PERSONAL HEALTH INFORMATION AND THE RIGHT TO PRIVACY IN CANADA

An overview of statutory, common law, voluntary and constitutional privacy protection

A FIPA Law Reform Report

Prepared for
B.C. Freedom of Information and Privacy Association
by
Susan Prosser
BC Public Interest Advocacy Centre

Vancouver, May 2000

ACKNOWLEDGEMENTS

We wish to thank Susan Prosser for writing this report and the BC Public Interest Advocacy Centre for accepting FIPA as a client for this purpose.

FIPA gratefully acknowledges
financial assistance from

THE LAW FOUNDATION OF BRITISH COLUMBIA

BC Freedom of Information and Privacy Association
103 - 1093 West Broadway, Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Email: info@fipa.bc.ca • Web: www.fipa.bc.ca

TABLE OF CONTENTS

> A recent survey conducted by the Canadian Medical Association (CMA) revealed that three out of four Canadians believe that the information they give their doctor is kept confidential. The reality is far different; the lineup behind the doctors – all claiming the "need to know" – is long and growing….And technology offers new ways of amassing health information without our consent.
>
> — Privacy Commissioner of Canada, 1999-2000 Annual Report

I. INTRODUCTION[1]

Personal health information is personal information of a particular nature. The Supreme Court of Canada (the "Supreme Court") has characterized medical records as sensitive, highly private and personal to the individual.[2] Moreover, the Supreme Court has recognized that the therapeutic relationship is trust-like in nature and is one in which patients have a high expectation that their personal information will remain confidential. As a result, individuals maintain a fundamental interest in controlling the dissemination of their personal information, especially, as the Supreme Court has said, where aspects of the individual's identity are at stake.[3]

In spite of individuals' interest in maintaining control over the collection, use and disclosure of their personal health information, it is not clear to what extent Canadians have a right to exercise that control. It is clear that Canadians have a right to privacy under the *Canadian Charter of Rights and Freedoms* (the "*Charter*"), but it is unclear what the scope of that right is. Similarly, while Canada and a majority of the provinces and territories have laws designed to protect privacy, it is not clear they provide adequate protection for personal health information in an increasingly networked world.

This climate of uncertainty about individual rights has intensified as information technology has expanded into government offices, health professionals' offices, hospitals and laboratories, to mention only a few. As individuals' health records are increasingly digitized, so the demand for that information grows: with the cost of healthcare claiming an ever-greater percentage of provincial and federal budgets, governments claim that they need access to individual health records to improve the efficiency and effectiveness of government health services, researchers claim that they require personally identifiable health information, and industries such as the pharmaceutical industry want access to personal health information to more effectively develop and market their products.

---

[1] I am grateful to Mary A. Marshall, Richard Speers, Michael Yeo, Brian Foran, David Loukidelis and Pierrot Peladeau for their thoughtful comments on earlier drafts of this paper. Any errors or omissions are, of course, my own.

[2] *McInerney* v. *MacDonald*, [1992] 2 S.C.R. 138 at 148 [hereinafter *McInerney*].

[3] *R.* v. *Mills* (2000), 180 D.L.R. 1 at 46 [hereinafter *Mills*]; see the section entitled Personal Health Information, below, for discussion of identifiable and non-identifiable information.

The Advisory Council on Health Info-Structure, the body that was charged with providing strategic advice to the Minister of Health on the development of an online, national health information system, recognized that privacy is an overarching concern with respect to the collection, use and disclosure of personal health information and individuals' access to their own medical records.[4] The Advisory Council recommended that "all governments in Canada should ensure that they have legislation to address privacy protection specifically aimed at protecting personal health information through explicit and transparent mechanisms"[5], recognizing that the legal mechanisms actually in place to safeguard privacy are woefully inadequate.

For its part, the Canadian Institute for Health Information ("CIHI"), the non-governmental body charged with developing standards and managing some aspects of the health information infra-structure, emphasizes the need for "person oriented information" (read "personal") in order to track individuals' medical history over long periods of time and to integrate "survey or household information with person-oriented data to provide outcome information, socio-economic context, and non-medical health determinants for … healthcare encounters."[6] While CIHI states that privacy is a fundamental value, facilitating adequate privacy protection for the personal health information is not among what it terms "deliverables" in its report entitled the *Health Information Roadmap*.[7]

In the virtual absence of privacy legislation specifically aimed at protecting personal health information, it seems important to examine the nature and extent of privacy rights in Canada. The laws currently in place to protect the privacy of Canadians' personal information have been described by many as a "patchwork". [8] Federal and provincial privacy laws govern their respective public sectors; provincial laws govern the different care facilities such as hospitals and extended care facilities; and codes of ethics govern healthcare professionals. While some provinces have adopted legislation that deals specifically with health information, the privacy standards vary wildly between them. **And finally, with the exception of Quebec, no jurisdiction either**

---

[4] Final Report of the Advisory Council on Health Info-Structure, *Canada Health Infoway: Paths to Better Health* (Ottawa: Minister of Public Works and Government Services, 1999) [hereinafter ACHI's Final Report] at 5-1. Available on the internet at http://www.hc-sc.gc.ca/ohih-bsi/achis/fin-rpt/fin-rpt_e.pdf.
The Canada Health Infoway is a pan-Canadian health information highway that is being developed, in the words of ACHI, to provide better health information; to improve the quality, accessibility, portability and efficiency of health services across the entire spectrum of care; to enable the creation, analysis and dissemination of the best possible evidence from across Canada and around the world as a basis for informed decisions by patients, citizens, informal caregivers, health and providers, and health managers and policymakers. ACHI's Final Report, infra note 4, at 3.

[5] *Ibid.* at 5-3.

[6] Health Canada, Statistics Canada, *Health Information Roadmap: Beginning the Journey* (Canadian Institute for Health Information: Ottawa, 1999) at 6 [hereinafter *Information Roadmap*].

[7] *Ibid.*.

[8] House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Where do We Draw the Line* (Ottawa: Public Works and Government Services Canada, April 1997) at 23 [hereinafter Where do We Draw the Line].

provincial or federal has passed laws specifically governing privacy in the private sector, although Bill C-6 may well be passed in the spring 2000 session of Parliament.

The objective of improving the effectiveness and efficiency of the Canadian health system through information technology while protecting privacy is often presented as a balancing act[9] in which, it is asserted, some aspects of personal privacy must give way to the public interest in improving healthcare. Privacy is more often seen as an obstacle rather than a goal.

There are, however, challenges on several fronts to the notion that privacy can or ought to be sacrificed in the public interest. One, a legal challenge, is that individuals have a reasonable expectation of privacy with regard to their personal health information and that this reasonable expectation of privacy is a constitutionally protected human right.

A second challenge is a political one: the goal of improving the effectiveness and efficiency of healthcare provision depends on the accuracy and comprehensiveness of the information at issue. If patients and their care-providers do not have full confidence in the way medical information is handled, the accuracy and comprehensiveness of the information they provide may be undermined."[10]

A third challenge to the alleged need to sacrifice privacy comes from the realm of technology: the technological means to encrypt or otherwise render health information non-identifiable do exist, and this is a workable solution since there are very few transactions that require personally identifiable health information.

This paper will only address the first challenge, by examining the legal basis for challenging the proposition that the right to privacy must – or even can– be sacrificed to develop a robust health infostructure.

This paper will provide an overview of the statutory, common law, voluntary and constitutional rules and principles that currently protect individuals' personal health information. While there will be some discussion of the adequacy of current statutory protection, the primary objective of this paper is to present the law as it currently stands in order to generate discussion about the future of privacy protection for health information in Canada.[11]

---

[9] Andrea Neill, "Regulatory and Legislative Strategies in Canada" Background Document for Discussion in Workshops (Document presented at the Conference Ensuring Privacy and Confidentiality on the Health Iway, St. John's Newfoundland, 2-3 October, 1997) at 2.

[10] Drew Duncan, *Health Information Legislation Review: Does British Columbia need a Health Information Act?*, A Report to the Health Information Steering Committee, Ministry of Health, February 27, 1998, University of Victoria.

[11] This paper is indeed an overview of privacy protection as it relates to personal health information and not a comprehensive analytical or comparative study of the laws themselves.

Throughout this paper, the principles of the Canadian Medical Association's Health Information Privacy Code[12] (the "CMA Privacy Code") will be referred to by way of counterpoint. This form of commentary has been chosen for several reasons. First, the CMA Privacy Code is a sectoral code based on the Canadian Standards Association's Model Code[13] (the "CSA Model Code"), the same code that is appended to the *Personal Information Protection and Electronic Documents Act* ("Bill C-6").[14] Secondly, the CMA Privacy Code has, in its own words, been "produced by physicians to protect the privacy of their patients, the confidentiality and security of their health information and the trust and integrity of the therapeutic relationship."[15] And thirdly, the development of the CMA Privacy Code was inspired by the report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities entitled *Privacy: Where Do We Draw the Line*?

For all these reasons, the CMA Privacy Code provides a unique touchstone for privacy principles founded on patients' expectations of and physicians' duty of confidentiality, and patients' right to maintain control over the personal health information they divulge in confidence.

Because the *Charter* forms the backbone of human rights protection in Canada, and all other laws in Canada must be compatible with it, an analysis of the Supreme Court's position on the right to privacy under the *Charter* is covered in somewhat greater depth than the statutory sections of the paper.

In order to better situate the overview that follows, this paper begins with a brief history of privacy and access to information legislation and considers some of the concepts on which privacy legislation is built.

