The patient should have access to the

---

[11]Stephen Owen (Ombudsman). Access to Information and Privacy. Public Report No. 26. Presented to the British Columbia Legislative Assembly. Victoria, March 15, 1991. p.3.

[12]Ibid. p. .3.

[13]"Open access to information, B.C.'s ombudsman urges", The Vancouver Sun, March 18, 1991, A1.

[14]Barry Jones. Barry Jones Report: The Extension of Citizen's Information and Privacy Rights to all Public Bodies in British Columbia. Presented to the Attorney General, Chair, Cabinet Caucus Committee on Information and Privacy. Victoria: Queen's Printer for British Columbia, 1992. p. 50

medical record and is entitled to a copy of the contents at cost."[15] Associational actors such as FIPA and the British Columbia Civil Liberties Association (BCCLA) were influential in the policy process.

Associational Actors

In 1990, Darrell Evans received a grant from the Law Society of British Columbia and created a public interest group called FIPA. FIPA's major purpose was to get a Freedom of Information and Protection of Privacy Act passed in British Columbia. In the area of access to information and privacy rights, FIPA was the primary public interest group advocating legislative protection of these rights in the province. The BCCLA also contributed to these efforts. Evans the Executive Director of FIPA, is an advocate for information rights and identifies himself as a key player in promoting the need for legislation in the province, along with law professor Murray Rankin and Barry Jones.[16] Members of FIPA's board of directors and working group include academics, lawyers and librarians. A Task Force was established to develop a legislative framework for access to government information and the protection of privacy. In June 1991, FIPA published a summary of recommendations for law reforms in British Columbia, to provide access to information and privacy rights. The recommendations were published before the Social Credit Government tabled its access to information and protection of privacy exposure bill, on June 24, 1991. FIPA's Legislative Task Force included academics, lawyers and advocates who studied the Social Credit Government's proposed Access to Information and Protection of Privacy Act (Bill 12). On November 7, 1991, two days after the swearing in of the NDP Government, the Task Force released a report titled *Information Rights for British Columbia: Recommendations for Access to Information and Protection of Privacy Legislation for British Columbia.*[17] The Report

[15]Ibid. p. 50

[16]Personal interview with Darrell Evans. Executive Director, Freedom of Information and Protection of Privacy Association, Vancouver, February 3, 1996.

[17]"Time is ripe for information law", The Vancouver Sun, November 18, 1991, A12.

expressed concerns with Bill 12 and provided recommendations for the final drafting of the legislation. One member from the media noted the timing was impeccable.[18] FIPA's Task Force Report according to Jones was the definitive statement on this type of legislation and proved valuable.[19]

The role played by FIPA and advocates in putting the issue of information rights on the forefront of the political agenda are best described by Pal. "Interest and advocacy groups coalesce around certain causes or goals, come up with solutions and policy proposals and then spend most of their time trying to convince authorities that 1) a problem exists; 2) it has the characteristics the group has identified, and 3) the best solution is the one the group has proposed."[20] Pal suggests that, "Defining a problem is a creative act, and a good deal of policy debate involves differing interpretations of what the problems "really" are."[21] FIPA was a key participant at both the developmental stages of the legislation and during the consultative process. The Attorney General, Colin Gabelmann during the committee stage to examine amendments to Bill 50 acknowledged that: "A very small number of these amendments were generated internally. There were a large number generated from external sources -- from groups such as the Freedom of Information and Privacy Association, the media owners' legal counsel...the Canadian Bar Association and the Civil Liberties Association made some suggestions."[22] FIPA strives to keep the issues high on the political agenda by raising public awareness, generating information and educational resources and

---

[18]Ibid.

[19]British Columbia. Official Report of Debates of the Legislative Assembly. 1st Session, 35 th Parliament. Vol. 4, No. 20: 2737 (June 18, 1992, morning sitting). Victoria: Queen's Printer for British Columbia, 1992. p. 2746.

[20]Leslie A. Pal (1992). Public Policy Analysis: An Introduction. p. 128

[21]Ibid. p. 8.

[22]British Columbia. Official Report of Debates of the Legislative Assembly. 1st Session, 35th Parliament. Vol. 4, No. 24: 2869 (June 22, 1992, morning sitting). Victoria: Queen's Printer for British Columbia, 1992.

providing public research in this policy field. Members of the academic community, the media and governments in other jurisdictions were influential in the initial development of the provincial legislation.

Attentive Public

Murray Rankin a professor at the University of Victoria and a practicing lawyer examined briefs, letters and recommendations on Bill 50 that were submitted to the Attorney General.[23] Rankin is considered an expert in the field of freedom of information and privacy legislation. Rankin has actively participated in consultation with various governments on access and privacy legislation and has written extensively in this area. Rankin was an advisor for FIPA's Task Force Report. The response to Bill 50 was extensive and involved input from individuals and organizations in British Columbia as well as other jurisdictions. Among others these included FIPA, the Canadian Bar Association, and a coalition of media companies represented by a Vancouver law firm. Briefs and letters were received from the news directors' association, the BCCLA and other groups. Rankin was asked to examine all the material and make recommendations on how to improve the legislation. Fifty amendments to Bill 50 were recommended by Rankin that were later presented at the committee stage for debate. Several other members from the academic community were also participating in the policy process. David Loukidelis from the University of Victoria is President and Director of FIPA. Loukidelis provided comments on Bill 50 to the Attorney General in June of 1992. Colin Bennett a faculty member at the University of Victoria has written extensively on data protection policies in several countries. Bennett made submissions to FIPA that were included in the Task Force Report. In a recent newsletter published by FIPA, Bennett states: "Indeed there is much of which privacy advocates can be proud. The BC legislation is regarded with high esteem all over the world. Any organization that can plausibly be considered in the "public sector" has to

---

[23]British Columbia. Official Report of Debates of the Legislative Assembly. 1st Session, 35 th Parliament. Vol. 4, No. 20: 2737 (June 18, 1992, morning sitting).

abide by the data protection principles in the legislation."[24] Bennett proposes that the next challenge for British Columbia is privacy protection for the private sector which has made its way onto the federal political agenda. The academic community in British Columbia, in particular members from the University of Victoria have supported access to information and privacy rights and have been instrumental in the development of the legislation. The media for a long period have also been strong promoters of access to information legislation.

A study by Robert Hazell suggests that in a number of countries the media welcomed this type of legislation.[25] Freedom of information augments the media's ability to obtain information from government departments. Gabelmann noted during a debate in the legislative assembly that, "some media companies are not enthusiastic about the degree of personal privacy protection..."[26] A member from the Liberal Party, A. Warnke agreed that a few members of the media have reservations about Bill 50. Editorials in the Vancouver Sun endorsed the legislation although some flaws were highlighted.[27] The media was critical of the list of exemptions and argued that loopholes in Bill 50 allowed the government to maintain secrets.[28] The lawyer who represented the media, Roger McConchie raised concerns about the exemptions. One of the questions posed by McConchie for example included; why should a sexual abuse in a day care centre remain secret? Jack Weisgerber (former member of the Social Credit Party) suggested that: "The media is the

---

[24]Colin J. Bennett. "Privacy Protection in the Private Sector: Where Do We Go From Here?" B.C. Freedom of Information and Privacy Association Bulletin. Number 1, Jan.-Feb. 1996. p. 7.

[25]Robert Hazell. "Freedom of Information in Australia, Canada, and New Zealand." Public Administration, Vol. 67, No. 2 (London) (Summer 1989), p. 210. Hazell reports that between 1986-87 the percentage of access requests were dominanted by special interest groups. In 31% of the cases the public requested information; businesses 31%; organizations 11%; the media 21% and 6% were from academics and students. Hazell argues that the Canadian media are heavy users of the federal legislation.

[26]British Columbia. Official Report of Debates of the Legislative Assembly. 1st Session, 35 th Parliament. Vol. 4, No. 20: 2738 (June 18, 1992, morning sitting).

[27]Ibid. p. 2739.

[28]Ibid. p. 2739.

natural conduit for that information between the government and the public generally. On the one hand, you have the media sources concerned about the blockage of certain bits of information; at the other end of the scale, you have organizations and groups that are interested in protecting the privacy of the individual concerned that the bill goes too far."[29] Jones during one debate emphasized that the media consider the protection of individual privacy subordinate to the right of the public to know.[30] The media is very supportive of the legislation and a major user of the Act.[31] The lawyer representing the media interest, McConchie opposed certain provisions and was involved in a number of high powered legal debates with Rankin.[32] Jones states the discussions involved the concept of privacy, privacy implications and law enforcement issues. In the end, Rankin's arguments in favour of the legislation dulled criticisms by McConchie.[33] A review of the discussions and debates on the legislation illustrates the impetus was on the access side, although Jones notes the privacy side proved to be more complex.[34]. British Columbia, one of the last provinces to enact legislation did draw from the experiences of other governments.

