Personal Medical Information: Privacy or Personal Data Protection? A Theoretical Approach to Understanding the Canadian Environment

Wilhelm Peekhaus†

> All that may come to my knowledge in the exercise of my profession or outside my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.
>
> – Hippocratic Oath, circa 4th century B.C.

Introduction

The Hippocratic Oath, which at some level is probably familiar to a large portion of the population, actually articulates a tension in contemporary society between the call for privacy rights and claims that access to medical data is necessary for the benefit of all of society. The former is a position espoused by libertarians and the latter is championed by communitarians. The libertarian applauds the Oath's insistence that the medical practitioner keep secrets; the communitarian supports the notion, present in the Oath, that there is information that ought to be spread about. This tension mirrors the inevitable discordance between privacy (understood in the context of the Oath as secrets relating to an individual) and access (to the information that ought to be spread abroad) that continues to be reflected in contemporary policy discussions about the privacy of personal information.

Some of the existing literature concerning the privacy of health information seems to suggest that medical information has a particularly special nature; either through its oft-cited association with dignity or the need for its "unobstructed" use by health care practitioners for a variety of reasons.[1] It is against such a backdrop that this paper will review and compare a number of legislative mechanisms that have been designed to meet the challenge of safeguarding the privacy of personal information without completely hindering the continued flow of information required by economic and health care systems. An attempt will be made to situate the Canadian legal environment in respect of privacy legislation within a suitable theoretical framework: Elizabeth Neill's model of privacy. Aside from providing the necessary conceptual framework for the paper that will help delineate between privacy and personal data protection, Neill's model will be adapted to develop a privacy–personal data protection continuum, on which the various legislative devices will be positioned. The analysis of the various statutory mechanisms will be limited to a descriptive discussion designed to conceptualize the degree to which contemporary legislation is more aptly construed as protective of privacy or personal data. Though some attention will be devoted to discussing the analytic advantages of Neill's model in responding to such a query, a normative assessment of her model or the various acts is beyond the scope of this paper. The research questions driving this paper include the following three:

(i) Considering Neill's ontology of privacy rights, are the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[2] and the European Union *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*[3] best characterized as protective of privacy or personal data?

(ii) Do the various provincial health information protection Acts go beyond the *Personal Information and Protection of Electronic Documents Act*[4] such that health information protection might better be considered more about privacy than personal data protection?

(iii) Which are aligned with Neill's model?

In order to respond to these questions, the first part of the essay will be devoted to explicating Neill's ontology of privacy. The paper will then consider the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the European

†Doctoral Candidate in the Faculty of Information and Media Studies, at the University of Western Ontario. The author would like to thank Dr. Margaret Ann Wilkinson, from the University of Western Ontario, for her valuable and constructive comments on an earlier draft of this paper. Thanks are also due to the anonymous reviewers who offered helpful suggestions for improving the manuscript.

Union *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* in order to assess whether they protect privacy or personal data. The next section will engage in a comparative examination of the Canadian federal *Personal Information and Protection of Electronic Documents Act* and the four provincial health information protection Acts (Alberta, Saskatchewan, Manitoba, and Ontario). Based upon this comparison, attention will then turn toward an assessment of whether the various statutes are concerned more with privacy or personal data protection, and where they fit in the privacy debate based on Neill's model.

Theoretical Model of Privacy

Before examining the extent of legislative protection afforded to personal health information in Canada, consideration must first turn toward the explication of a theoretical model capable of coherently defending claims to privacy. In *Rites of Privacy and the Privacy Trade*, Elizabeth Neill sets herself the task of developing a theoretical basis for the justification of privacy in the context of our technologically advanced society. At the core of her theory is the question of the ontological status of human dignity in relation to privacy, which permits her to delimit the boundaries of legitimate privacy interests and rights. As she correctly points out, much of the literature has been unable to determine definitively whether human dignity is an inherent characteristic of humans or rather something that is conferred by society.[5] Indeed, without an unambiguous theoretical foundation, many of the definitions of privacy that depend upon appeals to human dignity crumble like sandcastles with the rising tide. By considering the notion of the "sacred self", which is posited to be that part of the self integral to personhood, Neill is able to move beyond this debate.

Neill construes human dignity not as being inborn but rather as a "rationally constructed metaphor for innate properties".[6] In developing her theory, Neill further distinguishes between factual and metaphorical "innateness"; the former being something that is congenital, whereas the latter is a construction that represents the former properties. To further refine this distinction, Neill differentiates between physical and psychological natural properties, with the former reflecting subsistence properties and the latter being comprised of an individual's private and autonomous nature that helps an individual attain a minimal level of psychological security. Neill asserts that the production of thought reflects privacy and autonomy at their most elemental level. It is the privacy and autonomy of thought that embodies a person's perception of his or her innate privacy and autonomy. It is thus from factually innate properties that society then develops a conception of human beings as dignified. From this moral conception springs the creation and bestowal of rights. Morality therefore serves to rationally and metaphorically reconstruct factual reality. In order to avoid criticism that metaphor cannot ground entitlement, Neill appeals to the work of such scholars, as Lawrence Kohlberg, and Philip Wheelwright, who has defended "the ontological status of radical metaphor … [as] a medium of fuller, riper knowing".[7]

The dual ontological nature of Neill's theory, which postulates rights as being both originally created and bestowed by society, rejects natural rights theory that views rights as fixed objects given in nature that can be discovered and applied by humankind. Similar to Lockean rights theorists, Neill asserts that the development of rights is a gradual process by humans using rational means, although she does reject the claim that individuals contract to preserve natural rights. Instead, Neill posits that humans bestow rights upon one another as a means of metaphorically expressing the meaning of innate properties in their lives. By definition, she therefore also rejects the notion that humans are born with rights. Rather humans, by virtue of birth, are provided with the capacity to construct rights. By conceiving the right to privacy as both innate and culturally bestowed, Neill's theoretical model is able to differentiate between circumstances in which privacy is a political, social, and individual necessity reflective of the human dignity in which it is grounded and those in which claims to privacy stretch beyond any legitimate connection to the dignity of the "sacred self".[8]