II. A BRIEF HISTORY OF PRIVACY LEGISLATION

The right to privacy, in its most general expression, is understood as "the right to be let alone". Although this expression of the nature of privacy first appeared in a seminal article on privacy rights in the *Harvard Law Review* in 1890,[16] it has since been adopted by the Supreme Court in many of its decisions. Alan Westin defines "informational privacy" as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is

---

[12] Canadian Medical Association, CMA Health Information Privacy Code (Approved by the CMA Board of Directors, 15 August 1998), section A: Scope [hereinafter CMA Privacy Code].
[13] Canadian Standards Association, *Model Code for the Protection of Personal Information* (Etobicoke: Canadian Standards Association, 1996)
[14] S.C. 2000, c. 5. Bill C-6 received Royal Assent on April 13, 2000 and will enter into force on January 1, 2001.
[15] CMA Health Information Privacy Code, section A: Scope.
[16] Samuel C. Warren & Louis D. Brandeis, "The Right of Privacy" (1890) 4 *Harvard Law Review* 193 at 195.

communicated to others"[17] and his definition has often been cited by the Supreme Court. In a recent decision, the Supreme Court has affirmed that a right to a reasonable expectation of privacy against government encroachments is protected by both sections 7 and 8 of the *Charter* for, in the words of Mister Justice La Forest in *R*. v. *Dyment*, "privacy is at the heart of liberty in a modern state."[18] Not only has the Supreme Court recognized that "concerns about privacy are greatest where aspects of one's individual identity are at stake", but also that privacy is essential to maintaining relationships characterized by trust, such as that between healthcare providers and their clients.[19]

The first data protection laws were passed in Europe in the 1970s. In 1981, the Organization for Economic Cooperation and Development put forward its code of fair information practices, the *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* (the "OECD Guidelines").[20] Although the OECD Guidelines are voluntary, in 1984, Canada and 23 other industrialized nations formally agreed to adhere to them. For its part, the European Union has adopted the OECD Guidelines in its *Directive on the Protection of Individuals with Regard to the Processing of Personal Data* (the "EU *Directive*")[21] and the EU *Directive* binds member states. Even though Canada is not a signatory to the EU *Directive*, it has had a direct impact on the development of Canadian law because the EU *Directive* prohibits the transborder flow of personal information to non-member states that do not have equivalent or better data protection. For example a German research organisation might refuse to transfer its personal health information data to a research organisation in a Canadian province if that province did not offer the same or superior privacy protection for such data as the European Union member-state. This is one of the reasons why the federal private sector privacy Bill, Bill C-6 incorporates a code of fair information practices that is even more stringent than the *OECD* Guidelines.

Almost 30 years ago, a federal Task Force released its report, *Privacy and Computers*. Interestingly, in its conclusions, the Task Force noted that concerns about disparity in power between individuals and institutions sprang less from possible loss of individual privacy than from the more Orwellian fear that "the possession by institutions of extensive and efficient information systems will enhance their ability to manipulate individuals and induce conformity."[22] In 1980, Horace Krever

---

[17] Westin, Alan F., *Privacy and Freedom* (New York: Antheneum, 1967) at 7.
[18] (1989), 55 D.L.R. (4th) 503, at 513 [hereinafter *Dyment*].
[19] *Mills*, *supra* note 3 at 47.
[20] OECD, Guidelines *for the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1981).
[21] Council of the European Parliament. 1995. Directive 95/46/EC on the *Protection of Privacy and Transborder Flows of Personal Data and the Free Movement of such Data.*
[22] Privacy and Computers, Report of a Task Force established jointly by Department of Communications/Department of Justice (Ottawa: Information Canada, 1972) at 178.

released his *Report of the [Ontario] Commission of Enquiry into the Confidentiality of Health Information*.[23] What began as a modest study of provincial legislation and associated administrative processes became a large scale inquiry as "the true magnitude of the abuses that were taking place with respect to the confidentiality of healthcare records" was revealed.[24] Canada passed the *Privacy Act*[25] in 1982 and with the exception of Prince Edward Island all provinces and territories in Canada have since passed privacy legislation designed to protect personal information held by public sector institutions. However, only Quebec has legislation specifically aimed at protecting personal information held in the private sector.

As the use of information technology in the health field grew in the '80s and '90s, so did concerns about the adequacy of the common law and existing statutes to adequately protect the privacy of health information. New Zealand broke new ground by issuing its Health Information Code 1994 under its *Privacy Act* 1993.[26] That Code, like subsequent health information codes, is based on the privacy principles set out in the OECD Guidelines. Since that time Ontario developed a draft *Personal Health Information Protection Act*, but it was never introduced into the legislature. More recently, Manitoba, Saskatchewan and Alberta have passed statutes that deal specifically with the collection, use and disclosure of personal health information, but only that of Manitoba is in force.

III. PRIVACY CONCEPTS IN THE CONTEXT OF PERSONAL HEALTH INFORMATION

The following is an overview of the terminology and concepts that are essential to understanding any framework for the legal protection of privacy. Emphasis has been placed on these concepts in the hope that they will facilitate meaningful and informed discussion on the strengths and weaknesses of any given legislative framework by alerting the reader to privacy issues at stake.

1. Privacy as a Human Right

The human rights approach to privacy acknowledges privacy as a moral and social value.[27] Canada is a signatory to a number of international human rights

---

[23] (Queen's Printer for Ontario: Toronto, 1980) [hereinafter Krever Report].
[24] *Ibid*., vol. 1 at 1.
[25] *Privacy Act*, R.S.C. 1985, c. P-21.
[26] Barbara von Tigerstrom, "The 'Hidden Story' of Bill C-54: The Personal Information Protection and Electronic Documents Act and Health Information" (1999) 8: 2 *Health Law Review* 12 (QL), para 16.
[27] Privacy Commissioner/Ontario, "Privacy as a Fundamental Human Right vs. an Economic Right: an Attempt at Conciliation". Available on the internet at **Error! Reference source not found.** [hereinafter Privacy as a Fundamental Right]

instruments that recognize privacy as a fundamental human right. For example, the *Universal Declaration of Human Rights* provides, at Article 12, that no one shall be subjected to arbitrary interference with his privacy and that everyone has the right to the protection of the law against such interference. And Article 17 of the *International Covenant on Civil and Political Rights* prohibits arbitrary *and unlawful* interference with individuals' privacy.

Canada's *Charter*, like the United States' Constitution does not explicitly provide for privacy, but the Supreme Court of Canada has recognized that the right to privacy is a fundamental human right that underpins *Charter* rights to liberty and security of the person and the right to be free from unreasonable search and seizure. For its part, the *Quebec Charter of Human Rights and Freedoms* (the "*Quebec Charter*") states explicitly at section 5: "Everyone has the right to respect for his private life" and at section 9: "Every person has a right to non-disclosure of confidential information."

Sheila Finestone, the Chair of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities (the "Commons Committee") that heard from many Canadians on the issue of privacy in the private sector, defined privacy as "a core human value that goes to the very heart of preserving human dignity and autonomy."[28] This analysis echoes that of Madame Justice Wilson in *R.* v. *Morgentaler* where she noted that *Charter* rights and the right to individual liberty guaranteed by section 7 of the *Charter* are tied inextricably to the concept of human dignity, and that the section 7 right to liberty must be read to "guarantee[] to every individual a degree of personal autonomy over important decisions intimately affecting their lives."[29]

In its Report, *Privacy: Where Do We Draw the Line*, the Commons Committee noted that the kind of question you ask will often determine the answer you get. Thus they concluded:

> … if we approach privacy issues from a human rights perspective, the principles and solutions we arrive at will be rights-affirming, people-based humanitarian ones. On the other hand, if we adopt a market-based or economic approach, the solutions will reflect a different philosophy, one that puts profit margins and efficiency before people and may not first and foremost serve the common good.[30]

---

[28]Where do We Draw the Line, *supra* note 9 at 6.
[29] [1988] 1 S.C.R. 30, as cited by Madame Justice L'Heureux-Dubé in *R.* v. *O'Connor* (1995), 130 D.L.R. (4th) 235 at 287 [hereinafter *O'Connor*].
[30] Where do We Draw the Line, *supra* note 9 at 33.

The Commons Committee recommended that the federal government adopt a Canadian Charter of Privacy Rights that would enshrine, amongst other privacy rights, specific rights related to personal information as follows:

- Everyone is the rightful owner of their personal information no matter where it is held and this right is inalienable
- Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified.[31]

2. Confidentiality and Security

With respect to the use and disclosure of health information, physicians have traditionally been bound to guard the confidentiality of their patients' health information by the Hippocratic Oath.[32] Professional codes of conduct, adopted by most healthcare professional organizations pursuant to their regulatory powers, enshrine the duty of confidentiality. The interest of confidentiality is linked not to the autonomy and security of the individual, as privacy is, but to the nature of the information and to professional duty. As Mary Marshall has pointed out, "it is an interest only so far as recognized and fostered by the law making authority, and … a central law making authority may abrogate this interest when necessary."[33]

In *McInerney*, Mister Justice La Forest cited *Halls v. Mitchell*, a 1928 decision of the Supreme Court of Canada with approval: "There Duff J. held that professional secrets acquired from a patient by a physician in the course of his or her practice are the patient's secrets and, normally, are under the patient's control."[34] Mister Justice La Forest reiterated that the duty of confidentiality requires of the practitioner that professional secrets not be divulged, unless some paramount interest, such as public health or imminent harm to a third party, overrides it.[35] Patients confide information to physicians in trust. Any divulgation without

---

[31] *Ibid*. at 38; note that Senator Sheila Finestone has since released "Charting our Future Together: Consultation on a Draft Charter of Privacy Rights", a draft of a bill she intends to introduce before the end of the spring 2000 session of Parliament.

[32] J.K. Mason and R.A. McCall Smith, *Law, Medicine and Ethics*, as cited by Robert Lee, *Confidentiality and the Law, ed. by Linda Clarke* (Lloyd's of London Press: London, 1990) at 23-24. The Oath states that "whatever in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken abroad, I will not divulge as reckoning that all should be kept secret."

[33] The Office of Health and the Information Iway, *Confidence, Confidentiality and Privacy: A report on barriers to the transfer of personally identifiable health information between jurisdictions* by Mary A. Marshall (Alberta: Health Canada, May 6, 1998) at 3 [hereinafter Marshall].

[34] *Halls v. Mitchell*, [1928] S.C.R. 125 at 136, as cited in *McInerney*, *supra*, note 2 at 148.

[35] *Ibid*. at 154.

consent, even if it is *authorized* by law, is breach of the duty of confidentiality.[36] Likewise,

> Loose use of the term 'confidentiality' to mean assurance of 'authorized' use and disclosure likewise obscures the physician's duty of confidentiality. For a 'data custodian', protecting confidentiality could simply mean ensuring that information is disclosed only as 'authorized'. A data custodian is not under a duty of confidentiality in the proper sense of the term. A duty to ensure that information is disclosed only as authorized is not equivalent to a duty of confidentiality.[37]

Confidentiality must be distinguished from privacy. One thing that distinguishes them is control. The right to privacy protects individuals' rights to control the flow of their personal information. The duty of confidentiality defines professionals' obligations with regard to personal information disclosed to them. Another distinction between privacy and confidentiality is, as indicated above, a growing recognition of privacy as a fundamental human right possessed by every individual and deserving of constitutional protection. Note, however, that this distinction does not exist under the *Quebec Charter* which, as indicated above provides that every person has the right to non-disclosure of confidential information. The importance of a constitutionally protected right to privacy or confidentiality is that it cannot be abrogated by ordinary laws (see section VI.4, below).