The FOIPP Act is similar in many ways to the Ontario legislation. British Columbia, Ontario and Quebec are the only jurisdictions in Canada to adopt an independent tribunal with the power and authority to order the head of a public body to release information. The Federal government and most other provinces have commissions or agencies that can make recommendations on access to information applications and review institutional decisions. The commission or agency relies on the courts to order the release of information by a government agency. Representatives from

---

[29]Ibid. p. 2741.

[30]Ibid. p 2744.

[31]Personal interview with Barry Jones. Member of the Legislative Assembly for Burnaby North, Burnaby, January 23, 1996.

[32]Ibid.

[33]Ibid.

[34]Ibid.

Ontario and Quebec provided advice during consultation with Jones. One member from The Municipality of Metropolitan Toronto suggested that the province adopt one piece of legislation to address the needs of provincial and local bodies to avoid the shortcomings of the legislative approach in Ontario. Contrary to this view, representatives from the broader public sector believed there should be a separate piece of legislation to address the needs of local public bodies. Others recommended the amendment of individual governing statutes for each body.[35] An examination of the cost for implementation in Ontario led Jones to the conclusion that: "It was not a costly exercise or a significant cost to the public purse."[36] The response by organizations to the extension of the FOIPP Act (Bill 50) to include all public body records, including health records was mixed during the consultative process.

Extending Access and Privacy Rights to Public Bodies: The Case for Health Records

In September 1992 Jones began a consultative process on the extension of information and privacy rights for local public bodies. Advertisements were made requesting submissions, letters were sent to major interest groups and meetings were held with groups to discuss concerns. The participants included information holders, information seekers, public interest groups, and information and privacy specialists.[37] By December 1992, over one hundred submissions were given to Jones. The issue of access to health records was addressed during the process. A number of organizations believed they should be excluded from the legislation or they did not represent a public body. In response, Evans argues that: "Hospitals, health care institutions and the self-governing professional bodies all represent powerful groups which through government statutes are self-regulating. Each

---

[35]Barry Jones. Appendices to Barry Jones' Report Extending Freedom of Information and Privacy Rights in British Columbia. 1993.

[36]Personal interview with Barry Jones. Member of the Legislative Assembly for Burnaby North, Burnaby, January 23, 1996.

[37]Barry Jones. Barry Jones Report: The Extension of Citizen's Information and Privacy Rights to all Public Bodies in British Columbia. p. 2

represents a history of control and they do serve the public. Each is a legitimate public body."[38] FIPA originally did support legislation that would cover all health care records, but the line was drawn at self-governing professional bodies such as the College of Physicians and Surgeons. According to Evans the FOIPP Act should not be amended to include private health records since "it can go too far."[39] Evans points out that FIPA is primarily concerned with the "centres of power" and government functions. The self-governing professions perform some regulating functions over its members. According to FIPA and the B.C. Public Interest Advocacy Centre self-governing professions exercise at least eight governmental powers. These include: "...rule-making powers; advisory powers; supervisory powers; conciliatory tasks (e.g., between professionals and disgruntled clients); investigatory functions; prosecution; adjudicative functions; and determination of eligibility requirements and standards, i.e., for admission and practice."[40] One member of the legislative assembly, C. Serwa warned that: "There's going to be a substantial challenge to opening up self-governing professions to the degree that this Freedom of Information and Protection of Privacy Act enables."[41] The inclusion of self-governing professional bodies was advocated by a number of public interest groups as well FIPA argued that individuals should have the right to access personal health records in all health care facilities and this should be consistent with the provisions of Bill 50.

Bill 50 applies to a range of health care records under the control or custody of the MOH or health care facilities operated by the province. These include provincial health units, residential care

---

[38]Personal interview with Darrell Evans. Executive Director, Freedom of Information and Protection of Privacy Association, Vancouver, February 3, 1996.

[39]Ibid.

[40]Michael P. Doherty. Privacy and Access to Information Issues: Self-Governing Professions. Prepared for B.C. Freedom of Information and Privacy Association by B.C. Public Interest Advocacy Centre. Vancouver, no date. p. 6.

[41]British Columbia. Official Report of Debates of the Legislative Assembly. 1st Session, 35 th Parliament. Vol. 4, No. 20: 2749 (June 18, 1992, morning sitting).

facilities, mental health centres, mental health hospitals, alcohol and drug treatment centres.[42] Health records under the custody or control of the Ministry of Social Services and provincial correctional facilities are covered. These provincial health agencies must allow patients to examine health records and are bound by specific guidelines to protect the privacy of patients. Bill 50 did not apply to hospitals and other health care facilities even though many receive public funding or exist under a provincial enabling legislation. Bill 50 and Bill 62 do not apply to health records held by physicians in private practice. FIPA defended its position for the extension of the FOIPP Act based on the cost, time-delays and complexity of going to court, which was the option available to British Columbians before the Act. FIPA's view was similar to those of the B.C. Royal Commission on Health Care and Costs. The Commission stated that, "...existing provincial information and privacy legislation should be extended to cover medical records held by all health care providers, including those in the private sector."[43] The Health Care Alliance (HCA) representing the B.C. Health Association, the B.C. Association of Community Care, the B.C. Health Care Risk Management Society, the Health Administrators Association of British Columbia and the Health Records Association of B.C. took exception to this position.[44] The HCA felt the 1983 British Columbia Health Association (BCHA) *Guidelines on the Confidentiality of Health Information* adopted by most of its members was sufficient. The BCHA Guidelines are voluntary and provide full disclosure to patients of their medical records upon request. HCA felt the voluntary policies and common law remedies available to patients were adequate and further protection through provincial legislation was unnecessary. In the final recommendations, Jones pointed out that the BCHA Guidelines "do not apply to the clinical record and apparently require the patient to release the institution from any claims in order to receive the record."[45] In addition,

---

[42]Barry Jones. Barry Jones Report: The Extension of Citizen's Information and Privacy Rights to all Public Bodies in British Columbia.

[43]Ibid. p. 52.

[44]Ibid. p. 52 and Barry Jones. Appendices to Barry Jones' Report Extending Freedom of Information and Privacy Rights in British Columbia. 1993.

[45]Ibid. p .52.

public interest associations argued that the act of going through the courts and relying on common law remedies to obtain access to records is both costly and time-consuming. Jones suggests that a great deal of concern came from the medical area. Many argued that Section 57 of the Evidence Act that allowed hospitals and self-governing professional bodies to conduct the peer review process in complete confidentiality should be excluded from the Act. It was agreed that the Evidence Act should take precedence since the ability of doctors to take part in the review process required confidentiality.[46] Jones notes that with the threat of the Act, hospitals were shutting down peer review sections.[47]. The health sector was perturbed about the impact of the legislation on fund raising campaigns. Hospitals were concerned that the existing practice of using patient information upon registration for the hospital foundations' campaigns would be curtailed by the legislation.[48] FIPA does not support this practice. The problem was addressed using consent forms as part of the admissions process. Evans notes that several hospitals were concerned that the legislation would discourage staff members from coming forward and would limit full discussions during investigations involving a patient and the hospital.[49] Evans argues that checks and balances properly implemented would ensure personal information such as staff names could be kept confidential.[50] The argument that hospitals and individuals would not come forward and be open in their discussions is rejected by Evans. Jones was anxious about including the private records of physicians into the legislation, but noted recently that it will not be amended to include these records.[51] The College of Physicians and Surgeons was supportive of the Supreme Court of

---

[46]Personal interview with Barry Jones. Member of the Legislative Assembly for Burnaby North, Burnaby, January 23, 1996.

[47]Ibid.

[48]Ibid. Also Personal interview with Darrell Evans. Executive Director, Freedom of Information and Protection of Privacy Association, Vancouver, February 3, 1996.

[49]Personal interview with Darrell Evans. Executive Director, Freedom of Information and Protection of Privacy Association, Vancouver, February 3, 1996.

[50]Ibid.