Legitimating the Right to Privacy

As Neill argues, the psychological natural properties inherent in all individuals facilitate the autonomous production of thoughts as well as their protection, since a person exercises exclusive control over his communication to others. All individuals can therefore be viewed as innately possessing some degree of privacy. Privacy and autonomy are posited to factually exist as a property of people's thoughts. In turn, the ability to conceal and determine which thoughts and aspects of one are divulged to others influences the degree to which a person is perceived by others as being dignified. It therefore becomes clear how the conception of people as innately private and autonomous gives rise to the notion of individuals as being inherently dignified. Perhaps more importantly, this conception derives from the perception of something actually possessed by humans. As Neill states, "it is a moral metaphor for a non-moral fact of non-physical human nature".[9] Put another way, once humans, who are innately private and autonomous, perceive themselves as such, they develop a conception of themselves that metaphorically reflects the nature of these natural properties. Once constructed, this moral metaphor of dignity becomes factually inherent and notions of obligation attach to it. Thus it is not human dignity as a property in and of itself, but rather, a uni-

versal tendency to perceive people as dignified that forms the foundation for protecting human dignity as a right. By protecting privacy, society safeguards not only the innate natural properties of individuals but also the emergent perception of humans as dignified. As opposed to a number of other authors who seek to ground privacy rights in human dignity, but never convincingly make the connection, Neill's theory reaches further back and effectively unpacks the concept as a deliberate construction erected on innate facts, which thus supplies the moral origin of rights; value and meaning attach to innate psychological properties by imposing value and meaning on the moral metaphor that represents them. The result is an emergent perception of humans as dignified, which, once generalized to include the duties of all individuals to all others, facilitates the cultural bestowal of rights. Indeed, in Neill's theory, the conception of humans as inherently dignified serves as the moral metaphor for innate properties of privacy and autonomy and provides the foundation upon which a theoretical moral obligation to defend human dignity is constructed. It is from this moral obligation that concrete duties in the form of norms and rights are constructed. However, it is important to remember that privacy and autonomy rights bestowed by society safeguard the moral ideal of individual dignity, rather than the innate properties of individual privacy and autonomy, which the metaphor of human dignity represents.

Thus, Neill's model contains three levels, including the innate, the moral-metaphorical, and the manifest-symbolic, all of which aid in the universal development of natural rights. Once the rights are constructed, a fourth level materializes: the level of the "rights trade". In an attempt to secure a private life, individuals engage in what Neill alternately terms the "dignity trade" or the "rights trade".[10] It is in this sphere that humans assert claims to privacy, trade them in exchange for other goods, or, at times, see them expropriated for the public good. The moral legitimation for such claims is dependent upon whether they derive from absolute static norms based on innate natural properties (the "sacred self") or from the ideal of dignity that grounds those norms.

Applying the Model

As discussed above, the weakness of scholars, such as Edward Bloustein, who attempt to legitimate privacy rights through appeals to human dignity rests with their failure to sufficiently explicate the concept of dignity, which often leads to attributing to it a factual innateness that assumes an almost mystical character undeserving of ontological scrutiny.[11] By conceiving of human dignity as a metaphor for innate privacy and autonomy and as the basis upon which to construct duties, Neill not only addresses the limitations of previous theories, but also offers a model capable of determining legitimate fluctuating rights with reference to the source of rights in original human nature.

In applying her model to questions of privacy protection, Neill distinguishes between infringement of an individual's broad right to a private life and infringements of an individual's narrow privacy rights to inherent privacy and human dignity. Broad privacy rights arise as individuals seek to maintain a private life on the basis of the dignity to which society's view of personhood gives them a right. These broader rights are protected through conventional fluctuating norms. Narrow privacy rights are the static symbolic protections that defend the conception of human dignity in Neill's ontology by making manifest the obligation that symbolizes that dignity; i.e., the manifest-symbolic or third level of Neill's model. These narrow rights are thus safeguarded by natural, conventional static norms. Neill considers them to be conventional because they are culturally determined and natural since they are both locally absolute and designed to preserve the conception of humans that is based upon innate qualities. While transgressions of broad rights, or what Neill terms "trade transgressions", impinge on conventionally bestowed rights, infringements of narrow rights, which Neill refers to as "rites transgressions", violate "innate privacy, individual dignity, or the universal conception of humans as dignified".[12]

While society safeguards the basic conception of human dignity through static norms, individuals may attempt to have their entire persons viewed as sacred and therefore deserving of privacy protection. This, however, is a mistake, according to Neill, because it conflates the privacy of a private life with privacy of the "sacred self" and attempts to extend the "sacred self" beyond its inherent limits. The obligation that attaches to human dignity may only be applied to claims that derive from innate properties, which is why Neill labels any laws not based on claims to protect dignity as fluctuating rather than static norms. Nonetheless, Neill does argue that in some cases, static and fluctuating privacy norms are both required, in order to protect the human dignity upon which moral culture is built. Given this, Neill asserts that the criterion that should be applied when deciding whether an infringement of a privacy right is legitimate is the degree to which that right protects either the "sacred self" or society's moral conception of the dignity of humans. Put another way, decisions about what constitutes a legitimate claim to privacy must be decided by the degree to which they are grounded in an individual's ideologically deep, or what she terms "untradeable", right of privacy and human dignity. Neill therefore believes that policy analysis and legislative development should be guided by concern for human dignity, and the ideologically deep privacy rights that attach to this, rather than broader privacy claims. As she argues, "the potential violation of innate dignity rights is the only viable reason for a privacy right".[13] In order to determine whether an interest merits protection, its origin must be traced back through Neill's structure of rights. Some norms deserve strong symbolic rights because they emanate at the man-

ifest-symbolic level, while others may go right back to the very origin of rights to safeguard the fundamental privacy and autonomy of the mind. Yet many norms, while making claims to privacy and autonomy rights, bear little relationship to symbolic or psychological properties and rights. As Neill asserts, many that fall within this category are often protective of economic interests masquerading as privacy concerns.