Security is distinct from both confidentiality and privacy. It is the means by which informational confidentiality and privacy are achieved. Security measures are the safeguards put in place to control access to information in order to protect both the information system and its contents from unauthorized access. In a paper-based system, security may be as rudimentary as a lock on the records door or a pass-key system. In computer-based information systems, privacy enhancing technologies ("PETs") - a range of technologies that safeguard personal privacy by minimizing or eliminating the collection, use and disclosure of identifiable data,[38] are in a state of rapid development. Legislators often express the desire to make privacy

---

[36] Note, however, a disquieting decision of the England and Wales Court of Appeal, *Re Source Informatics Ltd.*, [1999] E.W.J. No. 6880 (Q.L.), wherein the Court found that the duty of confidentiality is not breached where, for a fee, physicians disclose anonymized personal health information to a company who in turn sell that information to pharmaceutical companies who seek information on doctors' prescribing habits for marketing purposes.

[37] Michael Yeo, Protecting the Privacy and Confidentiality of Health Information: Context, Perspectives and Stakeholders (Canadian Medical Association, Ottawa) [unpublished].

[38] Information and Privacy Commissioner/Ontario & Registratiekamer (The Netherlands), Privacy-Enhancing Technologies: The Path to Anonymity, vol. 1 (Information and Privacy Commissioner/Ontario: Toronto, 1995) at 5. Available on the internet at **Error! Reference source not found.**.

legislation "technology neutral" on the assumption that "although technology poses threats to privacy, the law and technology itself can be effective in countering these threats".[39]

3. Personal Health Information

The Supreme Court of Canada has defined personal health information to be "information that goes to the personal integrity and autonomy of the patient." In the context of the physician-patient relationship – or any other therapeutic relationship where the professional is bound by a duty of confidentiality- it is information that the patient "entrusts" to the physician with the expectation that it will be held confidential.[40] As discussed below, the context in which personal health information is disclosed by a patient, client, employee, student, life-insured, etc. determines the rights the individual has with respect to that information.

Until recently, personal information was divided into two broad categories: identifiable and non-identifiable. The information within each of these 2 categories is either eponymous (names the individual), pseudonymous (the person is identified by a personal information number ("PIN"), for example) or anonymous.[41] Identifiable or personal health information is information that contains identifiers permitting identification of the person concerned, whether that be through name, address, personal identification number or any other grouping of information that would permit the person to be identified.

Thus, it is possible to have anonymous or pseudonymous information, where the individual's name is simply removed or replaced by a PIN, that is nonetheless identifiable through the individual's phone number, medical condition, blood-type or some combination of factors that taken together identify the individual. Ontario, in its draft legislation, *An Act Respecting Personal Health Information and other Matters*, defined personal health information broadly to include "information that can be linked or matched with other information in order to identify the subject of the information."[42]

---

[39] von Tigerstrom, *supra* note 26 , para 33.
[40] *McInerney*, *supra* note 2 at 148.
[41] A further elaboration of these distinctions is beyond the scope of this paper, but for an excellent exposé of this terminology see Pierrot Péladeau's forthcoming book: *Par delà de la vie privée: Réelles ou virtuelles, nos vies informatisées* (working title). January 24, 2000 version of manuscript to be published in French and English (working title: *Beyond Privacy: Virtual or Real, Our Digitalized Lives*), Isabelle Quentin éditeur, Montreal.
[42] Health Information Steering Committee, *Health Information Legislation Review: Does British Columbia need a Health Information Act?* (Report) by Drew Duncan (Victoria: BC Ministry of Health, February 27, 1998) at 2 [hereinafter Duncan].

Non-identifiable or aggregate health information, then, is information from which the personal identifiers have been removed. Generally, this information does not raise privacy concerns because the individual cannot be identified. However, if this information is de-aggregated, linked or data-matched, or where sample sizes are small, even information which is non-identifiable on its face may allow individuals to be identified.[43] Non-identifiable or aggregate health information may also raise privacy concerns where it targets a group of individuals who may be distinguished – and possibly discriminated against - on the basis of race, age, sexual orientation, area of residence or other identifying characteristics.

4. Who Owns Personal Health Information?

To answer this question, one must, under Canadian law, make a distinction between the information itself and the record which contains the information. In 1985, the Canadian Medical Association made a policy statement entitled Confidentiality, Ownership and Transfer of Medical Records:

> The Canadian Medical Association regards medical records as confidential documents, owned by the physician/institution/clinic that compiled them or had them compiled. Patients have a right to the information contained in their records, but not to the records themselves.

In other words, the body that has produced the record is the owner of the physical record, while the information contained in the record remains, according to the Supreme Court, "in a fundamental sense" that of the patient.[44] In *McInerney* the Supreme Court found that although the patient does not own the records, s/he has an absolute right of access to the records unless the entity holding the records can demonstrate in a court of law that it has reasonable grounds for claiming that access to such information is not in the patient's interest.[45] Similarly, the patient has a right to require that professional secrets acquired by a practitioner not be divulged, and this right is absolute unless there is some paramount reason that overrides it. Whereas *McInerney* was concerned with the common law rights of the individual with regard to access to their personal health information, the Supreme Court has stated that the right to informational privacy is based on the notion of dignity and integrity of the individual,[46] fundamental values that the *Charter* serves to protect.

---

[43] *Ibid*. at 2.
[44] *McInerney*, *supra* note 2 at 148; see also *Halls* v. *Mitchell*, [1928] S.C.R. 125 at 136.
[45] *Ibid*. at 154.
[46] *Dyment*, supra note 18 at 429.

The question of whether a patient has a proprietary interest in his or her health records remains an open question. Alan F. Westin, an American privacy law expert, argues that individuals should be given proprietary rights in their personal information.[47] The Ontario Information and Privacy Commissioner recently published a paper putting forward an argument for empowering individuals, who are faced with limited choices when asked to divulge their personal information in exchange for services, by creating a structured market for personal information premised on ownership and its attendant legal principles.

Bill C-6 takes a rights rather than an ownership approach to information privacy. Section 3 of Bill C-6 provides that the purpose of Part 1 of the Bill is, *inter alia*, to establish rules "to govern the collection, use and disclosure of personal information in a manner that recognizes the *right of privacy* of individuals…." [Emphasis added.]

While most Canadian privacy advocates favour a human rights-based privacy approach rather than an economics-based property rights approach to the control of personal information, it is arguable that the former is preferable only inasmuch as the right to privacy is accorded constitutional protection.[48] But, as mentioned above, because *McInerney* explored the right to control one's personal health information from the perspective of patients' right of *access* to their records and not from the perspective of use or disclosure of that information, the Supreme Court was not required to address the nature and extent of the right to health information privacy.

5. Consent

On the one hand highly private personal health information is "in a fundamental sense one's own, for the individual to communicate or retain as he or she sees fit."[49] On the other hand, in the therapeutic context, patients do disclose their personal information, but usually within a relationship of trust where the expectation is that the information will be held confidential. Informed consent to collection, use and disclosure of individuals' personal health information is at the core of privacy protection.[50] Since an individual must necessarily divulge personal information in order to obtain services, consent is the only means by which individuals can exercise control over their personal information, control that

---

[47] Westin, *supra* note 17.
[48] For a discussion of these two approaches see Privacy as a Fundamental Human Right, *supra* note 27.
[49] *McInerney*, *supra* note 2 at 148.
[50] Canadian Medical Association, "Putting Patients First: Comments on Bill C-6" (Submission to the Senate Standing Committee on Social Affairs, Science and Technology, November 29, 1999) [hereinafter Putting Patients First].

individuals have the right to exercise.[51] Whereas the federal *Privacy Act* makes no provision for consent with respect to the collection of personal information, Bill C-6 provides for "express consent". However, express consent is not defined in the Bill. As the CMA points out, it appears that express consent is not what in the healthcare sector is termed "informed consent."[52]

From a patients' rights perspective, patients should have the right to have their health records maintained in confidence and not used for any purpose other than to provide them with public health services unless they consent to another use or disclosure to a third party. With regard to disclosure of an individual's personal health information to a third party, Mr. Horace Krever stated:

> Ideally, an informed consent, as applied to disclosure of confidential health information, should indicate that the person authorizing the disclosure of the information knows precisely what is being released, why it is being released, the possible consequences of the disclosure and that he or she knows that he or she may refuse to sign the consent, or may rescind it, if appropriate, after it has been signed.[53]

From the physician's perspective, informed consent means "a patient's informed and voluntary agreement to confide or permit access to or the collection, use or disclosure of his or her health information for specific purposes."[54]

Implied consent must be distinguished from explicit consent. Whether consent can be implied has nothing to do with the relative sensitivity of the information. Consent should not be implied, as is the case under Principle 4.3.6 of Bill C-6, merely because the personal information is less sensitive. Rather consent must only be implied "where agreement may reasonably be inferred from the action or inaction of the individual and there is good reason to believe that the patient has knowledge relevant to this agreement and would give express consent."[55]

6. Knowledge, Notification & Justification

In order to make an informed decision about whether to consent to the collection, use or disclosure of one's personal health information, an individual must be informed of the purpose for which that information is being collected. While knowledge of that purpose is an important component of consent, it is not, in and

---

[51] *McInerney*, *supra* note 2 at 148.
[52] Putting Patients First, *supra* note 50 at 21.
[53] Krever Report, *supra* note 23, vol. 3 at 5; see also Recommendation 90 at 9.
[54] Putting Patients First, *supra* note 50 at 22.
[55] CMA Privacy Code, *supra* note 15, section B: Definitions: "Consent".

of itself sufficient. Notification then must not be substituted for consent.[56] Furthermore, in the context of health information, knowledge and consent are not sufficient to guarantee individuals' right to privacy, that is, on their own they do not give individuals adequate control over their personal information. The effectiveness of consent as a mechanism for controlling the collection, use and disclosure of individuals' personal health information is attenuated by the fact that the individuals concerned generally require the healthcare services they seek (i.e. they do not have a choice about whether or not to divulge their personal information) and by the fact that obtaining effective service literally depends on individuals' thoroughly divulging the relevant information. As a result, in the therapeutic context, the principle of justification would limit organizations' authority to collect information to situations where there is a just or legitimate reason to do so.

A couple of jurisdictions have adopted a justification principle: Bill C-6, in subsection 5(3) states that "an organization may collect, use or disclose personal health information only for the purposes that a reasonable person would consider are appropriate in the circumstances"; section 4 of Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*[57] refers to a "serious and legitimate purpose" for establishing a file on an individual.

7. Collection

Personal information may be collected directly from the individual or from other individuals or entities. Principle 3 of the CMA's Privacy Code provides that non-consensual collection of health information...