[51]Ibid

Canada McInerney v. MacDonald decision and wanted members to adhere to the ruling as part of their membership.[52] Another route would be to include in the College's by-laws an access to information provision similar to the Court's ruling.[53]. Jones in the final report to Gabelmann concluded that,

> I am persuaded by the submissions presented to me that it is in the public interest to establish an avenue of last resort which does not involve costly, time-consuming litigation. The litigation is a barrier to individuals who may wish to appeal the decision of a record holder, and is a burden to both the individual and to the institution or office holding the record.[54]

The FOIPP Act was amended to include the health records in all hospitals and health care facilities without exception. In November 1995, self-governing professional bodies came under the Act. The legislation has changed some organizational practices, providing benefits to institutions while imposing additional costs. This is part of the "growing pains of the legislation" that Jones believes was inevitable.[55]

Impact and Assessment of the FOIPP Act

A number of perspectives on the FOIPP Act are examined in the following section. A series of interviews was conducted with staff members from hospitals and self-governing professional bodies to determine their views on the legislation. Members were asked a number of general questions concerning their personal views on privacy and the need for the legislative protection of personal information. This was followed by specific questions on organizational practices and challenges from the requirements of the FOIPP Act. The interview process involved on-site

---

[52]Personal interview with Barry Jones. Member of the Legislative Assembly for Burnaby North, Burnaby, January 23, 1996.

[53]Ibid.

[54]Barry Jones. Barry Jones Report: The Extension of Citizen's Information and Privacy Rights to all Public Bodies in British Columbia. p. 53

[55]Personal interview with Barry Jones. Member of the Legislative Assembly for Burnaby North, Burnaby, January 23, 1996.

personal interviews with representatives or staff members from hospitals and the self-governing professional bodies who are directly affected by the Act. These included, Patricia Stevens, Director of Patient Documentation of the Fraser-Burrard Hospital Society (recently renamed the Simon Fraser Health Board) which includes three hospitals, Eagle Ridge in Port Moody, Ridge Meadows Hospital in Maple Ridge and the Royal Columbian in New Westminster; Donella Brooks, Manager of Clinical Records Services and Shirley Macdonald, Health Information Professional from Riverview Hospital; Dr. M. Vanandel, Deputy Registrar and Jian Liu, Freedom of Information and Privacy Analyst Records Manager from the College of Physicians & Surgeons of British Columbia; and Linda J. Lytle, Registrar at the College of Pharmacists of British Columbia. Staff members shared their organization's experiences in implementing the legislation and reflected on a number of important issues and concerns. The questions posed during the interviews varied considerably depending on the subject interviewed. The list of questions presented in Appendix E are general in nature and somewhat open-ended. This approach was beneficial as participants provided additional details and commentary and other questions emerged as the interview progressed.

The staff members from hospitals and self-governing professional bodies believe the protection of personal information is very important and rules are necessary to prevent unauthorized collection and inappropriate release of information. Many agree the public has a right to know and to access their own personal health information. In most health care facilities the quantity of records generated is quite extensive. Riverview Hospital, for example has approximately 200 forms in Clinical Records that contain personal information. These include, information on psychiatric and psychology history, family data, social history, diagnostic files and legal information. Since 1943 all records are kept intact. A computerized patient index system exists which contains information relating to demographics, family information, diagnostic data, Personal Health Number and billing information. Clinical records are not computerized. At the Fraser-Burrard Hospital Society the types of information recorded on a patient file include, demographics, admission history, diagnostic

information, consultations, information that is deemed important for continuing care such as Social Services or Ministry of Health records, psychology and psychiatric records. The Hospital's computer systems contain patient records and nurses' notes. Patient care records are on-line at Eagle Ridge Hospital. A majority of the records held by the College of Physicians and Surgeons provides the history of medical practice by physicians. There are eight thousand physicians across British Columbia that are registered with the College. The College's directory of records includes education records (pre-registration training programs and medical students interview files); practice/competency review files; registration (membership information) and regulation files (complaints, investigation/discipline cases). The College maintains a personal information bank directory for staff members. The College of Pharmacists maintains similar types of records for members. In addition patients can obtain a printout of prescription records from the Pharmanet system through the College. The number of requests by patients to access personal health records have increased since the enactment of the FOIPP Act.

Since the 1980s, the policy at Riverview did allow individuals to view personal records on a case by case basis. Before the enactment of the legislation, approximately four to six requests were made per year. At present it is not uncommon to have five requests per month from patients to view personal health records. The change in the number of requests is the result of several factors. First, patients are informed about their rights to access health records through the Mental Health Law Program at the Hospital. Second, more family members of deceased patients are requesting access to records. This can be attributed to the growing field of genealogy. Third, patients are questioning their physicians and aware of their rights. The Mental Health Law Program is actively involved with patients. Patients are given access to records and are asked if they would like to have a health care professional present. The access provisions of the legislation have not caused an increase in litigation.

The Fraser-Burrard Hospital Society received approximately two patient requests per month five years ago. Since the enactment of the FOIPP Act the number of requests by patients is twenty to thirty per month. In addition, there are many legal requests by lawyers on behalf of patients. The lawyers require a letter of authorization, which has been the policy for the last five years. Approximately ten percent of the increase in the number of access request can be attributed to the legislation since lawyers increasingly use the Act as a lever to obtain records. Moreover, individuals are aware of rights, curious and more litigious. The Society received approximately 2200 access requests in the past year. Only two of those requests were to correct personal information, although one request was denied since the individual could not prove the information was incorrect. Since February 1996, the College of Physicians and Surgeons have received approximately twenty-five access requests under the legislation. Seventeen of the twenty-five requests have been completed. Ten of the requests required 30 days for completion; seven were completed in 60 days; and three required more than 120 days. At the College of Pharmacists there has been no access requests under the FOIPP legislation as of February 1996. The general policy of the College is to release information if permission is granted by all individuals involved. The FOIPP Act presents some organizational challenges to hospitals and self-governing bodies.

At Riverview it was noted that requests for access to information involve a line by line search and require a great deal of time. A 1995 survey by the Health Records Association for British Columbia found similar concerns in a number of health care facilities.[56] The survey indicated increases in workload and limits to resources pose challenges to health organizations. At Riverview each request requires a line by line search of the patient record that can range from 100 to 7000 pages. The records are extremely bulky and photocopying presents considerable difficulties. The problem is highlighted by one example in which a patient requested a record that consisted of approximately 3000 pages. The record was photocopied, although the patient did not

[56]Results of the HRABC Survey - Release of Information and the Freedom of Information and Protection of Privacy Act. Health Records Association of British Columbia. 1995.

take the record upon discharge. In other cases a patient may request a record more than once if the original copy is lost. There is no cost recovery for providing copies of records to patients. Riverview has never imposed a cost on patients to view records and the FOIPP Act also prohibits fees for access to personal information. At the Fraser-Burrard Hospital Society no additional staff was hired, although the workload did increase as a result of the legislation. Severing the information in files that relate to third parties takes the most time. Patients requiring access to files must make an appointment with the Health Records Department. The Department may use the thirty days as stipulated in the FOIPP Act to grant a request if required.

To date the cost for the College of Physicians and Surgeons ranges from $100,000 to $150,000 and includes the salary of one and a half staff members. Lawyers and physicians are also involved in the process. It was suggested that retroactive files must be reviewed to protect privacy and third party information must be severed. Staff members are conscious of what is placed in the physician's file since members of the College may request to see personal files. If an anonymous complaint is made against a physician it is not placed in the physician's file but in a general correspondence file. The identity of a complainant must be known to the College, and cannot be anonymous. Medical expertise is required to review complaints from the public. Under the legislation, the complainant can obtain all the information required to adjudicate the concern. The subject of litigation is a major concern and it was noted that the College should not be used as a screening tool for the civil court process. Before the Act, the claimant was assured of privacy. If disciplinary action is taken against a member of the College, the claimant's name may become public knowledge to satisfy the public's interest to know. Moreover, in many instances the Act is designed for government departments and may not always fit the College's mandate. The College of Pharmacists collects information about members and is extremely protective of personal information. The College does not have any concerns about providing individuals with access to information either widely or on a case by case basis. Information practices in many organizations have improved as a direct result of the legislative requirements.

In response to the FOIPP Act, a number of policies were recommended by the Health Records Association of British Columbia (HRABC). Some hospitals and health care facilities are examining and implementing policies and guidelines. These include policies on the use of fax machines and e-mails and encouraging staff members to uphold confidentiality and privacy of patient information. One recommendation by the HRABC FOI Impact Task Force is for health care providers to use identification numbers instead of names in the health record.[57] This should alleviate any concern staff members have about personal security. The 1995 report titled *Review of the Storage and Disposal of Health Care Records in British Columbia* by the Deputy Provincial Health Officer did recommend that all health care facilities and hospitals develop disposal policies. Many organizations are in the process of improving and updating guidelines for the retention and disposal of health care records. Several health organizations recognize that education and training on the issues relating to access and privacy of health information is paramount for effective enforcement of the FOIPP Act.