From this analytical standpoint, Neill concludes that medical databases, when used for their intended purposes and with adequate safeguards against unauthorized access, do not violate static privacy norms. This would include use of the medical database made by insurance companies when making decisions about issuing life insurance policies. According to Neill, an insurance company does not transgress an individual's privacy when it acquires that person's health information for decision-making purposes. In such cases, according to Neill, the individual is seeking to protect an economic interest in obtaining a life insurance policy without fully disclosing all the relevant information necessary for the insurance underwriter to reach a decision.[14] It is only if information held within medical databases is released to a third party without the consent of the person that her innate privacy would be violated. Indeed, Neill claims that medical information is *about* the body rather than *of* the body and therefore merits protection not through static norms but rather through fluctuating norms; norms that are determined by governments who are under pressure in our information age to demonstrate that rights are being taken seriously and safeguarded. To put it another way, Neill's ontology of natural rights views the body as a symbol of human dignity and thus deserving of protection by static norms that express the dignity of the inner self through reference to the observable self. Information about the health of that body; however, does not reside within the refuge of what is considered innately private.

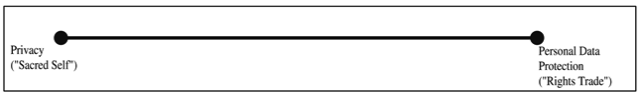
The view of a national medical data bank as not approaching inherent privacy is grounded in the recognition that the body is neither itself factually innately dignified nor, a related point, that from which our metaphor of human dignity arises. This, I think, has been a point of massive confusion in Western culture where the body, which (as an aspect of dignity) is merely a concrete symbol of what we revere, has, through its concreteness and as the object around which static norms are constructed, come wrongly to be viewed as the seat of inherent dignity itself. Yet it is only in its concreteness that the body represents our dignity and the innate properties of human thinking, and so facts about our bodies are not inherently private, even where economic and other social interests might cause us to wish that they were.[15]

The one area of medical information where Neill makes an exception is with regard to counselling records, which she argues are inherently private because they reflect the thoughts, and thus the "mind" of an individual, rather than just information about the mind. Thoughts expressed in confidentiality to a counsellor provide immediate access to the "sacred self" and therefore warrant the protection offered by static privacy rights. However, it should be pointed out that this analysis does not mean Neill is arguing against measures designed to protect medical information, rather, that any such instruments would defend, under the rubric of privacy, interests other than inherent privacy and dignity.

According to Neill, human dignity is a metaphor that assumes a dual role; it reflects the innate natural properties of privacy and autonomy, and, based on these original, innate properties, it provides the moral justification for constructing societal norms protective of privacy. Though Neill does not couch her analysis of privacy in terms of access to information or personal data protection, her model anticipates the tension between these policy goals. Neill's model demonstrates that medical information, with the exception of mental health counselling notes, should be protected by conventional fluctuating norms, rather than the static norms that protect the fundamental privacy of the "sacred self". Put another way, because medical information lacks a clear relationship to symbolic or psychological properties and rights, it, according to Neill's model, does not warrant protection through an appeal to a strict privacy right. Instead, this type of personal information merits protection through fluctuating norms that are subject to tradeoffs with other fluctuating rights.

Although not explicit, Neill's distinction between the privacy of the "sacred self" and the broader privacy rights associated with the "rights trade" that can be exchanged for other goods, appears roughly analogous to the differences between privacy and personal data protection.[16] A "true" privacy interest that protects the "sacred self" warrants strict protection, while other claims not linked to the "sacred self" are subject to tradeoffs with competing interests. Thus, Neill's model offers a compelling theoretical justification of privacy that not only establishes a convincing link between narrow privacy interests and human dignity, but also helps explain instances in which interests related to broader privacy claims and rights might be subject to opposing public policy claims, which seems to closely reflect the purposes of personal data protection legislation. Based upon this distinction it is proposed that we construct a privacy–data protection continuum, which can be utilized to situate claims to privacy protection. "True" privacy claims, or those reflective of an individual's inherent privacy and dignity, occupy one end of the spectrum, while those broader claims to privacy, which, extrapolating from Neill's model, might more appropriately be termed "data protection", find a base at the opposing end (see Figure 1).

Figure 1 — Privacy–Personal Data Protection Continuum Based on Elizabeth Neill



With reference to Neill's ontology of privacy rights, various international and national legislative devices in respect of personal (health) information can be evaluated in terms of the degree to which they address privacy claims or data protection imperatives and, thus, where they might be situated on the continuum. It is exactly upon such an analysis that attention will now focus.

International Privacy Guidelines and Legislation: Privacy or Data Protection?

As a number of researchers argue, the privacy legislation of the 1970s and 1980s was generally designed to address concerns about the privacy relationship between the individual and the state.[17] Yet, in the interim, transformations in the economic, political, and technological landscape have occasioned the locus of concern regarding privacy protection to shift toward a sharpened emphasis on the commercial exploitation of privacy.[18] Health information, as a sector, has also been caught up in such changes and has not escaped domestic and international pressures for minimum standards of protection for personal information, as well as harmonization between jurisdictions. To better understand some important responses to this situation, the following examination of international guidelines and legislation is offered.

Organisation for Economic Co-operation and Development

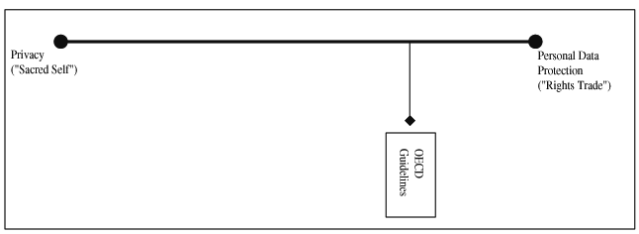
By the late 1970s, the Organisation for Economic Co-operation and Development ("OECD") recognized the potential for conflict between automatic data processing capabilities and privacy protection. Indeed, this concern was being reflected by the introduction of privacy laws in a number of countries "to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data".[19] Concerned about the effect that disparate national treatment of personal data could have on commerce, the OECD adopted and published in 1980, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Guidelines") in an attempt to spur harmonization of national legislation. The OECD Guidelines set out the following eight basic principles that establish what are often referred to as "fair information practices":

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[20]
2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with paragraph 3 [purpose specification principle] except
   (a) with the consent of the data subject; or
   (b) by the authority of law.
5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle: An individual should have the right:
   (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   (b) to have communicated to him, data relating to him
      (i) within a reasonable time;
      (ii) at a charge, if any, that is not excessive;
      (iii) in a reasonable manner;
      (iv) in a form that is readily intelligible to him;
      (v) to be given reasons if a request made … is denied, and to be able to challenge such denial; and
      (vi) to challenge data relating to him and, if the challenge is successful to have the

data erased, rectified, completed or amended.