> …is a violation of the patient's right of privacy, compromises the physician's duty of confidentiality and is potentially disruptive of the trust and integrity of the therapeutic relationship. Therefore it must occur in very limited circumstances – namely emergency situations, in accordance with legislation that meets the requirements of this Code or in response to a court decision or order.[58]

In contrast to this view, many privacy statutes provide that information must be collected directly from the individual concerned, but do not require that the individual concerned consent to such collection. Moreover, statutes such as the federal *Privacy Act* and the BC and Ontario Freedom of Information and Protection of Privacy Acts, create many exceptions to direct collection and no provision is

---

[56] See Putting Patients First for a detailed analysis of the shortcomings of Bill C-6 regarding the distinction between knowledge and consent, *supra* note 50 at 16-18.
[57] R.S.Q., c. P-39.1.
[58] *Supra* note 15.

made for obtaining consent: the federal *Privacy Act* creates 14 exceptions to direct collection, the BC *Freedom of Information and Protection of Privacy Act* ("BC FIPPA)creates 20 and sections 39 and 42 of the Ontario Freedom of Information and Protection of Privacy Act create at least 20 exceptions. Significantly, section 6 of Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* creates only 3 exceptions to direct collection. Admittedly, these laws are general privacy laws. The question is whether health information should be treated differently; whether direct collection is an acceptable substitute for informed consent; whether the myriad exceptions to direct collection of personal health information are acceptable.

8. Use

Once an entity collects personal information, it may simply hold or store it, it may use it or it may disclose it to third parties. Use, then, is use by the entity that has collected the information. Privacy statutes determine what is a valid or legal use of personal information. Under the federal *Privacy Act* and most of its provincial equivalents an entity may use personal information for the purpose for which it was gathered or for a consistent purpose without the consent of the individual concerned. In contrast, section 13 of Quebec's *Act Respecting the Protection of Personal Information in the Private Secto*r provides that personal information may not be used or communicated to a third party for a purpose not relevant to the object of a file "unless that person concerned consents thereto or such communication or use is provided for by [the] Act." The *Act* creates no exceptions to the principle of use with consent.

When information is collected directly from individuals in order to provide healthcare services to the individuals concerned, and individuals are informed of the purpose to which that information will be put, it is acceptable to use their personal health information for the purpose for which it was collected. The CMA argues that in the case of health information it is absolutely necessary or the medical system would grind to a halt.[59] The case of use for the purpose for which the information was collected is an example of where consent can be implied – unless of course the individual concerned has expressly withdrawn his or her consent. However, use for a *consistent* purpose is highly controversial because it is often ill-defined or undefined and leaves broad latitude for information to be used

[59] *Ibid*. at 15. Note that the CMA makes a distinction between collection, use and disclosure of personal information for a "primary therapeutic purpose", which is defined in section B as the delivery of healthcare to the particular patient with respect to a particular and immediate health need or problem, and a "secondary legislated or non-legislated purpose". The CMA's strongest criticism of Bill C-6 is based on the Bill's failure to recognize that in the case of personal health information it is imperative to make this distinction and to have rules which apply accordingly.

in ways individuals would never have anticipated when their personal information was collected.

9. Disclosure

When an entity gives personal information it holds to a third party, be it an individual, an organization or a government official, this is disclosure. The rules surrounding disclosure are much more nuanced than those surrounding collection and use and thus far, with the exception of Quebec's private sector privacy legislation, the general privacy laws in Canada only regulate disclosure by government bodies. Generally, the private sector is under no legal obligation to limit how or to whom it discloses personal health information.[60] Under fair information practices, the principle guiding disclosure is consent, just as it is for collection and use. As a corollary, individuals are entitled to refuse or withdraw their consent. For example, under Principle 4.3.7 of the CSA Model Code, individuals must be provided with an opportunity to consent or refuse consent. However, under most privacy laws, including Bill C-6 and even those that specifically address the treatment of personal health information, there are many exceptions to the principle of consent with regard to disclosure.

First, entities governed by provincial and federal public sector privacy laws and provincial health information laws, may disclose individuals' personal information without their consent where disclosure is made for the purpose for which the information was originally collected (in most cases this purpose would be the provision of healthcare for the benefit of the individual concerned.) The CMA's Privacy Code and Saskatchewan's *Health Information Privacy Act* (HIPA) define this purpose as the primary purpose.[61] The CMA code avoids the difficulty of disclosure without consent by providing that, with some exception, consent to disclosure may be implied where disclosure is for a primary purpose. For example, a medical laboratory need not ask an individual for consent to disclose the results of a lab test to his or her physician. Disclosure of the test results to the treating physician is considered to be disclosure for a primary purpose or for the purpose for which the test was taken in the first place; that is, diagnosis. In this example, consent can be implied: from the individual's actions there is good reason to believe that if asked explicitly, s/he would consent to having the test results sent back to the treating physician.

---

[60] But see below, section V.2: many health professionals in the private sector are regulated by professional codes of conduct that enshrine the duty of confidentiality.

[61] Note however that Saskatchewan's HIPA fails to define primary purpose in terms of **delivery of care** and **benefit** to the patient; rather the definition begs the question: section 2(m) states: "'primary purpose' means the purpose for which personal information was originally collected, and includes any purpose that is consistent with that purpose."

Second, entities may disclose personal information for a consistent purpose. Where this purpose is not a primary purpose - that is to deliver healthcare for the benefit of the patient - the CMA considers disclosure of personal health information unacceptable.[62] This is even more emphatically the case in the context of the Health Infoway given that the CIHI's *Health Information Roadmap* mandates "combin[ing] administrative data over time and across the continuum of care" and expanding the range of data collected, used and disclosed to include the "non-medical determinants of health." [63]

Third, the privacy statute itself may create statutory exceptions to the rule of consent for such things as law enforcement, compliance and fraud investigations, compliance with a court order, compliance with audit procedures, or compelling circumstances that may affect an individual's health or safety.

And finally, other statutes may, for reasons of public health and/or safety, create exceptions to the relevant privacy statute and/or a duty of confidentiality by requiring disclosure of personal health information. This is the case, for example, with the Ontario *Health Protection and Promotion Act*,[64] which requires health professionals, hospital administrators and lab operators to report a number of "reportable" communicable and virulent diseases. Many provincial highways acts provide for mandatory or voluntary reporting by physicians of conditions that would make it dangerous for an individual to drive.[65] Professional codes, which generally impose a duty of confidentiality on the professional, may also create exceptions to confidentiality. For example, the Ontario Council of the College of Physicians and Surgeons defines "professional misconduct" with respect to the duty of confidentiality as:

> Giving information concerning the condition of a patient or any services rendered to a patient to a person other than the patient or her authorized representative *except* with the consent of the patient or his or her authorized representative *or as required by law.*[66] [Emphasis added.]

10. Access

Access must be distinguished from disclosure. With respect to personal health information, access refers to an individual's right to see his/her own medical

---

[62] Putting Patients First, *supra* note 50 at 14.
[63] *Information Roadmap*, *supra* note 7 at 6.
[64] R.S.O. 1990, c. H-7.
[65] *Ontario Traffic Act*, R.S.O. 1990, c. H-8 (mandatory reporting); *Nova Scotia Motor Vehicle Act*, R.S.N.S., 1989, c. 292 (reporting is permitted, not required)
[66] O. Reg. 856/93, s. 1(1)10 under the *Regulated Health Professions Act*, 1991, S.O. 1991, c. 18, as cited by Ronald D. Manes & Michael Silver, *The Law of Confidential Communications in Canada* (Toronto: Butterworths, 1996) at 18.

record or other personal information held by the government. Currently in Canada, federal and provincial access to information laws only guarantee access to information held by federal and provincial, municipal and local public bodies respectively. Bill C-6, should it be passed will guarantee that citizens have access to such information held by private sector commercial entities. Currently, some businesses, anxious to demonstrate their commitment to respecting individual privacy and to foster a climate of transparency have voluntarily adopted fair information practices, such as the CSA Model Code or a sectoral code based on the CSA Model Code, and have made information about their policies and practices relating to management of their clients' personal information available to the public.

11. Oversight

Oversight is the mechanism by which compliance with a statute's provisions is monitored and, in some cases, enforced. With respect to privacy legislation, not all jurisdictions have created the same oversight mechanisms. For instance, the federal *Privacy Act* and those of the territories and the province of Manitoba, provide for an ombudsman or ombudsman-like body to oversee the functioning of their respective privacy acts.

Ombudsmen are politically independent and impartial intermediaries who rely on consultation, conciliation and negotiation to facilitate the public's access to information and/or ensure that individuals' statutory privacy rights are respected.[67] Ombudsmen have no order-making power, meaning that their decisions, with regard to investigations and in response to privacy and access complaints, are in the form of recommendations. While ombudsmen have no power to enforce their decisions, in some cases, under section 41 of the *Privacy Act* for example, their decisions may be appealed to a court of law or the Ombudsman may apply to a court for a review of a refusal to disclose information.

Other provinces, such as Quebec, Alberta, British Columbia and Ontario have created oversight regimes wherein a privacy commissioner has extensive investigative and regulatory or order-making powers. However, the two models are not necessarily mutually exclusive in that the order-making power is not necessarily exercised if the complaint can be resolved through mediation.

Under the *Privacy Act*, Bill C-6 and some provincial regimes, privacy commissioners have powers of audit or inspection. These powers address the

---

[67] Brian Foran, "Electronic Commerce: *The Personal Information Protection and Electronic Documents Act* and the Role of the Office of the Privacy Commissioner" (Notes for Riley Information Services Inc. Seminar *Electronic Commerce & Privacy Legislation: Building Trust and Confidence*, 23 February 1999). Available on the internet at http://www. privcom.gc.ca.

interrelated goals of transparency and public confidence. In the context of information networks, audit power is especially important because generally individuals will be unaware that their personal information has been collected, used or disclosed in a manner that does not conform with the relevant statute. As David Flaherty has said, "Audits are crucial to an activist, aggressive stance; …it is necessary to create an atmosphere of prior restraint for prospective privacy offenders."[68] The May, 2000 exposure of Human Resources and Development's data file by the Office of the Privacy Commissioner of Canada is a perfect example of the power of the power of audit !

IV. PUBLIC SECTOR PROTECTION OF PERSONAL INFORMATION

1. The Federal Public Sector: The *Privacy Act*

The federal *Privacy Act* has two purposes: to protect the privacy of personal information, that is information about an identifiable individual that is recorded in any form; and to provide individuals with a right of access to that information. Unlike Bill C-6,[69] the *Privacy Act* does not recognize a right of privacy *per se*. Under section 3 of the *Privacy Act*, an individual's name, address, information relating to an individual's medical history, opinions about the individual are all "personal information", as are one's fingerprints and blood type. The *Privacy Act*'s definition of personal information has two advantages: it creates a non-exhaustive list of what is considered personal information; and by including fingerprints and blood type it extends informational privacy into the realm of biometrics , which presumably would include genetic information. It does not however define biological samples as personal information.