The Fraser-Burrard Hospital Society, before the Act, had guidelines dealing with paper and computerized patient records. The hospital's computer systems contain patient records and nurses' notes. To protect privacy of computer information, access is restricted on a need to know basis. Hospital staff members are restricted to information on the ward, and an audit process and trail are available to determine who has gained access to records. If entry to the system is unauthorized, the identity of the individual attempting to gain access is "flagged" and may result in disciplinary action. During orientation the issues of confidentiality and privacy are reviewed with new employees. At present, the Society is trying to implement a Confidentiality Pledge for hospital staff.

---

[57]Results of the HRABC Survey - Release of Information and the Freedom of Information and Protection of Privacy Act. Health Records Association of British Columbia. 1995.

The records management practices at the College of Physicians and Surgeons has improved as a result of the legislation. Individual staff members are careful on the types of information placed in files. The Deputy Registrar noted that physicians presently have rules in place, such as professional ethics that are sufficient. The new legislation will not add to existing rules. The College presently does not use electronic mail. Legal Counsel has their own fax machines and the College relies more on courier services. The Deputy Registrar suggested the legislation may be beneficial since it is making the College review its records and may improve the way things are done. The FOIPP Act did result in a few changes to the College of Pharmacists. All seventeen staff members are required to sign a confidentiality agreement. During orientation the issues on access and privacy are discussed with new employees. Failure to comply with rules may lead to disciplinary action. A records management review by an external consultant was conducted to facilitate implementation of new procedures. A number of safeguards are in place, including the locking of filing cabinets. Staff members have limited access to computer files based on the need to know and require passwords. In September 1995, the Council of the College approved a record destruction policy, which incorporated the recommendations by the Deputy Provincial Health Officer following the review on health records retention and disposal in British Columbia.

The interviews conducted with the hospitals and self-governing professional bodies suggest the legislation poses some challenges to organization resources. Conversely, the improvements in record-keeping practices, greater public accountability and wider recognition of patient rights are some of the benefits. These organizations and the public have gained in a number of important ways from the FOIPP Act. A number of policy actors continue to engage in discussions and debates on information rights and challenge provincial and public body decisions. A review of the literature and discussions with participants suggest members of the policy community were actively involved in the legislative process and helped to set the agenda for access to information and privacy legislation in British Columbia.

Chapter VI - Conclusion

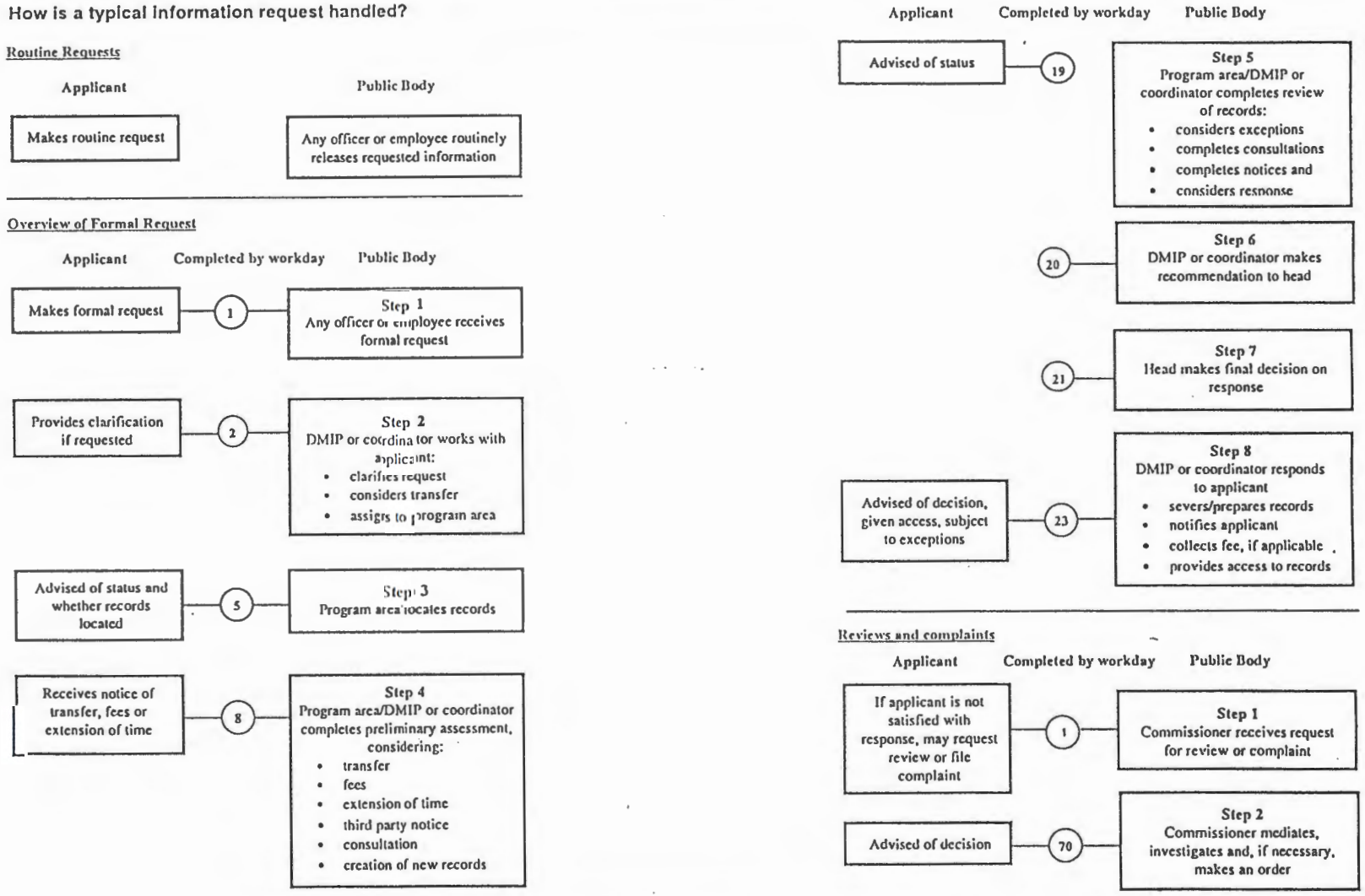
Privacy does not exist in a vacuum, but is part of a larger social, political, economic and technological world. Privacy may increase or decrease as other values emerge. Information practices became an important social and political issue beginning in the 1960s. The policy literature suggests increasing record-keeping activities and computerization brought the issue on to the public agenda. Government organizations began to rely on records to make decisions and the cumulative effect was an incremental shift in the relationship between the citizen and the state. The state developed formal arrangements to deal with clients.

The relationship between governments and societal interests are changing as well as the relationship between the medical profession and society. The salient feature of the health care community is the historical dominance of the medical profession's control over patient information. This situation is changing. Citizens are becoming more adversarial and are reacting against social and bureaucratic controls. Chapter IV suggested that a number of values may conflict with individual privacy. Some of the values explored in this study include the public's interest in preventing fraud and abuse of publicly funded health care programs; effective enforcement of regulation and the promotion of research. The bureaucracy's interest in using the latest technology to provide more efficient and effective services may conflict with individual privacy if adequate safeguards are not put into place. Information technology is being used in more creative ways to reduce duplication, fraud, multi-doctoring and to promote sharing of information. The Ministries of Health across Canada are examining or experimenting with elaborate information systems that permit sharing of health information within the health care community. Each of the technologies discussed present some challenge to privacy, as the control over information may be lost as more individuals exchange health information.

In response to the growing tension between information control and the bureaucracy's demands for personal information, data protection legislation was enacted throughout North America. The Freedom of Information and Protection of Privacy (FOIPP) Act poses a regulatory challenge to governments who must balance the individual's right to privacy with the need to collect information for effective and efficient delivery of services. The state's responsiveness to privacy issues is largely dependent on the importance society places on this value. The policy discussions and debates on the FOIPP Act highlighted a host of competing perspectives and interests. As public interest groups such as FIPA mobilizes support through public education and information the issues will remain high on the political agenda. Many in the health sector espouse the view that the Oath of Hippocrates, professional ethics and guidelines provide adequate protection to patients. This reflects one traditional view that the legislative protection of health records is not necessary. Since the enactment of the FOIPP Act, the requests by patients to examine personal health records have risen. Diverse members from the health community indicate that patients are becoming more educated about their rights and are questioning the medical profession. These findings support the "consumer theory of health care" and the concept of "consumerism" in medicine. Privacy is an important value in liberal democratic regimes and individuals have a growing interest in the accuracy, completeness and relevance of agency records. From a public policy perspective a significant policy challenge exists. There is a trade-off between public interest and privacy. The quest for cost containment, administrative accountability and efficiency may inevitably result in a loss to individual privacy and limits to information self-determination in the health care system.