8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.[21] These Guidelines, which Canada adopted in 1984, were designed to strike a balance between respect for privacy as a human right and the facilitation of international data flows. The importance attributed to the free flow of information in support of commercial purposes is reflected in one of the recommendations made by the OECD, contained in its Guidelines, which states that member countries should refrain from erecting barriers to data flows in the name of privacy protection. The OECD Guidelines themselves, which are neutral with regard to type of technology, apply only to identifiable information, whether in the public or private sector and are to be interpreted as minimum standards that national governments can supplement to legitimately protect personal privacy and individual liberties. Since the OECD Guidelines attempt to establish a minimal threshold of privacy protection that can be applied broadly by individual nations, it is not surprising that they do not treat health information specifically. The OECD Guidelines also recognize that different types of data have different degrees of sensitivity and thus may not all require protection; however, any exceptions, including those made on the basis of national sovereignty, national security and public policy, should be as few as possible and made known to the public. Considering Neill's model and the privacy–data protection continuum, the OECD Guidelines appear more concerned with the protection of personal data than with privacy and should therefore be situated toward the middle right of the spectrum, closer to the ontological level of the "rights trade" that protects the broader, fluctuating rights to a private life (see Figure 2).

Figure 2 — Location of the OECD Guidelines on Privacy–Personal Data Protection Continuum



While not a universal or binding standard, the eight principles articulated by the OECD Guidelines are reflected in one form or another in most Western privacy laws, including Canadian legislation and a European Union Directive that protects personal data, to which attention will now turn.

The European Union

The Council of Ministers of the European Union (EU) formally adopted the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* ("EU Data Protection Directive") on October 24, 1995.[22] A Directive from the Council of Ministers is a type of framework legislation that, while binding on Member States, does provide each with the right to determine the means of implementation and the actual wording of the national legislation necessary to implement the Directive. For this reason all members of the EU were granted three years for implementation. It took five years to develop the Directive, during which time a number of changes were made, including: the deletion of a distinction between the public and private sector, thus mirroring the OECD Guidelines; the permissibility of a "negative option" with regard to informed consent; an exemption for the press; the application of the rules to manually processed data; the processing of sensitive data; and, the role and independence of national supervisory bodies.[23] The inclusion of the phrase "Free Movement of Such Data" in the title of the EU Data Protection Directive, which also accords with one of the stated purposes of the OECD Guidelines, is telling of the influence of private sector lobbyists on its development and content.[24]

The EU Data Protection Directive, similar to most directives promulgated by the Council of Ministers, requires the reader to first wade through 72 "whereas statements", drafted to help interpretation and state intentions, before actually getting to the articles it sets out. Broadly stated, the 34 articles contained in the EU Data Protection Directive reflect the "fair information practices" also found in the OECD Guidelines. The Directive's purpose, as outlined in article 1, is to protect the fundamental rights and freedoms of natural persons, especially privacy with respect to the processing of personal data, without obstructing the free flow of information between Member States. Article 2, which sets out definitions, states, "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[25] Additionally, it is interesting to note that the EU Data Protection Directive defines "processing of personal data" in a manner that combines collection, use, and disclosure of information. Some commentators have argued that this is perhaps a more realistic conception of information manipulation that reflects the fluidity and decentralization of the contemporary environment.[26] Article 3, which discusses scope, states that "processing operations concerning

public security, defence, State security (including the economic well-being of a State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law" as well as the processing of personal information "in the course of a purely personal or household activity" fall outside the purview of the EU Data Protection Directive.[27]

The OECD "collection limitation principle", arguably the most important element of "fair information practices", is incorporated in the EU Data Protection Directive through article 6. It requires that personal data may only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".[28] There is, however, an exception made for data processing if done for historical, statistical or scientific purposes. Data controllers must also ensure that the data are accurate, that the amount of information collected is not excessive in relation to the stated purpose for collection and processing, and that the data are not kept in identifiable form for any longer than is necessary to fulfil the original purpose for their collection.[29]

Article 7 of the EU Data Protection Directive outlines the six criteria for judging whether a data processing operation satisfies the requirement of clause 1(a) of article 6 that personal data must be "processed fairly and lawfully". The six legal grounds are: the data subject has given unambiguous consent; processing is necessary to perform a contract to which the individual is a party; processing is necessary to comply with a legal obligation; processing is necessary to protect the vital interests of the data subject; the processing is necessary for the performance of a task carried out in the public interest; or processing is required to satisfy the legitimate interests of the data controller or third party.[30] The last two grounds for processing personal information may be overridden by the data subject on "compelling legitimate grounds relating to his particular situation".[31] Data subjects may also object to the use of their data for direct marketing purposes, although the Directive leaves the mechanism, either opt-in or opt-out measures, to the discretion of Member States.[32]

The EU Data Protection Directive also includes demands related to the OECD "security safeguards principle". Data controllers must "implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access" and all measures undertaken must be appropriate to the level of risk.[33] These requirements apply to data controllers who process their own data as well as to third party organizations contracted by a data controller to process data on its behalf.[34]

The EU Data Protection Directive reflects the "openness principle" of the OECD Guidelines and "fair information practices" in its requirement that data subjects be provided with information about the identity of the data controller or representative, the purposes for which the data will be processed, the identity of recipients or categories of recipients of the data, and any rights regarding access to and correction of data.[35] Moreover, the data controller must "notify the supervisory authority referred to in article 28 [public authorities similar to Canada's Privacy Commissioner] before carrying out any wholly or partly automatic processing operation or set of such operations".[36] Article 21 further stipulates that the supervisory authority must maintain a register of all processing operations for which it receives a notification and that this register shall be made available to the public.