A federal government institution may not collect personal information unless it relates directly to an operating program or activity of that institution. The institution must collect the information directly from the individual except where the individual permits otherwise or where the *Privacy Act* allows disclosure of personal information to the institution. Under section 8, the *Privacy Act* allows disclosure: for the purpose for which the information was compiled; for a use consistent with that purpose; for any purpose mandated by another act of parliament; for the purposes of law enforcement; for research or statistical purposes; for any purpose in which the public interest in disclosure outweighs the

---

[68] *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989) as cited by David Flaherty, "Controlling Surveillance: can Privacy Protection be Made Effective?" Available on the internet at http:// oipcbc.org/publications/presentations/surveil.htm.

[69] Section 3 of Bill C-6 "recognizes the right of privacy of individuals with respect to their personal information…".

privacy interest of the individual; and for any purpose where disclosure would clearly benefit the individual to whom the information relates.

Under the *Privacy Act*, a government institution must not use personal information under its control without the individual's consent, *except* to use it for the purpose for which the information was obtained, for a use consistent with that purpose or for a purpose for which the information may be disclosed to the institution. Similarly, no consent is required to disclose information to third parties if the information is disclosed for a consistent purpose. Consistent purpose is not defined. On a more positive note, a government institution must: ensure that the information it uses is as accurate and up-to-date as possible; that it retains the personal information it has used for such a time as to ensure that the individual to whom it relates may obtain access to it; and that it disposes of the personal information in accordance with the regulations made under the *Privacy Act*.

One of the tenets of fair information practices is transparency. In order to ensure transparency, all personal information that is used by a federal government body for an administrative purpose must be entered into a data bank and the institution is required to publish an index of its personal information banks at least once per year. The index must identify the purpose for which the information was obtained or compiled as well as the consistent purposes for which the information was used or disclosed. As mentioned, the *Privacy Act* enshrines the right of Canadian citizens and permanent residents to access their personal information either held in the data bank of a federal institution or under the control of the latter. Thus the publication of these indexes dovetails with access provisions of the *Privacy Act*, allowing individuals to identify where to access personal information that a public body may be holding.

The federal *Privacy Act* provides for an oversight mechanism. The *Privacy Act* creates the Office of the Privacy Commissioner and empowers the Privacy Commissioner to investigate and report on complaints filed under either the privacy or access provisions of the *Act*, to ensure compliance with sections 4 to 8 and to review exempt banks under section 36. Although the Commissioner has fairly extensive investigative powers, s/he does not have the power to render legally binding decisions in the form of orders. However, Bruce Phillips, the Privacy Commissioner of Canada and a strong advocate for the ombuds model, has noted that his office has a commitment to conflict resolution and that recourse to review by the Federal Court, as permitted pursuant to section 41 of the *Act*, has been extremely rare, less than a dozen cases in the 20,000 complaints his office has handled since 1983.[70]

---

[70] Privacy Commissioner (Canada), "The *Charter* - A Reasonable Expectation of Privacy", 1997-1998 Annual Report.

2. Provincial Public Sector Privacy Legislation

With the exception of Prince Edward Island all provinces and territories in Canada have some form of privacy and access to information legislation, although New Brunswick's *Protection of Personal Information Act* is not yet in force. These statutes are designed to make provincial public bodies more accountable to the public and to protect personal privacy by, to paraphrase the BC *Freedom of Information and Protection of Privacy Act ("BC FIPPA")*, giving individuals a right of access to, and a right to request correction of, personal information about themselves; specifying limited exceptions to the right to access; preventing the unauthorized collection, use and disclosure of personal information by public bodies; and providing for an independent review of decisions made under the statute.[71]

Because the privacy protection offered by most provincial privacy acts is substantially similar to that offered by their federal counterpart[72], what was said above with regard to the *Privacy Act* will not be restated. Rather emphasis will be placed on legislative schemes that are significantly different.

New Brunswick's *Protection of Personal Information Act* is a bare bones statute that, like Bill C-6, incorporates a statutory code of practice. Schedule A of the Act comprises the Statutory Code of Practice, and the Interpretation and Application of the Statutory Code of Practice is provided for in Schedule B. While the Statutory Code of Practice is based on the CSA Model Code, Schedule B is given far more summary treatment than the "Scope" provisions of the CSA Model Code. In some cases, this brevity promotes clarity and in other cases it dispenses with fundamental principles. For example, with regard to the principle of consent, Schedule B provides that the consent may be "express" or "implied". It defines implied consent, providing clarity, but it fails to define express consent, or to provide for either informed consent or a knowledge requirement. Similarly, while the Schedule B interpretation of consent laudably limits the situations in which disclosure may be made without consent, its language is not consistent with the consent principle itself in the Statutory Code. Principle 3: Consent states that "[t]he consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate." But is not clear whether the exceptions enumerated in Schedule B at subsection 3.4 are the only circumstances in which consent is inappropriate since the subsection simply lists those situations where "[c]onsent is not required…".

---

[71] Taken from section 2 of the BC *Freedom of Information and Protection of Privacy Act*, 1996, R.S.B.C., c. 165, which states the purpose of FIPPA.

[72] Note that this is a huge generalization, but a detailed analysis and comparison of the various provincial statutes is beyond the scope of this report.

Privacy protection for personal health information held in the public sector is broader in BC than other provinces because the BC FIPPA directly regulates health information in the public sector and it defines the public sector to include Regional Health Boards, Community Health Councils, local and metropolitan health boards, hospitals, mental health facilities, health authorities, student health centres, different health-related agencies, and the governing bodies of health professions such as pharmacists, dentists, nurses, physiotherapists and massage therapists. In the latter case, it is the professional organisations themselves that are bound by the legislation, and not the practitioners who are members of those organisations.

The BC FIPPA is also unique in that it defines "consistent purpose". Under section 34 of the BC FIPPA, a consistent purpose is one that has a reasonable and direct connection to that purpose and is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information. While it is arguably insufficient to ensure privacy in the absence of consent, it does invite a higher standard of oversight than in jurisdictions where consistent purpose is not defined.[73] In addition, that same section provides that the minister responsible for FIPPA must publish annually a list of the consistent purposes for which personal information is used or disclosed.

3. Provincial Statutes Governing Personal Health Information

Manitoba is the only jurisdiction in Canada to have legislation specifically dealing with the treatment of health information in both the public and the private sectors which is currently in force. Alberta's Bill 40, *Health Information Act*,[74] was assented to on December 9, 1999, and Saskatchewan's *Health Information Protection Act*[75] was assented to on April 28, 1999, but neither has been proclaimed in force. A common criticism of the health information initiatives of both Alberta and Manitoba is that that their primary objective is to facilitate information sharing through data linkages rather than to protect the privacy interests of those whom the system is designed to serve. [76]

Manitoba's *Personal Health Information Act* [77](the "Manitoba PHIA") was passed in 1997 in order to facilitate the Manitoba Health Information Network.[78] Although the Manitoba PHIA regulates private sector entities such as hospitals, nursing homes and laboratories, which are defined by the Act as "trustees", and prohibits

---

[73] For a more nuanced discussion of the issue in the healthcare context, see Putting Patients First, *supra* note 50 at 20-21.
[74] 3rd Session, 24th Legislature, December, 1999.
[75] Statutes of Saskatchewan, 1999, c. H-0.021.
[76] Marshall, *supra* note 33 at 15.
[77] S.M. 1997, C.C.S.M. c. P33.5.
[78] Manitoba "Privacy Protection of Health Information" (Discussion Paper) as cited by Duncan, *supra* note 36 at 25.

the sale of information by trustees, the powers extended to trustees to collect, use and disclose personal health information are broad. Specifically, the Manitoba Act creates five exceptions to the principle that personal health information should be collected directly from individuals, including when "time and circumstances"[79] do not permit direct collection, and the Act creates 24 exceptions to the requirement to obtain individuals' consent to disclose personal health information.[80] Moreover, as Drew Duncan points out, "there is doubt as to whether there can be sufficient enforcement of the privacy provisions, since the provincial Ombudsman, who has no binding order-making powers, serves as the oversight agency for the Act."[81]

Alberta's Bill 40, the *Health Information Act* (HIA), was designed to facilitate access to individual health information to support diagnostic, treatment and care decisions; to enable the increased use of information technology in the area of health for the benefit of Albertans; to improve the health management system and integrate the delivery of care; and to track fraud and abuse of the system. Bill 40 creates an information "arena" to which "custodians" of personal health information have access.

Some of the strong, privacy-enhancing points of the Alberta health information regime are that consent is required to disclose identifying diagnostic or treatment information by electronic means; it provides for the tracking of certain disclosures; researchers will only have access to personal health information with the consent of an ethics committee; it creates a hierarchy of information use, favouring the highest degree of anonymity possible in the circumstances; and it explicitly prohibits data matching between custodians or between a custodian and a non-custodian in the absence of approval from the Privacy Commissioner. Some of the difficulties with the HIA in terms of broad-based privacy rights are that it overrides *Alberta's Freedom of Information and Protection of Privacy Act* and provides less privacy protection than the latter; consent is not required for the collection, use and disclosure of personal health information in many situations; the controls on access to the health information arena lack rigor; and the creation of an arena of information is in and of itself problematic unless access to *identifiable* information is restricted to a select few.[82]

The Alberta Office of the Information and Privacy Commissioner's response to Bill 40 was cautious. Although the Office did not oppose Bill 40, as it has done in the past with respect to previous health information bills, its response emphasised that Bill 40 does *not* legislate privacy protection and that it will allow for *greater* access

---

[79] *Health Information Protection Act*, S.A. 1999, c. H-4.8 (awaiting proclamation), section 14(2).
[80] Duncan, *supra* note 42 at 23-24.
[81] *Ibid*. at 24.
[82] For a more detailed analysis of these provisions see Office of the Information and Privacy Commissioner (Alberta), "Response to Bill 40, *The Health Information Act*", November 22, 1999. Available on the internet at www.oipc.ab.ca.

to personal health information than is currently possible under the province's public sector privacy legislation. The Commissioner's Office alerted Albertans that it was up to them to decide whether they accepted the government's justifications for curtailing privacy protection for personal health information.[83]

Saskatchewan's *Health Information Protection Act* (HIPA), on the other hand, is premised on protecting the rights of the individual rather than on data sharing. As Saskatchewan Health has said:

> The basic goal of the legislation is to protect privacy of personal health information, while at the same time ensuring that information is available as needed to provide services and to monitor, evaluate and improve the health system in Saskatchewan for the benefit of individuals and the province.[84]

HIPA's principles are based on those of the CSA Model Code and the CMA's Code, amongst others. Some of the principles enshrined by HIPA are the right to consent to the collection, use and disclosure of one's personal health information; to revoke such consent; to be informed when a trustee has entered into an agreement with the Saskatchewan Health Information Network (SHIN) for the purpose of storing and making available personal health information; to prevent information from being stored on the SHIN; and to not have consent implied unless use or disclosure are directly related to the principle purpose for which the information was collected. HIPA establishes a health information system managed by health information "trustees" who may only disclose information on a "need to know basis" and whose actions are subject to review by the Saskatchewan Privacy Commissioner. These reviews are subject to appeal. Interestingly, HIPA creates significant fines for prohibited use or disclosure of personal health information: up to $50,000 in the case of an individual and up to $500,000 in the case of a corporation.[85]

Quebec has far outstripped other Canadian jurisdictions in the steps it has taken to protect personal information. Although it does not have legislation specifically governing personal health information, it is the only jurisdiction in North America to have a legislated data protection regime for both the public and private sectors.[86]

---

[83] *Ibid*.