Appendix A
Information Requests Using the FOIPP Act

How is a typical information request handled?



Source: British Columbia, Ministry of Government Services. Information and Privacy Handbook: An Interpretive Guide to the Freedom of Information and Protection of Privacy Act. Second edition. Prepared and published by Interact Public Policy Consultants. Vancouver, 1995. p. 0-12 and p. 0-13.

Appendix B

Records Exempt From the FOIPP Act

According to Section 3 of the British Columbia Freedom of Information and Protection of Privacy Act all records in the custody or under the control of a public body are subject to the legislation with the exception of the following records.

(a) a record in a court file, a record of a judge of the Court of Appeal, Supreme Court or Provincial Court, a record of a master of the Supreme Court , a record of a justice of the peace, a judicial administration record or a record relating to support services provided to the judges of those courts;

(b) a personal note, communication or draft decision of a person who is acting in a judicial or quasi judicial capacity;

(c) a record that is created by or is in the custody of an officer of the Legislature and that relates to the exercise of that officer's functions under an Act;

(d) a record of a question that is to be used on an examination or test;

(d.1) a record containing teaching materials or research information of employees of a post-secondary educational body;

(e) material placed in the British Columbia Archives and Records Service by or for a person or agency other than a public body;

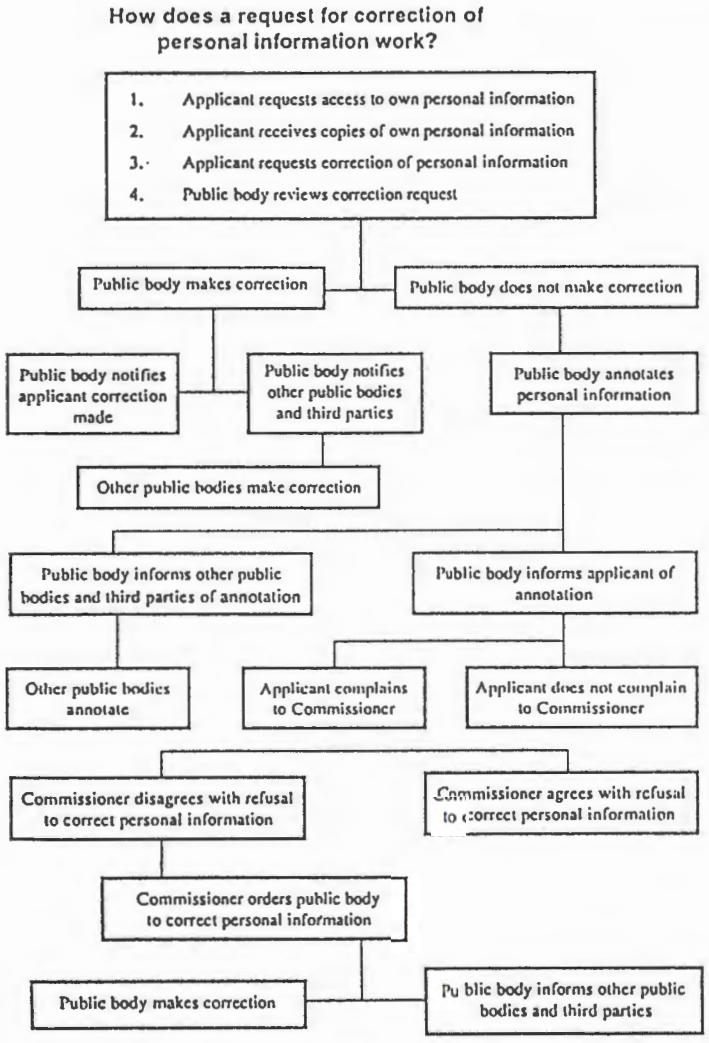
(f) material placed in the archives of a public body by or for a person or agency other than the public body;

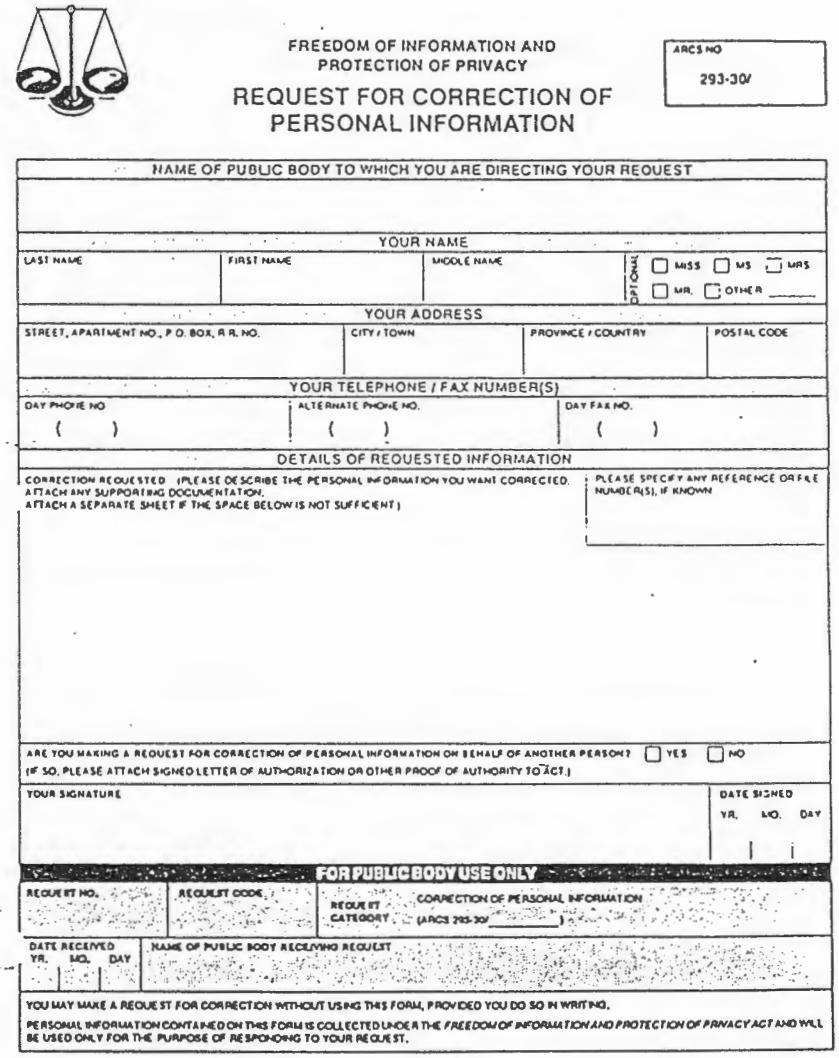
(g) a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed;

(h) a record of an elected official of a local public body that is not in the custody or control of the local public body.

Source: British Columbia Statute. "Freedom of Information and Protection of Privacy Act", R.S.B.C. 1992-Bill 50". Victoria, Queen's Printer, 1992.

Appendix C
Correction of Personal Information Using the FOIPP Act





FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

REQUEST FOR CORRECTION OF PERSONAL INFORMATION

ARCS NO 293-30/

NAME OF PUBLIC BODY TO WHICH YOU ARE DIRECTING YOUR REQUEST

YOUR NAME

LAST NAME | FIRST NAME | MIDDLE NAME | OPTIONAL: ☐ MISS ☐ MS ☐ MRS ☐ MR. ☐ OTHER _____

YOUR ADDRESS

STREET, APARTMENT NO., P.O. BOX, R.R. NO. | CITY / TOWN | PROVINCE / COUNTRY | POSTAL CODE

YOUR TELEPHONE / FAX NUMBER(S)

DAY PHONE NO. ( ) | ALTERNATE PHONE NO. ( ) | DAY FAX NO. ( )

DETAILS OF REQUESTED INFORMATION

CORRECTION REQUESTED (PLEASE DESCRIBE THE PERSONAL INFORMATION YOU WANT CORRECTED. ATTACH ANY SUPPORTING DOCUMENTATION. ATTACH A SEPARATE SHEET IF THE SPACE BELOW IS NOT SUFFICIENT)

PLEASE SPECIFY ANY REFERENCE OR FILE NUMBER(S), IF KNOWN

ARE YOU MAKING A REQUEST FOR CORRECTION OF PERSONAL INFORMATION ON BEHALF OF ANOTHER PERSON? ☐ YES ☐ NO

(IF SO, PLEASE ATTACH SIGNED LETTER OF AUTHORIZATION OR OTHER PROOF OF AUTHORITY TO ACT.)