The "individual participation principle" found in the OECD Guidelines is also reflected in the EU Data Protection Directive, through article 12, which outlines a right of access for data subjects. Data controllers must confirm "without excessive delay or expense" whether or not they possess information about an individual, and if so, the purposes for which the data are being processed and to whom they will be disclosed. The data controller must also inform the person as to the source of the information[37] and an individual has the right to correct, delete or demand a halt to the processing of any personal information that is incomplete, incorrect or otherwise in contravention of one of the provisions of the Directive.[38] Any rectification, erasure or stop to processing must also be communicated to third parties who have received the information.[39]

The EU Data Protection Directive differs from the OECD Guidelines in that it generally prohibits the processing of data concerning health or sex life or any other personal data that would reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.[40] The Directive does, however, provide the following exceptions to this prohibition: if the data subject provides consent; if the information is required by a Member State's national employment law, provided adequate safeguards are in place; if the processing is necessary to protect the vital interests of the data subject; if the processing is done by a non-profit entity, with a political, philosophical, religious or trade union mandate only with regard to its own members, and there is no third party disclosure without consent; if the data are already in the public realm or are required for legal proceedings; if the data are required to facilitate medical care and are processed by a health care professional subject to either legal or professional obligations of secrecy; and, if the processing is required for police activities and done only by official authorities.[41] This article also provides a clause that permits Member States to allow additional exceptions if they are in the national public interest.[42] The EU Data Protection Directive thus carves out, subject to limited exemptions, health information, treating this type of information analytically exceptionally *vis-à-vis* the rest of the Directive. This may have been done to reflect a perceived higher

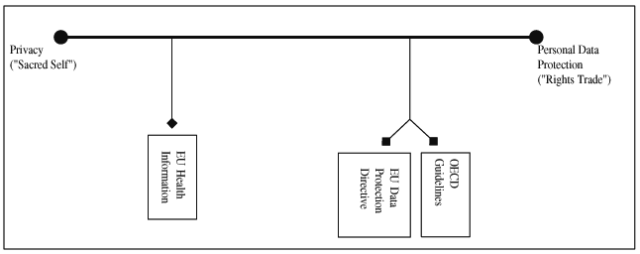
value and thus need for protection that attaches to personal health information, while at the same time including an exception for medical practitioners so as not to impede the provision of medical services. Similarly, this qualified prohibition on the use of data regarding an individual's health or sex life might also have been included in the EU Data Protection Directive to ensure compliance with the *Convention for the Protection of Human Rights and Fundamental Freedoms* ("ECHR")[43] adopted by the Council of Europe in 1950, which stipulates in article 8 the "right to respect for private and family life".[44] [45]

Article 9 of the EU Data Protection Directive provides exemptions for the processing of personal data carried out for journalistic, artistic, or literary purposes. Article 13 outlines the exemptions related to national security, defence, public security, police investigation activities, economic interests of a Member State or the European Union, and the protection of the data subject or of the rights and freedoms of others.

Finally, as briefly alluded to above in the discussion of the "openness principle", the EU Data Protection Directive specifies that each Member State must have an independent public authority responsible for monitoring the provisions adopted pursuant to the Directive. Each national authority must be endowed with investigative powers, the power to engage in legal proceedings or bring any violations to the attention of the applicable judicial authorities, and powers of intervention. This latter power should include the ability to issue opinions and orders that block or ban processing, the right to admonish data controllers, and the right to refer matters to national parliaments.[46] The public authority is also responsible for receiving and investigating claims from any person relating to the lawfulness of data processing about that person.

The EU Data Protection Directive appeals to the necessity of protecting fundamental rights and freedoms, or what Neill would presumably consider innate privacy and autonomy, especially with regard to the qualified prohibition on the processing of information about a person's health or sex life. In general, however, the EU Data Protection Directive endeavours to protect rights and freedoms without obstructing data flows; a fact attested to by the full title of the Directive. For this latter reason, the Directive contains a number of exemptions from its scope that are based upon public policy priorities other than privacy protection. The Directive, therefore, cannot be considered to defend what Neill would consider "legitimate" privacy interests based upon protection of the "sacred self". The rights enunciated by the EU Data Protection Directive, except with regard to health and sex life information, align more closely with broader claims to privacy whose ontological status would place them closer to the data protection than the privacy side of the spectrum, similar to that of the OECD Guidelines. Nonetheless, the special treatment afforded health information by the Directive indicates that its protection is considered to be more about privacy than personal data protection. This somewhat anomalous nature of the EU Data Protection Directive *vis-à-vis* other legislative schemes to protect privacy, which warrants dual placement on the privacy–personal data protection continuum, is outlined in Figure 3.

Figure 3 — Dual Location of EU Data Protection Directive on Privacy–Personal Data Protection Continuum



The OECD Guidelines and the EU Data Protection Directive thus contain a number of similarities that, in general, make them more about personal data protection than privacy. The exception is EU health information, which, given its special status under the EU Data Protection Directive, is allied more closely with privacy issues than with personal data protection. If this is the situation at the international level, what is happening in Canada?

Canadian Federal and Provincial Legislation

Having outlined Neill's model of privacy protection and established where two prominent international devices putatively designed to regulate privacy are situated within that model, this section will engage the second question driving this paper by comparing the *Personal Information Protection and Electronic Documents Act* and the provincial Acts in Alberta, Saskatchewan, Manitoba, and Ontario that deal specifically with health information. In addition to presenting a comparative analysis, these pieces of legislation will be assessed to establish where they fit on the privacy–personal data continuum, in order to discern whether health information protection in Canada is more about privacy than personal data protection.