[84] See also Duane Mombourquette, "Overview of the *Health Information Protection Act*" (Saskatchewan Health, July, 1999).

[85] By way of comparison, see Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*, *supra* note, which provides for much less substantial fines: under s. 91 of the *Act* a person who fails to comply with the *Act* may be fined from $1000 to 10,000 for a first offence and from $10,000 to 20,000 for a second.

[86] Parliamentary Research Branch, Law and Government Division, *Legislative History of Bill C-6*, by John Craig (Ottawa: Library of Parliament, 1999) at 5 (pagination as downloaded from the internet).

While the *Act Respecting the Protection of Personal Information in the Private Sector* only applies to the collection, use and disclosure of personal information in the course of carrying on an enterprise, both the *Civil Code of Quebec* [87] and the *Quebec Charter of Human Rights and Freedoms*[88] enshrine the right to privacy. In addition, provisions relating to the confidentiality of health records are found in the *Act Respecting Health Services and Social Services*. These laws, as well as specific regulations that apply to health records, create guidelines and provide for training for health professionals and archivists of medical records, mean that Quebec provides comprehensive protection for personal health information held in both the public and private sectors.

Although Ontario has held public consultations on health information legislation and released a draft Personal Health Information Protection Act in 1997, a bill was never introduced in the legislature.

V. PRIVATE SECTOR & COMMON LAW PROTECTION OF PERSONAL INFORMATION[89]

With the exception of the provinces that have passed laws aimed specifically at health information, the only jurisdiction in Canada to have private sector information access and privacy legislation is Quebec. However, on December 9, 1999, an amended version of federal Bill C-6 passed third reading in the Senate and it was returned to the House of Commons for review.[90] Bill C-6 notwithstanding – since it would only apply to health information captured by commercial transactions under federal jurisdiction (see below) - the virtual absence of privacy-specific private sector legislation does not mean Canadians' personal health information has been completely without protection in the private sector. Provincial health sector statutes provide for confidentiality and/or privacy. Professional codes of ethics or conduct have been adopted under the authority of the statutes governing professions' professional bodies. And voluntary codes of conduct have been adopted by such healthcare organizations as the Canadian Medical Association and by health industry organizations such as CIHI.[91] Also, the

---

[87] C.C.Q., Art. 35-41; under s. 37 of the Civil Code of Quebec, no person may establish a file on another person without a serious and legitimate reason for doing so. Note that the privacy provisions of the Civil Code include the right of access and correction of personal information regardless of who is in possession of the information.

[88] R.S.Q., c. C-12, s. 5.

[89] Due to limitations of space and time, examples for this section are drawn almost exclusively from B.C.

[90] See below for discussion of Bill C-6.

[91] Although CIHI's privacy code "Privacy and Confidentiality of Health Information at CIHI: Principles and policies for the protection of health information" is based on the CSA Model Code, its provisions with

Canadian Standards Association's Model Code has received some acceptance in the private sector. In this section we will present an overview of these various and varied forms of private sector privacy protection, including Bill C-6.

1. Hospitals

As mentioned above, in BC the information in hospital records is subject to the access, collection, use and disclosure provisions of the BC FIPPA. Under section 51 of the BC *Hospital Act*[92], the records prepared in the hospital by a physician, a dentist or an employee of the hospital remain the property of the hospital. We have seen that this formulation of ownership is consistent with that of the Supreme Court of Canada in *McInerney* and does not interfere with the patient's right of access to the information contained in the record. Even when the hospital contracts with a private company to maintain its healthcare records, the records are subject to FIPPA's privacy and access provisions because, under section 3 the records remain under the "control" of the hospital.

2. Physicians

In BC, the statute that establishes the governing bodies for some healthcare professionals such as physicians, pharmacists, psychologists, chiropractors and dentists, imposes a duty on the governing bodies to require their members to provide clients with access to their health records and to inform their patients of their rights under BC FIPPA.[93] As indicated above, the common law also provides a legal basis for individuals' access to their personal health records, whether they are held in the public or the private sector.[94]

While provincial privacy laws do not apply to client health records held by private physicians' offices, confidentiality obligations are contained in various privacy codes governing the health professions. Breach of professional duty of confidentiality is generally categorized as professional misconduct and complaints can be brought before the disciplinary arm of the relevant professional body or a civil action in negligence brought before the courts.

With regard to confidentiality, under section 52 of the BC *Health Professions Act*, health professionals may only disclose information obtained for the purposes of carrying out their duties under that *Act*, the regulations or the by-laws or if required by law. Section 1 of the *Health Professions Act* explicitly limits the

---

respect to consent to collection, use and disclosure of personal health information all admit exception where "permitted by law." Thus it will not receive any specific attention in this paper.

[92] R.S.B.C. 1996, c. 200.

[93] *Health Professions Act,* R.S.B.C. 1996, c. 183.

[94] *McInerney*, *supra* note 2 at 145-155.

disclosure of information obtained by the "health profession", defined as a profession in which a person exercises skill or judgment or provides a service related to the preservation or improvement of the health of individuals, or the treatment or care of individuals who are injured, sick, disabled or infirm. However, it says nothing about the collection or use of personal health information.

In addition to professional sanctions, breach of the common law duty of confidentiality can give rise to civil liability based on breach of contract, negligence, defamation or an action for breach of confidence.[95] In *McInerney*, the Supreme Court of Canada decision that established patients' right of access to medical records containing their health information, Mister Justice La Forest characterized the physician-patient relationship as fiduciary "for some purposes". Further, he said:

> …certain duties do arise from the special relationship of trust and confidence between a doctor and patient. Among these are the duty of the doctor to act with utmost good faith and loyalty, and to hold information received from or about a patient in confidence.[96]

Mister Justice La Forest then went on to discuss judicial support for characterizing the duty of confidentiality as contractual. Although he found some support for this view, he concluded that it was "unnecessary to reify the patient's interest in his or her medical records" concluding that fiduciary duty is "sufficient to protect the interest of the patient."[97]

That the Canadian Medical Association and Canadian Dental Association have come out strongly in favour of more stringent privacy protection than Bill C-6 currently provides is completely consistent with doctors' duty of confidentiality. Indeed physicians' duty of confidentiality, built on an ethical/legal foundation as old as the Hippocratic Oath, is virtually absolute. Physicians are bound by a duty of confidentiality both by the common law and by their professional codes of conduct.

Under the BC *Pharmacists, Pharmacy Operations and Drug Scheduling Act*, pharmacists must "collect, retain, maintain, correct, protect, use and disclose patient record information for specific purposes provided for in the by-laws."[98] They must not disclose information, files or records obtained under the Act except to carry out a duty under the *Act* or by-laws; or to comply with the law; or to

---

[95] Manes & Silver, *supra* note 66 at 19.
[96] *McInerney*, *supra* note 2 at 149.
[97] *Ibid*. at 152.
[98] R.S.B.C. 1996, c. 363, s. 35(3).

comply with a request by a patient, another pharmacist, a government payment agency, the college of pharmacists, the minister or a regulatory body of a practitioner for specific reasons detailed in section 39 of the *Act*. This same section states explicitly that no information can be disclosed for market research.

Finally, as indicated above, one of the exceptions to a physician's duty of confidentiality is where statutory or common law rule provides that patient information must be disclosed to the courts. Under the common law, some highly confidential information, such as solicitor-client communications, is subject to "privilege", a doctrine that refers to a right to withhold information from a court. But doctor-patient communications and records are not protected by the doctrine of privilege in the common law system. Thus doctors have an ethical duty of confidentiality, but before the courts, it can be overridden by a public interest in avoiding a miscarriage of justice. Under the Quebec civil law system, however, doctor-patient communications *are* protected by the doctrine of privilege. Section 308 of the *Quebec Code of Civil Procedure*[99] states that physicians and dentists cannot be obliged to divulge what has been revealed to them in confidence by reason of their status or profession.

3. Medical Benefits

The regulations of the *BC Medicare Protection Act*[100] provide for information sharing necessary for the administration of healthcare and medical benefits in BC. Information may be shared between agencies and bodies created under the *BC Benefits (Income Assistance) Act*, the *Insurance Corporation Act*, the *Insurance (Motor Vehicle) Act* and the *Workers Compensation Act*. However, section 49 of the *Medicare Protection Act* states that current or former members of the commission, employees, inspectors and any other person engaged or previously engaged in the administration of the *Act* must keep confidential matters that identify an individual beneficiary or practitioner that come to his or her knowledge in the course of their employment or duties.

4. Employment Records

Under provincial labour standards legislation, private sector employers are required to keep employment records. These records may contain health information due to occupational or other statutory requirements. However, no fair information practices apply to the collection, use and disclosure of that information. Under section 4(1), Bill C-6 applies to personal information about an employee "that the organization collects, uses and discloses in connection with the

---

[99] R.S.Q., c. 25.
[100] R.S.B.C. 1996, c. 286.

operation of a federal work, undertaking or business." The words "in connection with the operation of" are ambiguous and raise concerns about the scope of the privacy protection afforded by Bill C-6 to the employment records of federal private sector employees.