YOUR SIGNATURE | DATE SIGNED YR. MO. DAY

FOR PUBLIC BODY USE ONLY

REQUEST NO. | REQUEST CODE | REQUEST CATEGORY: CORRECTION OF PERSONAL INFORMATION (ARCS 293-30/ _____)

DATE RECEIVED YR. MO. DAY | NAME OF PUBLIC BODY RECEIVING REQUEST

YOU MAY MAKE A REQUEST FOR CORRECTION WITHOUT USING THIS FORM, PROVIDED YOU DO SO IN WRITING.

PERSONAL INFORMATION CONTAINED ON THIS FORM IS COLLECTED UNDER THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT* AND WILL BE USED ONLY FOR THE PURPOSE OF RESPONDING TO YOUR REQUEST.

Source: British Columbia, Ministry of Government Services. Information and Privacy Handbook: An Interpretive Guide to the Freedom of Information and Protection of Privacy Act. Second edition. Prepared and published by Interact Public Policy Consultants. Vancouver, 1995. p. 0-17 and p. 9-3.

Appendix D

General Guidelines for Protecting Personal Privacy

Public bodies collect and retain personal information for a variety of purposes that are essential to their effective and efficient operation. These purposes are balanced carefully with the interests of individuals in their own information and privacy. The Act provides that:

Individuals have the right to access their own personal information and to request correction of errors or omissions in it;

Public bodies collect personal information only for purposes authorized under an Act, for law enforcement or for operating programs or activities;

Public bodies collect personal information directly from the individual concerned unless the individual authorizes collection from another person, the Act authorizes indirect collection or specific legislation authorizes collection from other sources;

Public bodies notify individuals about the authority for and purpose of collecting their personal information unless notice is not required in limited and specific circumstances under the Act;

Public bodies use personal information only for the purpose for which it was collected, for a consistent purpose, for another purpose to which the individual has given express consent or for a specific purpose set out in the Act;

Public bodies make reasonable efforts to ensure that the personal information they collect for decision-making purposes is accurate and complete;

Public bodies retain personal information used for decision-making purposes for a reasonable period of time so that individuals may exercise their rights of access and correction; and

Public bodies make reasonable security arrangements to protect personal information in their custody or under their control.

Source: British Columbia, Ministry of Government Services. Information and Privacy Handbook: An Interpretive Guide to the Freedom of Information and Protection of Privacy Act. Second edition. Prepared and published by Interact Public Policy Consultants, Vancouver, 1995. Part 3:1-4.

Appendix E

Interview Questions

General Questions for Hospitals and Self-Governing Professional Bodies:

What do you think about privacy and the protection of information?

How important is privacy?

How does your organization protect personal information?

What types of information are recorded in the patient's file?

Does your organization have computerized patient information?

What has been the impact of the Freedom of Information and Protection of Privacy Act (FOIPPA) on your organization?

What concerns, if any do you have about the provincial legislation?

Has the legislation changed the way your organization handles information and uses information technologies? Has record-keeping practices changed?

Does your organization have a disposal policy?

Are there any benefits from the legislation?

Has the number of access requests increased since the FOIPP Act?

What has been the overall effect on your organization in terms of workload, cost and resources?

What challenges does your organization face in trying to implement the requirements of the Act effectively?

What changes would you make to the legislation?

Was your organization involved in the government's consultative process dealing with the legislation?

What are your views on Pharmanet, the computerized drug information network?

All interviewees were given an opportunity to comment on the interview notes. Letters of Acknowledgment were provided and permission to use the information was obtained.

Bibliography

Books

Andersen, David F. and Dawes, Sharon S. Government Information Management: A Primer and Casebook. New Jersey: Prentice-Hall, Inc., 1991.

Angus, Douglas, E., Auer, Ludwig, Cloutier, J. Eden and Albert, Terry. Sustainable Health Care for Canada: Synthesis Report. Ottawa: Queen's-University of Ottawa Economic Projects, University of Ottawa, 1995.

Bennett, Colin J. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. New York: Cornell University Press, 1992.

Boase, Joan Price. Shifting Sands: Government-Group Relationships in the Health Care Sector. Montreal and Kingston: McGill-Queen's University Press, 1994.

Bolaria B. Singh and Davidson, Harley D. Health, Illness and Health Care in Canada. Second edition. Toronto: Harcourt Brace & Company Canada Ltd., 1994.

Bruce, Jo Anne Czecowski. Privacy and Confidentiality of Health Care Information, second edition. Illinois: American Hospital Publishing Inc., 1988.

Buchanan, Allen. "Medical Paternalism." In Medicine and Moral Philosophy. Edited by Marshall Cohen, Thomas Nagel and Thomas Scanlon. Princeton, New Jersey: Princeton University Press, 1982. pp. 214-234.

Corburn, D., D'Arcy Carl, Torrace, George M. and New, Peter Kong-Ming. Health and Canadian Society: Sociological Perspectives. Second edition. Markham: Fitzhenry & Whiteside, 1987.

Cox, Michael G. "Personal Access: the Canadian Human Rights Act of 1977 and the Privacy Act of 1982." In Canada's New Access Law: Public and Personal Access to Governmental Documents. Edited by Donald C. Rowat. Ottawa: Published by the Department of Political Science, Carleton University, 1983, pp. 19-44.

Etzioni-Halevy, Eva. Bureaucracy and Democracy: A Political Dilemma. London: Routledge & Kegan Paul, 1983.

Flaherty, David H. Protecting Privacy in Two-way Electronic Services. New York: Knowledge Industry Publications, Inc., 1985.

Flaherty, David H. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States. London: The University of North Carolina, 1989.

Haug, Marie and Lavin, Bebe. Consumerism in Medicine: Challenging Physician Authority. Beverly Hills: Sage Publications, Inc., 1983.

Hixson, Richard F. Privacy in a Public Society: Human Rights in Conflict. New York: Oxford University Press, 1987.

Humphreys, Edward H. Privacy in Jeopardy: Student Records in Canada. Toronto: The Ontario Institute for Studies in Education, 1980.

Institute of Medicine. Health Data in the Information Age: Use, Disclosure and Privacy. Edited by Molla S. Donaldson and Kathleen N. Lohr. Washington, D.C.: National Academy Press, 1994.

Jardine, Donald A. "Health Care Information Technology." Healthy Populace, Health Policy: Medicare Toward the Year 2000. Edited by S. Mathwin Davis. Kingston: School of Policy Studies/School of Public Administration, Queen's University, 1990.

Kernaghan, Kenneth and Langford, John W. The Responsible Public Servant. Halifax: The Institute for Research on Public Policy, 1990.

London, Jack R. "Privacy in the Medical Context." In Aspects of Privacy Law: Essays in Honour of John M. Sharp. Edited by Dale Gibson. Toronto: Butterworths & Co. (Canada) Ltd., 1980. pp. 281-294.

Marsh, Norman (ed.). Public Access to Government-Held Information. London: Stevens & Son Ltd., 1987.

McHale, Jean V. Medical Confidentiality and Legal Privilege. New York: Routledge, 1993.

McMiller, Kathryn. Being a Medical Records Clerk. Brady Medical Clerical Series. Edited by Kay Cox. New Jersey: Prentice-Hall, Inc., 1992.

Miller, Arthur M. The Assault on Privacy: Computers, Data Banks, and Dossiers. Ann Arbor: The University of Michigan Press, 1971.

O'Brien, David M. Privacy, Law, and Public Policy. New York: Praeger Publishers, 1979.

Osborne, Philip H. "The Privacy Acts of British Columbia, Manitoba and Saskatchewan." In Aspects of Privacy Law: Essays in Honour of John M. Sharp. Edited by Dale Gibson. Toronto: Butterworths & Co. (Canada) Ltd., 1980.

Picard, Ellen I. Legal Liability of Doctor's and Hospitals in Canada. Second edition. Toronto: Carswell Legal Publications, 1984.