Personal Information Protection and Electronic Documents Act

Although in Canada personal information maintained by the federal government was first safeguarded by Part IV of the *Canadian Human Rights Act*[47] of 1977, and subsequently through the *Privacy Act*[48] of 1982, which came into force on July 1, 1983, it was not until April 13, 2000 when the *Personal Information Protection*

and Electronic Documents Act ("PIPEDA") received Royal Assent, that protection began to be extended to information held by the private sector in Canada.[49] In the meantime, protection of personal information throughout much of the rest of the public sector in Canada had gradually been enacted.[50] Part of the motivation behind enacting the PIPEDA for private sector privacy protection was perceived international pressure from the European Union, the member states of which, in adherence to its Data Protection Directive, would limit transnational data flows to only those foreign countries with similar legislative mechanisms in place. As the legislative history of the PIPEDA points out, "Part I of Bill C-6 (PIPEDA) also responds to recent privacy initiatives in Europe … The Directive [EU Data Protection Directive] could, therefore, have a negative impact on Canadian businesses engaged in commerce with companies in European Union countries, unless adequate privacy legislation is introduced in Canada".[51] Indeed, article 25 of the EU Data Protection Directive provides:

> 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
>
> 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. . . . .[52]

In a decision from December 20, 2001 the EU Commission stated that Canada's PIPEDA did meet the required standard under its Data Protection Directive.[53] Thus, the PIPEDA achieved the objective of ensuring that EU Member State companies could continue to do business with Canadian firms.

The full scope of the PIPEDA was implemented in a staggered fashion. As of January 1, 2001, it applied to all federally regulated private sector organizations as well as those that disclosed personal information for consideration across provincial or national boundaries. A Senate amendment motivated by concern over the applicability of the Act to personal health information resulted in an exemption from coverage for health information until January 1, 2002.[54] In the third phase, all provisions outlined by the PIPEDA came into full force on January 1, 2004: the Act now covers all information collected, used or disclosed during the course of commercial activities by private sector organizations, not governed under equivalent provincial legislation. It is the "commercial clause"[55] that the federal government has used to constitutionally justify the reach of the PIPEDA into what otherwise might be considered provincial jurisdiction. The application of this notion of "commercial activity" to the health sector has caused much unresolved confusion since health has traditionally been an area of provincial legislative activity.[56]

As defined by the PIPEDA, "'commercial activity' means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists".[57] Aside from being circular, such a definition does not go very far in helping to clarify the scope of the Act. As the Canadian Institutes of Health Research has pointed out:

> There are some important activities in the health sector, the nature of which cannot yet be clearly determined one way or another. For example, whether the services of a health professional carried out in a private clinic reimbursed by the public purse will be considered "commercial activity" within the meaning of the PIPED Act is not yet known. Whether the activities of private, not-for-profit organizations and/or cost-recovery activities constitute "commercial activity" is likewise impossible to ascertain at this stage and will likely be circumscribed over time through judicial interpretation.[58]

There is an element of the PIPEDA itself, however, that might render these constitutional concerns largely redundant; namely the "substantially similar" clause, which exempts provinces from having to adhere to the Act if they pass legislation that the federal government recognizes as "substantially similar" to the PIPEDA.[59] If the four provincial health information protection Acts examined in this paper are so recognized by the federal government, then not only would the PIPEDA no longer apply to health information within those provinces, but such information would receive constitutionally unambiguous protection through provincial acts.

The federal Department of Industry, whose Minister is responsible for making recommendations about exemptions to the Governor in Council, outlined in the *Canada Gazette*[60] the process that will be employed to determine whether provincial legislation may qualify for an exemption based on the "substantially similar" clause in the PIPEDA.[61] With reference to the presentation by then Industry Minister John Manley to the Standing Senate Committee on Social Affairs, Science and Technology, substantially similar statutes will generally require "legislation that provides a basic set of fair information practices which are consistent with the CSA Standard, oversight by an independent body and redress for those who are aggrieved".[62] As of writing, only Ontario's *Personal Health Information Protection Act, 2004* ("PHIPA")[63] has been recognized as being "substan-

tially similar".[64] The health information protection legislation in Alberta,[65] Manitoba, and Saskatchewan has not. It should be pointed out that even if the provincial Acts are deemed equivalent to the PIPEDA, it is the federal government's position that the federal Act would still apply to a health care provider or hospital when engaging in inter-provincial and international commercial dealings.[66] This might, in turn, still raise the constitutional battle between provincial regulation of health and federal regulation of inter-provincial trade and commerce.

The PIPEDA is an interesting piece of legislation in that it sets out the bulk of its requirements related to fair information practices in a Schedule rather than directly in the Act. Moreover, Schedule 1, which sets out the main information handling provisions with which all organizations subject to the Act must comply, is, verbatim, the *Model Code for the Protection of Personal Information* ("CSA Code")[67] developed by the Canadian Standards Association in 1996. Thus the PIPEDA is not worded as legislation usually is, but rather, is formulated using what was originally a voluntary guide to conduct. Schedule 1 of the Act sets out the following 10 information principles:

1. Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
6. Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.[68]

As is readily apparent, this Schedule very closely resembles the OECD Guidelines discussed above, which is not surprising given that Canada adopted them in 1984, and both the Schedule and the Guidelines are motivated by the desire to strike a balance between privacy and the free flow of information for commercial purposes. The only major difference between the two schemas is that Schedule 1 includes a right for individuals to challenge concerns about compliance with these "fair information practices", something that is not contained in the OECD Guidelines. The PIPEDA, unlike the *EU Data Protection Directive*, does not offer a separate regime of protection for "sensitive data"; the PIPEDA does not provide rules pertaining to the recipients of personal information; and, the PIPEDA applies only to organizations engaged in commercial activities; whereas, the EU Data Protection Directive and the OECD Guidelines apply to all controllers of personal information.