Neither Bill C-6, nor public sector privacy laws cover prospective employees, but in light of both the competitiveness of the job market and the American drug-testing trend, the personal health information of prospective private sector employees ought to be covered by privacy laws and employers' information practices should be subject to the same oversight mechanisms.[101]

5. The Federally Regulated Private Sector: Bill C-6

Bill C-6 (initially Bill C-54), the *Personal Information Protection and Electronic Documents Act*, is designed to regulate privacy in the federal private sector with respect to commercial transactions. Bill C-6 also purports to regulate the same transactions under provincial jurisdiction 3 years after it has come into force if the provinces do not themselves pass "substantially similar" legislation. From the perspective of commerce, the Bill came as a response to public concerns about privacy in the private sector in general, and on the internet in particular. From the perspective of data protection and the trans-border flow of data, Bill C-6 is a response to the *European Directive on Data Protection*. Article 24 of the *European Directive* prohibits member countries from transferring personal information to a non-member country or to a business located in a non-member country where the laws of the non-member country do not provide privacy protection at least equivalent to that provided by the OECD Guidelines, which are incorporated into the *European Directive*.[102]

The privacy protection provided for by Part 1 of Bill C-6 only extends to the collection, use and disclosure of personal information "in the course of commercial activities" in the private sector. The extent to which the Bill would apply to personal health information in the records of hospitals, physicians, long-term care facilities, public health units, home care agencies, or pharmacies is uncertain. Because commercial activity is defined in terms of the *conduct* of an organization rather than the *nature* of the organization, personal health information would be protected in some circumstances and not others within any given organization, depending on the nature of the activity performed. Similarly, the words "in the course of" are themselves imprecise, thus the scope of commercial activities

---

[101] Murray Mollard, "Submission of the B.C. Civil Liberties Association to the B.C. Committee on Information Privacy in the Private Sector", at 4.

[102] Parliamentary Research Branch, *Legislative History of Bill C-6* by John Craig (Ottawa: Library of Parliament, 1999).

covered is uncertain.[103] Bill C-6, as it is currently drafted would, of course, pose the same problems in the provincial private sector. In fact the difficulties would be even greater given that most health information is held by entities under provincial jurisdiction and the public and private sectors are quite intertwined where the delivery of healthcare is concerned.

Bill C-6 breaks new ground in the realm of Canadian privacy legislation: the Bill incorporates the CSA Model Code of fair information practices, which itself provides for more rigorous privacy standards than the *OECD* Guidelines and Bill C-6 is arguably more rigorous than all the federal and provincial public sector privacy statutes with the exception of Quebec and possibly British Columbia. The business community, which was widely consulted in the five years of intense negotiations taken to develop the CSA Model Code and in the period of consultations leading up to the introduction of Bill C-6, is largely in support of Bill C-6, but the health sector, in hearings before the Standing Senate Committee on Social Affairs, Science and Technology (the "Senate Committee") almost unanimously opposed Bill C-6 in its present form.[104]

However, the health sector is deeply divided on its *reasons* for opposing the Bill. Some groups, such as the Canadian Healthcare Association, representing individual healthcare facilities and agencies, and the Ontario Association of Medical Laboratories opposed the Bill on the grounds that Bill C-6 may constrain effective measurement of outcomes and quality of healthcare delivery. And, the Ontario government vociferously opposed the Bill. Other groups, such as the Canadian Medical Association and Canadian Dental Association, claim that the CSA Model Code, which was developed without input from primary healthcare providers, would not adequately protect individual Canadians from misuse of their personal health information.[105]

In response to health sector opposition, the Senate passed an amendment to Bill C-6, which has the effect of excluding the health sector from the application of the Act for 2 years after it is proclaimed. According to Senator Michael Kirby, who chaired the Senate Committee, this should allow the members of the health sector sufficient time to participate in the development of appropriate legislation while motivating the stakeholders and governments to move quickly to formulate a solution that is appropriate for the protection of personal health information.[106]

---

[103] The Ontario Minister of Health and the CMA have raised serious concerns about what health information is covered by Bill C-6.
[104] Parliament, 2nd Report of the Standing Senate Committee on Social Affairs, Science and Technology, Sessional Paper, No. 2/36-183S (6 December 1999).
[105] *Ibid*.
[106] *Ibid*.

Those who argued that Bill C-6 does not provide sufficient privacy protection for personal health information raised the following objections: the Canadian Dental Association objected to Bill C-6 on the basis that it does not require "informed consent" with respect to the collection, use and disclosure of personal health information and that that unless Bill C-6 were amended to provide stronger protection to health information, the provinces might well fail to adopt appropriate protections. The Canadian Medical Association and the College of Family Physicians of Canada maintained that health information requires stronger privacy protection than other types of information since health records are "highly private, sensitive and vulnerable to abuse by secondary and tertiary users."[107] Among those who advocated on behalf of passing the Bill were the federal privacy commissioner and privacy expert Valerie Steeves. They feel that legislation that "articulates broad statements of principles" is needed, and that adoption of the Bill would not prevent the provinces from exercising their jurisdiction to adopt more stringent legislation.

In May 1998, the New Brunswick government issued a discussion paper on privacy in the private sector,[108] but no bill has been introduced as yet. As mentioned, the CSA Model Code is already the basis of New Brunswick's recently enacted *Protection of Personal Information Act*. The discussion paper proposes that the content of private sector legislation be based on the CSA Model Code. But unlike Bill C-6, the discussion paper starts from the premise that the scope of privacy protection should be broad; that it could apply to all commercial or non-commercial organizations, including individuals when they collect and use personal information for commercial or other non-domestic purposes.

VI. THE CONSTITUTIONALLY PROTECTED RIGHT TO PRIVACY: SECTIONS 7, 8 & 15 OF THE CHARTER

In a number of cases dating as far back as 1928, the Supreme Court of Canada has delineated a common law right to privacy as between individuals and between individuals and the state. In the time since the enactment of the *Charter* in 1982, the Supreme Court has accorded privacy constitutional protection as a fundamental human right, despite the lack of an explicitly entrenched right to privacy in the *Charter*. However, the scope of the constitutional right of privacy, like the scope of every right enshrined in the *Charter*, will only be unveiled as courts are faced with factual situations that take them beyond the facts on which they have hitherto based their findings. Thus it is impossible to say, for example, whether and in what circumstances individuals' right to privacy are infringed by disclosure of personal health information to third parties without their consent. Facts that might

---

[107] *Ibid*. at 4.

[108] Available on the internet at http://inter.gov.nb.ca/legis/comite/priv-ii/index.htm.

bear out such a finding have simply not been before the courts. Nonetheless, the Supreme Court has established some important principles and the ambit of the constitutionally protected right to privacy is widening. This section explores the scope of the *Charter* right to privacy and the significance of such a constitutionally protected right, beginning with the latter.

1. Legal Rights versus *Charter* Rights

The statutory privacy rights discussed in the first and second sections of this paper are legal rights to privacy, that is rights that are protected by common and civil law rules and by federal and provincial statutes. Whereas legal rights are always vulnerable to encroachment by subsequent statutory enactments, no law or rule may derogate from constitutional rights, except in two circumstances (see below). Section 52(1) of the Canadian *Constitution Act, 1982* provides that the Constitution of Canada is the supreme law of Canada and that "any law that is inconsistent with the provisions of the Constitution is, to the extent of the inconsistency, of no force or effect."[109] However, the *Charter* entrenches two limiting principles.

First, with regard to rights protected under sections 7 through 14 of the *Charter*, section 7 provides that "everyone has the right to life, liberty and security of the person and the right not to be deprived thereof *except in accordance with the principles of fundamental justice*." [Emphasis added]. Put another way, a law will be found to be constitutional even if it deprives a person of life, liberty, or security of the person, if it conforms to the principles of fundamental justice (the fundamental precepts that underlie Canada's justice system). This rule is extremely important for the purposes of the present discussion because recently, in the *Mills* case, the Supreme Court found that when two different individual rights, both or which are protected by section 7, come into conflict, there is no hierarchy of those rights. Rather, the court must ask what is required by the principles of fundamental justice in that particular context and seek to balance those rights in a manner that respects both sets of rights.[110] Thus, in *Mills*, the Supreme Court found that the complainant's right to privacy was not trumped by the accused's right to full answer and defence. This balancing process goes some way to delineating the right to privacy in light of other competing human rights.

Secondly, section 1 of the *Charter* provides as follows:

> The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

---

[109] *Constitution Act*, *1982*, being Schedule B to the *Canada Act*, *1982* (U.K.), 1982, c.11.
[110] *Mills*, *supra* note 3 at 19 and 39.

Where a Court has decided that a law is unconstitutional, it must engage in this second test under section 1 in order to decide whether the law has struck an appropriate balance between the fundamental human rights guaranteed by the *Charter* and the "competing social or economic objectives pursued by the law."[111] At issue under section 7, is the delineation of the boundaries of the - sometimes competing - rights in question, whereas under section 1, the question is whether the violation of these boundaries may be justified in a free and democratic society. The Supreme Court has elaborated a detailed test that courts must apply to determine whether the law in question is justifiable in a free and democratic society.

First, the law must have a sufficiently important objective, that is related to state concerns that are "pressing and substantial."[112] As the Supreme Court stated in the *Singh* case, "certainly the guarantees of the *Charter* would be illusory if they could be ignored because it was *administratively convenient* to do so." [Emphasis added.] Most importantly, the law must achieve its objective by infringing the right or freedom in question *as little as is reasonably possible*.[113] As Peter Hogg has written, "this step of the analysis has turned out to be the heart and soul of section 1 justification."[114]

The significance of section 1 for the constitutionality of privacy legislation is manifest. However, it is here, where the courts must balance the interests of the state against the fundamental rights of the individual, that the limitations on the right to privacy are as yet uncharted by the Supreme Court.

2. The Right to Privacy Pursuant to the *Charter*

The function of the *Charter*, according to then Chief Justice Dickson, in *Hunter* v. *Southam*, "is to provide … for the unremitting protection of individual rights and liberties."[115] Privacy, grounded in individual moral and physical autonomy, is fundamental to *Charter* values of dignity and autonomy of the individual.[116] Section 7 of the *Charter* provides that "everyone has the right to life, liberty and security of the person…" Privacy, the Supreme Court has said, is at the heart of liberty in a modern state, and the limits the *Charter* imposes on government to pry into the lives of its citizens go to the essence of a democratic state.[117]

---

[111] Peter Hogg, *Constitutional Law of Canada*, Loose-leaf Edition, Vol. 2 (Scarborough: Carswell, 1997) at 33-10.
[112] *R.* v. *Oaks*, [1986] 1 S.C.R. 103 at 138-139.
[113] *R.* v. *Edwards Books*, [1986] 2 S.C.R. 713 at 772.
[114] Hogg, *supra* note 111 at 35-32.
[115] *Hunter* v. *Southam*, [1984] 2 S.C.R. 145 at 160.
[116] *R.* v. *Osolin* (1994), 109 D.L.R (4th) 478 [hereinafter *Osolin*].
[117] *Dyment*, *supra* note 16 at 513.

Initially, the *Charter* right to privacy was developed under s. 8 of the *Charter* which provides that "everyone has the right to be secure against unreasonable search and seizure." Section 8 protects citizens against "unreasonable" search and seizure by government, that is searches that infringe citizens' right to a reasonable expectation of privacy. The Supreme Court held that the essence of balancing state needs against the privacy rights of individuals lies in assessing the "reasonable expectation of privacy" of the individual concerned. What is reasonable will depend on circumstances such as the *nature of the interest* sought to be protected and the deleterious effects flowing from its breach.[118] Accordingly, the more sensitive the information, the higher the expectation of privacy.