Pross, A. Paul. Group Politcs and Public Policy. Toronto: Oxford University Press, 1986.

Regan, Priscilla, M. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: The University of North Carolina Press, 1995.

Rozovsky, Lorne E. and Rozovsky, Fay A. The Canadian Law of Patient Records. Toronto: Butterworths & Co., 1984.

Rozovsky, Lorne E. The Canadian Patient's Book of Rights: A Consumer's Guide to Canadian Health Law. Second edition. Toronto: Doubleday Canada Limited, 1994.

Rule, James, MacAdam, Douglas, Stearns, Linda and Uglow, David. The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York: Elsevier, 1980.

Sadofsky, David. Knowledge as Power: Political and Legal Control of Information. New York: Praeger Publishers, 1990.

Schafer, Arthur. "Privacy: A Philosophical Overview." In Aspects of Privacy Law: Essays in Honour of John M. Sharp. Edited by Dale Gibson. Toronto: Butterworth & Co. (Canada) Ltd., 1980.

Shah, C. P. Public Health and Preventative Medicine in Canada. Third edition. Toronto: University of Toronto Press, 1994.

Shaw, Erin, Westwood, John and Russell, Wodell. The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them. Vancouver: Prepared for the B.C. Civil Liberties Association and B.C. Freedom of Information and Privacy Association, 1994.

Sieghart, Paul. Privacy and Computers. London: Latimer New Dimensions, 1976.

Smith, B. C. Bureaucracy and Political Power. New York: St. Martin's Press, Inc. 1988.

Vandeveer, Donald. "The Contractual Argument for Withholding Medical Information." In Medicine and Moral Philosophy. Edited by Marshall Cohen, Thomas Nagel and Thomas Scanlon. Princeton, New Jersey: Princeton University Press, 1982. pp. 235-242.

Wahn, Michael. "The Decline of Medical Dominance in Hospitals." In Health and Canadian Society: Sociological Perspectives. Second edition. Edited by D. Coburn, Carl D'Arcy, George M. Torrace and Peter Kong-Ming New. Markham: Fitzhenry & Whiteside, 1987. pp. 422-440.

Wallace, Jill. "The Canadian Access to Information Act 1982." In Public Access to Government-Held Information. Edited by Norman Marsh. London: Stevens & Son Ltd., 1987, pp. 122-171.

Waugh, Nanci-Jean. "A Critique of the Privacy Act." Canada's New Access Law: Public and Personal Access to Governmental Documents. Edited by Donald C. Rowat. Ottawa: Published by the Department of Political Science, Carleton University, 1983, pp. 45-56.

Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967.

Woodward, Christel A. and Curry, Lynn. "The Health Encounter Card Pilot Project: An Innovation in Health Care." In Health Care Innovation, Impact and Challenge. Edited by S. Mathwin Davis. Kingston: School of Public Administration, Queen's University, 1992.

Conference, Presentation and Lecture Proceedings

Flaherty, David H. Protecting Privacy in an Open Society: The Canadian Experience. Lansdowne Lecture in Law, University of Victoria, British Columbia, February 7, 1995, unpublished.

Flaherty, David H. Pharmanet. Excerpt from a speech presented to the University of Victoria, School of Law, British Columbia. February, 7, 1995.

Flaherty, David H. Privacy and Data Protection in Health and Medical Information. Notes for Presentation to the 8th World Congress on Medical Informatics. Vancouver: July 27, 1995, unpublished.

Flaherty, David H. Provincial Identity Cards: A Privacy-Impact Assessment. Notes for a Presentation. Victoria: September 26, 1995, unpublished.

Miller, A. B. The Researcher's Need for Access. Proceedings of the Workshop on Computerized Record Linkage in Health Research on May 21-23, 1986 in Ottawa. Edited by Geoffrey R. Howe and Robert A. Spasoff. Toronto: University of Toronto Press, 1986.

Government Publications and Public Documents

British Columbia. Closer to Home: The B.C. Royal Commisssion on Health Care and Costs. Victoria: Crown Publications, 1991.

British Columbia. Official Report of Debates of the Legislative Assembly (Hansard). 5th Session, 34th Parliament. Vol. 21, No. 6: 12042 (May 13, 1991, afternoon sitting). Victoria: Queen's Printer for British Columbia, 1992.

British Columbia. Official Report of Debates of the Legislative Assembly (Hansard). 1st Session, 35th Parliament. Vol. 4, No. 20: 2737 (June 18, 1992, morning sitting). Victoria: Queen's Printer for British Columbia, 1992.

British Columbia. Official Report of Debates of the Legislative Assembly (Hansard). 1st Session, 35th Parliament. Vol. 4, No. 24: 2867 (June 22, 1992, afternoon sitting). Victoria: Queen's Printer for British Columbia, 1992.

British Columbia. Official Report of Debates of the Legislative Assembly (Hansard). 1st Session, 35th Parliament. Vol. 5, No. 1: 2949 (June 23, 1992, afternoon sitting). Victoria: Queen's Printer for British Columbia, 1992.

British Columbia. Official Report of Debates of the Legislative Assembly (Hansard). 2nd Session, 35th Parliament. Vol. 12, No. 13: 8998 (July 21, 1993, afternoon sitting). Victoria: Queen's Printer for British Columbia, 1993.

British Columbia, Ministry of Government Services. Information and Privacy Handbook: An Interpretive Guide to the Freedom of Information and Protection of Privacy Act. Second edition. Vancouver: Prepared and published by Interact Public Policy Consultants, 1995.

British Columbia, Ministry of Health and Ministry Responsible for Seniors. PharmaNet - The Basics. Victoria: no date.

British Columbia, Ministry of Health and Ministry Responsible for Seniors. Shaping the Future of Pharmacare. Victoria: May, 1993.

British Columbia, Ministry of Health and Ministry Responsible for Seniors. Vision for Health Information Management in British Columbia. Health Information Management Project. Victoria: May 1995.

Canada, Privacy Commission. Annual Report 1993-1994. Ottawa, The Privacy Commissioner of Canada.

Canada, Privacy Commission. Annual Report 1994-1995. Ottawa, The Privacy Commissioner of Canada.

Canada, Task Force established jointly by the Department of Communications/Department of Justice: Privacy and Computers. Ottawa: Information Canada, 1972.

Jones, Barry. Barry Jones Report: The Extension of Citizens' Information and Privacy Rights to all Public Bodies in British Columbia. Presented to the Attorney General, Chair, Cabinet Caucus Committee on Information and Privacy. Victoria: Queen's Printer for British Columbia, 1993.

Jones, Barry. Appendices to Barry Jones' Report Extending Freedom of Information and Privacy Rights in British Columbia. Victoria: Queen's Printer for British Columbia, 1993.

Karim, Jenny. Sharing Health Information: The B.C. Scenario. Prepared for the Provincial Health Information Management Steering Committee and the Ministry of Health, Victoria: April 1993.

Karim, Jenny. Clinical Data Supporting the Need for a Pharmacy Network. Prepared for Ministry of Health and Ministry Responsible for Seniors. Victoria: February, 14, 1994, unpublished.

Krever, Horace (Commissioner). Report of the Commission of Inquiry into the Confidentiality of Health Information, Volumes I, II and III. Royal Commission Report. Toronto: Queen's Printer for Ontario, 1980.

Organization for Economic Co-operation and Development. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Paris: OECD, 1981.

Organization for Economic Co-operation and Development. Privacy and Data Protection: Issues and Challenges. Paris: OECD Documents, 1994.

Owen, Stephen, (Ombudsman). Access to Information and Privacy. Public Report No. 26. Presented to the British Columbia Legislative Assembly. Victoria: March 15,1991.

New Brunswick, Task Force on Data Sharing and Protection of Personal Privacy. Protecting Privacy in an Information Sharing Environment. August 1994.

Peck, Shaun H. S. Review of the Storage and Disposal of Health Care Records in British Columbia. Report by the Office of the Provincial Health Officer to the B.C. Ministry of Health and Ministry Responsible for Seniors. Victoria: Queen's Printer for British Columbia, July, 1995.

Science Council of British Columbia, SPARK Health Sector. Sharing Health Information: An Overview of Fifty Projects. SPARK Report Strategic Planning for Applied Research and Knowledge. Prepared by SPARK Health Sector: Health Informatics Working Group, Burnaby: January, 1992.

Sterling, Norman W. (Provincial Secretariat). Discussion Paper on Privacy: Initiatives for 1984. Ontario; Provincial Secretariat for Resources Development, 1984.