Like the EU Data Protection Directive, the PIPEDA provides exemptions from coverage, with respect to personal and domestic use of personal data, as well as use for journalistic, artistic, or literary purposes. Where these exemptions do not apply, the PIPEDA generally requires the knowledge and consent of the individual who is the subject of the data (data subject) before any personal information may be collected, used, and/or disclosed. There are, however, some important exceptions. Collection may occur without consent, if consent cannot be obtained in a timely manner, if it would compromise the availability or accuracy of the information, or if the collection is necessary to investigate a crime.[69] Personal information can be used without consent for police investigations, in a case of an emergency that threatens the life, health, or security of an individual, and for statistical or scholarly study or research as long as confidentiality is ensured.[70] Disclosures of personal information may be made by an organization without the knowledge or consent of the data subject for debt collection, law enforcement, national security, emergency situations, statistical compilation and research,[71] to comply with a

subpoena or warrant, and at the earlier of 100 years after the record was created or 20 years after the death of the individual to whom the information pertains.[72] Moreover, if these exemptions apply, an organization may disclose personal information for purposes other than those for which it was collected.

The PIPEDA also sets out the procedures for making requests for access to the information an organization holds about an individual, including time limits for response, notification and response requirements for organizations, and prohibitions on access to certain types of information. Denying access is permissible if doing so would reveal personal information about a third party (unless that person consents to disclosure or the information can be severed), if the information is protected by solicitor–client privilege, if disclosure would reveal confidential commercial information, if release of the information could threaten the life or security of another person, or if the information was generated in the course of a formal dispute resolution process.[73]

Individuals may file complaints with the federal Privacy Commissioner against organizations that have contravened any of the provisions related to the collection, use, and disclosure of personal information. When investigating complaints the Commissioner is provided with powers to summon witnesses, administer oaths, receive evidence, and enter premises to examine records and talk with any person located therein. However, unlike the national authorities in the EU, the federal Privacy Commissioner lacks any order-making power and must rely on mediation, conciliation, and recommendations.[74]

The above explication and analysis of the PIPEDA has helped develop a basis of comparison to the four provincial Acts in respect of health information in order to respond to the second research question of this paper; namely, do the various provincial health information protection Acts go beyond the PIPEDA, such that health information protection might better be considered, more about privacy than personal data protection? This comparative examination will also lay the groundwork for developing a response to the query about which of the Acts is aligned with Neill's model.

Provincial Legislation

The PIPEDA does not hamper the provinces from enacting legislation within their respective jurisdictions. It purports to provide a baseline for the protection of personal information in Canada. In fact, the "substantially similar" clause invites provinces to develop their own legislation applicable to their distinctive needs and requirements. As mentioned, to date, four provinces have promulgated information protection legislation specific to the health care industry.

All of the provincial Acts, as opposed to the PIPEDA, apply to health care providers, regardless of whether they are engaged in commercial activities. Alberta's *Health Information Act* ("HIA") received Royal Assent on December 8, 1999 and came into force on April 25, 2001.[75] Saskatchewan passed the *Health Information Protection Act* ("HIPA") on May 6, 1999, which was proclaimed in force on September 1, 2003.[76] Manitoba's *Personal Health Information Act* ("PHIA") was passed on June 28, 1997 and came into force on December 11, 1997.[77] Ontario's *Personal Health Information Protection Act* (PHIPA) came into force on November 1, 2004[78] and, as mentioned previously, it is the only provincial health information protection act that, as of writing, has been recognized by the federal government as being "substantially similar" to the PIPEDA.[79] Each of the four Acts outlines similar purposes, including the following: to protect the privacy of individuals with regard to their health information; to enable access to and the sharing of health information in order to provide health services and manage the health system; to prescribe rules for the collection, use, and disclosure of personal health information; to provide individuals with rights of access to and correction of their medical records; to establish remedies for contravention of the Acts; and, to provide for independent reviews of decisions made under the Act.[80] All four provincial Acts apply to identifiable personal health information,[81] which includes information about both mental and physical health.[82] While Saskatchewan, Manitoba, and Ontario limit the scope of their respective Acts to encompass only personally identifiable information, Alberta legislation sets out explicit provisions that permit the collection, use, and disclosure of non-identifying health information, with very few restrictions.[83] All of the Acts further specify their scope by outlining who qualifies as a "custodian" (Alberta),[84] "trustee" (Saskatchewan and Manitoba), [85] or "health information custodian" (Ontario).[86] These are the people and organizations required to abide by the provisions of the Acts with regard to the collection, use, disclosure, retention, and disposition of personal health information. They include physicians, hospitals, pharmacists, district health boards, medical laboratories, special-care homes, mental health care facilities, and ambulance services, among others. Trustees and custodians are also responsible for ensuring the security, confidentiality, accuracy, and integrity of personal health information in their custody.[87]

All of the four Acts contain detailed sections pertaining to the collection of personal health information. In most cases, the collection of non-identifying information is permissible. Identifiable information may only be collected if it is directly related and necessary to carry out a purpose specified by the Act, which is usually the provision of health services. The Acts provide that information should always be collected directly from the individual to whom it pertains, unless otherwise authorized by the individual, impossible in the circumstances, or would result in the collection of inaccurate information. In Alberta and Manitoba, a custodian is only required to take reasonable steps to inform the individual of the purpose for the collection and there are no provisions

about consent,[88] while in Saskatchewan and Ontario consent must be informed, although it may be express or implied and need not be in writing.[89] Although, at face value, Alberta and Manitoba would appear to offer less protection, presumably most individuals would consent to the collection of personal health information by their health care provider in order to facilitate the diagnosis and treatment of services being offered. The more troubling areas of provincial legislation where personal health information is susceptible to abuse relate to use and disclosure provisions, to which attention will now turn.

As mentioned previously, the Acts in Saskatchewan, Manitoba, and Ontario apply only to personally identifiable information,[90] while the Act in Alberta also includes provisions that permit the collection, use, and disclosure of non-identifying health information for any purpose.[91] In general, under these Acts, personally identifiable health information may only be used to provide health services: for purposes consistent with those that gave rise to the original collection, to determine the eligibility of a patient to receive a health service, to monitor and prevent or reveal cases of fraudulent use of publicly funded health services, to conduct research (subject to ethics committee review), to conduct investigations relating to members of a health profession, to provide health services provider education, to obtain payment for services, to conduct internal management activities, to comply with subpoenas, warrants, or orders issued by a court, and for use by a prescribed professional body to discharge its duties.[92] Additionally, in Alberta, provincial health boards, regional health authorities and the Minister and Ministry of Health may use identifiable health information for planning and resource allocation, health system management, public health surveillance, and health policy development.[93] Similar provisions are also found in Saskatchewan's, Manitoba's, and Ontario's legislation.[94] The relatively broad range of institutions in all four provinces that can use personal health information without the consent of the information subject, has occasioned at least one observer to claim that the provincial statutes "have been variously described as having very little to do with privacy and [being] much more concerned with providing government and researcher[s] access to confidential medical records".[95] While there is certainly some truth to this accusation, these exemptions are not surprising when one considers that all the statutes were enacted by provinces; provinces that are responsible for administering and substantially funding the health care systems within their jurisdictions. Without reliable information about these systems, management in times of tight fiscal conditions and rising expectations, is made quite difficult, if not impossible.