The right to privacy with respect to documents and records was addressed by the Supreme Court in *R.* v. *Plant* as follows:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* seek to protect a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[119] [Emphasis added.]

In the *O'Connor* case the Supreme Court confirmed that s. 7 of the *Charter* includes the right to privacy. In that case, the accused sought disclosure of the complainant's therapeutic records. Madame Justice L'Heureux-Dubé, for the majority in that case, held that pursuant to s. 7 of the *Charter*, witnesses have a right to privacy in relation to private documents and records.[120] Citing Madame Justice Wilson's decision in the 1988 *Morgentaler* case, she stated that s. 7 guarantees of liberty and security of the person are "tied inextricably to the concept of human dignity" and must be interpreted broadly to ensure individuals' personal autonomy over important decisions intimately affecting their lives.[121] Failure to respect individual privacy, she stressed "undeniably impinges upon an individual's 'liberty' in our free and democratic society."[122]

In *O'Connor*, Madame Justice L'Heureux-Dubé declined to decide whether the above definition, taken from *Plant*, was exhaustive of the right to privacy in respect of all manner of documents and records. Nonetheless, she was convinced that a complainant's therapeutic records did indeed fit within the rubric of a biographical

---

[118] *Ibid*. at 159.
[119] *R.* v. *Plant*,[1993] S.C.J. No. 97 (Q.L.), para. 19 [hereinafter *Plant*].
[120] *O'Connor*, *supra* note 29 at 294.
[121] *R.* v. *Morgentaler*, [1988] 1 S.C.R. 30, as cited in *O'Connor*, *ibid*. at 287.
[122] *O'Connor*, *supra* note 29 at 287.

core of personal information. In *R.* v. *Osolin*,[123] Madame Justice L'Heureux-Dubé confirmed that:

> …the interest in the privacy of medical records was recognized in the [*Dyment*] case as a broad and independent value, separate and distinct from considerations about the fairness of the trial process. Thus the privacy interest discussed in *Dyment* may be seen as an interest that pertains to all of us, which may arise in a number of different circumstances. Indeed, it would be odd if the protection of medical records were to be available only to those accused of criminal offences.[124]

In both the *O'Connor* and the *Mills* cases, the Supreme Court found that a court order to produce records, in this case therapeutic records, made under the *Criminal Code* is a "seizure" within the meaning of section 8 of the *Charter*. In *Mills*, the Court upheld an amendment to the *Criminal Code*[125] which provides that to order production of a medical, therapeutic, counselling or other record in which the person concerned has a reasonable expectation of privacy, a court must be satisfied that the record is "necessary in the interests of justice." This is an important finding as it sets a high standard for what the Supreme Court considers to be a "reasonable" infringement of individuals' constitutionally protected right to privacy of their therapeutic records.

Regarding control over one's personal information, Mister Justice La Forest stated in *Dyment* that while

> [w]e may, for one reason or another, wish or be compelled to reveal such information… situations abound where the reasonable expectations of the individual that the information shall remain *confidential to the persons to whom, and restricted to the purposes for which it is divulged*, must be protected. [126] [Emphasis added.]

Whereas in the past the Supreme Court had most often characterized the philosophical and legal underpinnings of privacy in terms of the right to liberty, in *Mills*,[127] the Supreme Court further broadened the scope of fundamental values the right to privacy protects. In *Mills* Madame Justice McLachlin considered the right to security of the person under section 7 of the *Charter*. At issue was whether amendments to the *Criminal Code* that recognize complainants' and witnesses' right to privacy of their therapeutic records were unconstitutional because they infringe

---

[123] *Osolin*, *supra* note 116 at 490.
[124] *Ibid*. at 491.
[125] *Criminal Code*, R.S.C. 1985, c. C-46, s. 278.5(1)(c).
[126] *Dyment*, *supra* note 18 at 515.
[127] *Mills*, *supra* note 3.

defendants' rights to make full answer and defence. She found that the therapeutic relationship is fundamentally founded on trust. The therapeutic relationship is "characterized by confidentiality, an element of which is trust."[128] She concluded that the protection of a complainant's reasonable expectation of privacy in his or her therapeutic records protects the therapeutic relationship and that unless the confidential nature of that relationship is protected, an individual's trust may be shattered and the security of his or her person undermined.

Mills confirmed an earlier decision handed down by the Supreme Court in 1999 in which a mother claimed that the Province of New Brunswick must provide her with legal aid in order to challenge state apprehension of her children, a majority of the Supreme Court affirmed that the right to security of the person protects "both the physical and psychological integrity of the individual." [129] Recognition by the Supreme Court that confidentiality is essential to trust in the therapeutic context and that breach of confidentiality may compromise the mental security of the patient are vital components of the constitutionally protected right to privacy of personal health information.

Another relevant facet of constitutionally protected privacy rights is that they must be protected from the outset. As Madame Justice L'Heureux-Dubé said in *O'Connor*, "The essence of privacy … is that once invaded, it can seldom be regained."[130] She quoted Mister Justice La Forest's findings in the *Dyment* case with approval:

> …if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only *after* it has been violated.… Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be *clear rules setting forth the conditions in which it can be violated.*[131] [Emphasis added.]

With regard to information that is stored electronically, Madame Justice McLachlin found that computers should be private places "where the information they contain is subject to the legal protection arising from a reasonable expectation of privacy."[132] In this case, police had received a tip that the accused was growing marihuana. They gained access to a terminal linked to the electrical utility's computer that allowed them to check electrical consumption at a specified address, confirming that the energy consumption was extremely high. Whereas the majority found that one's electricity record does not reveal intimate details of one's

---

[128] *Ibid*. at 47.
[129] *New Brunswick (Minister of Health and Community Services)* v. *G. (J.) [J.G.]* (1999), 177 D.L.R. (4th) 127 at 146.
[130] *O'Connor*, *supra* note 29 at 290.
[131] *Ibid*.
[132] *Plant*, *supra* note 119, para. 44.

life, and thus give rise to a reasonable expectation of privacy, Madame Justice McLachlin, dissenting, found that in each case, the question that must be asked is whether the evidence discloses a "reasonable expectation that the information will be kept in confidence and *restricted to the purpose for which it is given*."[133] [Emphasis added.]

Finally, the *Charter* guarantees of equality are relevant to the issue of privacy protection. In the *Osolin*[134], *O'Connor*[135] and *Mills* cases, the Supreme Court recognized that a failure to govern disclosure of the therapy records of victims of sexual offences with the same rigorous rules of disclosure by which other confidential records are governed would infringe the victim's equality rights. Moreover, in *Mills*, Madame Justice L'Heureux-Dubé stated the following:

> When the boundary between privacy and full answer and defence is not properly delineated, the equality of individuals whose lives are heavily documented is also affected, as these individuals have more records that will be subject to wrongful scrutiny."[136]

This equality argument against disclosure was raised by Mary A. Marshall and Teresa L. Meadows, counsel for the Appellant/Complainant.[137] That the Supreme Court accepted this argument further broadens and entrenches the right to privacy and could have far-reaching implications for legislation that permits data matching and disclosure of personal health information in the absence of consent.

In conclusion, it is apparent that a constitutionally protected right to privacy is not monolithic, nor is it absolute. Rather privacy may aptly be described as a bundle of rights that are integral to human dignity and autonomy, two of the fundamental values on which the *Charter* guarantees of liberty, security and equality are built. By making *Charter* protection of privacy contingent on a "reasonable expectation of privacy", the Supreme Court has created a sliding scale of privacy protection that recognizes that the more sensitive the information, the more compelling is the reasonable expectation of privacy. Significantly, in the *McInerney*, *Osolin*, *O'Connor* and *Mills* cases, the Supreme Court has consistently emphasized the highly private nature of medical records.

To date, the Supreme Court has not dealt specifically with the notion of consent as it relates to individuals' right to privacy. However, the Supreme Court has recognized time and again that the very notion of privacy is grounded in

---

[133] *Ibid*., para. 40.
[134] *Osolin*, *supra* note 116 at 496.
[135] *O'Connor*, *supra* note 29 at 291.
[136] *Supra* note 3 at 51.
[137] Appellant's Factum in *R*. v. *Mills* (Supreme Court of Canada) at paragraphs 98-101.

individuals' physical and moral autonomy[138] and liberty. Thus one retains the right to control one's personal information to the extent that that right is not limited by either section 7 or 8 of the *Charter*. That this right to control or not divulge personal information is equivalent to consent is demonstrated by Madame Justice McLachlin's statements in *Mills* wherein she held that privacy, the interest in being left alone by the state, "includes the ability to control the dissemination of confidential information. She cites Mister Justice La Forest with approval:

> …it has long been recognized that this freedom not to be compelled to share our confidences with others is the very hallmark of a free and democratic society. Yates J., in *Millar* v. *Taylor*(1769), states,
>
> > It is certain every man has a right to keep his own sentiments, if he pleases: he has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends.
>
> These privacy concerns are the strongest where aspects of one's individual identity are at stake…[139][Citations omitted.]

VII. CONCLUSION

This fragmented and cursory overview rather mirrors the state of Canada's provincial and federal privacy legislation as it applies to personal health information. It seems clear that, with the exception of Quebec, none of the general privacy acts adequately addresses the privacy rights of individuals with regard to their personal health information. On the other hand, the development of Bill C-6 through extensive community consultation and consensus-building demonstrates that it is possible to develop privacy legislation where indeed privacy is understood to be the goal and not merely a hurdle. Lawmakers contemplating law reform with regard to the privacy treatment of personal health information will be forced to reconcile many divergent sources of privacy law and privacy policy analysis, not to mention the divergent interests of those who are directly involved with the administration of Canada's healthcare system, those who provide healthcare, those who have the most to gain financially by unbridled access to personal health information and, most importantly, those for whom the privacy of their personal information is at stake.

Confidentiality and informed consent form the backbone of the medical system. As Bruce Phillips, the federal Privacy Commissioner, argued in his 1996-97 Annual Report, "an individual's right to control the disclosure of personal medical

---

[138] *Dyment*, *supra* note 18 at 427.
[139] *R.* v. *Duart*, [1990] 1 S.C.R. 30, as cited in *Mills*, *supra* note 3, para. 80.

information should be paramount. That right should be overruled only in the face of an *overwhelming and compelling public interest* (or to provide the patient emergency care)." [Emphasis added.] If the federal and provincial governments fail to pass legislation which protects individuals' rights to privacy, it will be up to the courts to decide under what circumstances individuals have a right to a reasonable expectation of privacy and whether legislation that permits either use or disclosure to third parties without consent passes constitutional muster.