Thacker, B. A. Open and Shut: Enhancing the Right to Know and the Right to Privacy. Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act. Ottawa: The Queen's Printer of Canada, March, 1987.

United States Privacy Protection Study Commission. Personal Privacy in An Information Society: The Report of the Privacy Protection Study Commission. Washington, D.C.: U.S. Government Printing Office, July 1977.

Westin Alan F. Computers, Health Records and Citizen Rights. Washington, D.C.: U.S. Department of Commerce: National Bureau of Standards, December 1976.

Wright, Tom (Commissioner). Health Care Technology: A Privacy Perspective. Toronto: Information and Privacy Commissioner of Ontario, October, 1992.

Wright Tom (Commissioner). Smart Cards. Toronto: Information and Privacy Commissioner of Ontario, April 1993.

Interviews

Brooks, Donella. Manager of Clinical Record Services, Riverview Hospital. Port Coquitlam, February, 8, 1996.

Evans, Darrell. Executive Director, Freedom of Information and Protection of Privacy Association. Vancouver, February, 3, 1996.

Flaherty, David H. Information and Privacy Commissioner of British Columbia.

Jones, Barry. Member of the Legislative Assembly for Burnaby North. Burnaby, January 23, 1996.

Liu, Jian. Freedom of Information and Privacy Analyst, Records Manager, College of Physicians and Surgeons. Vancouver, February, 9, 1996.

Lytle, Linda J. Registrar, College of Pharmacists of British Columbia. Vancouver, February 9, 1996.

MacDonald, Shirley. Health Information Professional, Clinical Records, Riverview Hospital. Port Coquitlam, February, 8, 1996.

Stevens, Pat. Director Patient Documentation, The Fraser-Burrard Hospital Society (Royal Columbian, Eagle Ridge and Ridge Meadows Hospitals). Port Moody, February, 7, 1996.

Vanandel, M. Deputy Registrar, College of Physicians and Surgeons. Vancouver, February 9, 1996.

Journals

Bennett, Colin J. "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-drawing." Canadian Public Administration, Vol. 33 No. 4 (Winter 1990), pp. 551-570.

Bennett, Colin J. "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." Science, Technology, & Human Values, Vol. 16, No. 1 (Winter 1991), pp. 51-69.

Cavoukian, Ann. "Comment: Cohorts and Privacy." Cancer Causes and Control. Vol., 5 (1994), p. 292.

Clark, L. A. "A State by State Evaluation of Patient Access to Hospital Records." Journal of the American Medical Record Association. Vol. 58, No. 6 (June 1987):17.

Flaherty, David H. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." Science, Technology, & Human Values, Vol. 11, Issue 1 (Winter 1986), pp. 7-18.

Flaherty, David H. (1992). "Privacy, Confidentiality, and the Use of Canadian Health Information for Research and Statistics." Canadian Public Administration. Vol. 35, No. 1, pp. 75-93.

Gevers, J. K. M. "Issues in the Accessibility and Confidentiality of Patient Records." Social Science Medicine, Vol. 17, No. 16 (1983), pp. 1181-1190.

Hazell, Robert. "Freedom of Information in Australia, Canada and New Zealand." Public Administration. Vol. 67, No. 2 (London), (Summer 1989), pp. 189-210.

Levine, Carol. "Sharing Secrets: Health Records and Health Hazards." Hastings Centre Report, Vol. 7, No. 6 (December 1977), pp. 13-15.

Levine, Gregory J. "Freedom of Information and Protection of Privacy: B.C.'s New Legislation." The Advocate, Vol. 51, Part 3 (May 1993), pp. 381-389.

McDowell, Jim. "Sick Secrets on the Beach." British Columbia Report, Vol. 5, No. 52 (August 29, 1994), p.11.

Newcombe, Howard B. "Cohorts and Privacy." Cancer Causes and Control, Vol. 5, No. 5 (1994), pp. 287-291.

Regan, Priscilla M. "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations." Journal of Public Policy, Vol. 4 Part 1 (February 1984), pp. 19-38.

Regan, Priscilla M. "Privacy, Government Information, and Technology." Public Administration Review, Vol. 46, No. 6 (November/December 1986), pp. 629-634.

Regan, Priscilla M. "Ideas or Interests: Privacy in Electronic Communications." Policy Studies Journal. Vol. 21, No. 3, (1993). pp. 450-469.

Warren, Samuel D. and Brandeis, Louis D. "The Right to Privacy." Harvard Law Review, Vol. 4 (1893), pp. 193-220.

Westin, Alan F. "Medical Records: Should Patients have Access?". Hastings Centre Report, Vol. 7, No. 6 (December 1977), pp. 23-28.

Westin, Alan F. "Civil Liberties in the Technology Age: Safeguarding the Framers' Guarantees Requires a Vigilant Congress and a Watchful Citizenry." Constitution, Vol. 3, No. 1, (Winter 1991), pp. 56-64.

Legal Cases

McInerney v. MacDonald [1992] 2 S.C.R. 138.

R. v. Dyment [1988] 2 S.C.R. 417.

Newspapers

"Open access to information, B.C.'s ombudsman urges", The Vancouver Sun, March 18, 1991.

"Open access to information, B.C.'s ombudsman urges", The Vancouver Sun, March 18, 1991, A1.

"Veitch declines to disclose amount of warrant request", The Vancouver Sun, March 28, 1991.

"Time is ripe for information law", The Vancouver Sun, November 18, 1991, A12.

"Privacy chief wants access to data bases tightened", The Vancouver Sun, January 10, 1995, A1.

"Invasion of privacy near 'crisis", The Vancouver Sun, March 2, 1995, C17.

"Women's medical records strewn on lawn", The Vancouver Sun, April 4, 1995, A1, A2.

"Shredding of files quick as $65 call", The Vancouver Sun, April 5, 1995, A1, A2.

"Tight restrictions urged on databases", The Vancouver Sun, April 5, 1995, B2.

"Ontario's move to smart card poses questions about privacy", The Vancouver Sun, March 26, 1996, A9.

Reports and Papers

Bennett, Colin J. "Privacy Protection in the Private Sector: Where Do We Go From Here?" B.C. Freedom of Information and Protection of Privacy Association Bulletin. Jan. - Feb. 1996, Number 1.

Doherty, Michael P. Privacy and Access to Information Issues: Self-governing Professions. Prepared for B.C. Freedom of Information and Privacy Association by B.C. Public Interest Advocacy Centre. Vancouver: no date.

Evans Darrell. "New Group Advocates Freedom of Information Law for B.C." Freedom of Information Bulletin. August 7, 1990.

Health Records Association of B.C. "Results of the HRABC Survey - Release of Information and the Freedom of Information and Protection of Privacy Act." 1995.

Lavis, John N and Geoffrey M. Andersen. Prescription Drug Use in the Elderly. Expenditures and Patterns of use under Ontario and British Columbia Provincial Drug Benefit Programs. Queen's-University of Ottawa Economic Projects, Working Paper No. 94-02. Ottawa: University of Ottawa, 1994.

Loukidelis, David, Hunt, Catherine, L. and Osborne, Valerie. Information Rights for British Columbia: Recommendations for Access to Information and Protection of Privacy Legislation for British Columbia. Vancouver: B.C. Freedom of Information and Privacy Association Legislative Task Force, 1991.

Loukidelis, David. Comments on Bill 50, The Freedom of Information and Protection of Privacy Act. The Freedom of Information and Privacy Association Submission to the Attorney General. Vancouver: June 10, 1992.

MacIntosh, Robert M. Information Technology for Health Care in Ontario. Backgrounder. C. D. Howe Institute. Toronto: January 12, 1995.

Trott, Bill, Ashbourne, Judith and Gareau, Richard. Access to and Confidentiality of Health Care Records in British Columbia. Prepared for B.C. Freedom of Information and Privacy Association by Community Legal Assistance Society. Vancouver: 1992.

Statutes

Canadian Statute. Access to Information Act. R.S.C. 1983, c.111.

Canadian Statute. Privacy Act. R.S.C. 1983, c. 111.

British Columbia Statute. Freedom of Information and Protection of Privacy Act. S.B.C. 1992, c.61..

British Columbia Statute. Freedom of Information and Protection of Privacy Amendment Act. S.B.C. 1993, c.46.

British Columbia Statute. Hospital Act B.C. Reg. 289/73.

British Columbia Statute. Privacy Act, 1968.

British Columbia Statute. The Medical Practitioners Act, R.S. B.C., 1979, c.254, s.4(2)(f).

United States Statute. Privacy Act, 1974.