The four provincial Acts contain disclosure provisions that generally prohibit health care providers from disclosing identifying health information without consent, unless permitted or required by another section of the respective Act. In addition to the release of information to other health practitioners and for research purposes, as will be discussed subsequently, all of the Acts permit disclosure without consent for evaluation purposes by quality of care committees, for court proceedings, for police investigations, for investigations by provincial Ministries of Health for fraud detection purposes, and to health professional regulatory bodies if required for investigations. With regard to disclosure, the Ontario Information and Privacy Commissioner has commented on the role of so-called "lock boxes" in health privacy legislation, which offer patients the statutory right to prohibit health care providers from disclosing their health information to any other providers.

> This so-called "lock box", which would provide individuals with some control over disclosures of their personal health information, is a key component of privacy protection. In the absence of any ability to control what information is shared among health care providers, in some cases extremely sensitive, subjective, personally damaging, irrelevant, or outdated personal health information could be shared against the wishes of the individual.[96]

Some observers argue that health care providers have opposed such restrictions on disclosure for fear that it would require the creation of multiple records, compromise patient care, and increase the potential liability of health care providers.[97] Only Manitoba's PHIA[98] and Ontario's PHIPA[99] provide this "lock box" type of protection for individuals, although Saskatchewan's HIPA only permits disclosure of medical information to other health care providers without consent "where it is not reasonably practicable to obtain consent"[100] and only if the person receiving the information agrees to use it "only for the purpose for which it is being disclosed" and does not "make a further disclosure of the information."[101] In addition, all of the provincial Acts permit disclosure without consent, in order to facilitate the permitted uses discussed above.

All four of the provincial Acts also contain provisions that require ethics approval for research using personally identifiable health information. Section 50 of Alberta's HIA empowers the ethics review board to determine whether consent is required from the individual to whom the information pertains. Similarly, Saskatchewan's HIPA allows for use of personal health information without consent if "in the opinion of the research ethics committee, the potential benefits of the research project clearly outweigh the potential risk to the privacy of the subject individual".[102] Manitoba's PHIA and Ontario's PHIPA contain very similar provisions.[103] The research exemptions in the provincial Acts are roughly analogous to the scholarly research exemption contained in paragraph 7(2)(*c*) of the PIPEDA.

Each provincial Act also confers on individuals a general right of access to their medical records under the control of a custodian or trustee. Each Act outlines the necessary procedures for making an access request and includes: a duty to assist individuals with their applications if required; rules about time frames to respond to requests; allowable fees; correction and amendment of

information in a record as well as rights of refusal by the custodian to make a correction; and exemptions for when access may be denied.[104]

The powers granted to Information and Privacy Commissioners, or Ombudsman in Manitoba, differ among the four provinces, with Alberta and Ontario conferring the strongest powers on their Commissioners. Sections 80 through 82 of the HIA grant the Alberta Commissioner the ability to make binding orders regarding access to records by patients, administrative matters pertaining to time limits and fees, and the collection, use, correction, disclosure, and destruction of health records. Sections 52 and 53 of Saskatchewan's HIPA equip the Commissioner with the ability only to comment and make recommendations. Although individuals do have the right under section 50 of the HIPA to appeal to a court a decision by a health care provider refusing access to a record, this section does not address any other issues surrounding health information such as use, correction, disclosure, and final disposition. In Manitoba, Part 4 of the PHIA permits the Ombudsman, as in Saskatchewan, to investigate complaints from individuals about the treatment of their personal information and to make recommendations. If warranted, the Manitoba Ombudsman may also forward complaints to the provincial Attorney General or professional regulatory bodies. In Ontario, section 61 of the PHIPA confers upon the Information and Privacy Commissioner the right to make binding orders about access, collection, use, and disclosure of personal health information, as well as orders concerning specific information practices of health information custodians. These powers were not contained in the original draft of the PHIPA, but were requested by the Commissioner in her detailed submission to the Standing Committee examining the bill.[105]

The preceding sections, devoted to explicating and comparing the federal and provincial statutes in respect of personal (medical) information, have laid the groundwork for engaging in the analysis, taken up in the next part of this paper, of whether health information protection legislation in Canada is best characterized as concerned about privacy or personal data protection.

Health Information Protection: Privacy or Personal Data Protection?

Although an exhaustive discussion of all of the provisions contained within the four provincial Acts is beyond the scope of this paper, the areas highlighted in the previous section do reflect the most substantive elements of each piece of legislation. While each of the provincial Acts reflects the "fair information practices" embodied in the OECD Guidelines and CSA Code, these are sectoral pieces of legislation designed to address exclusively the health care industry. The provincial Acts make no distinction between commercial and non-commercial activities and therefore apply to all health care providers within their respective jurisdictions. The PIPEDA is a much broader legislative instrument designed to establish a minimal threshold of data protection within all sectors of the private market. Moreover, while principle 4 ("limiting collection") of Schedule 1 of the PIPEDA allows an organization to specify the purposes for which it collects information, the provincial Acts actually enumerate, and thus limit, the purposes for which information may be collected. The provincial Acts further stipulate that information, subject to limited exceptions, should always be collected directly from the individual to whom it relates. The PIPEDA is silent on this point, which, given its commercial nature, is not that surprising.

Despite these differences, the preceding review has also made it clear that a number of the obligations imposed by provincial statute, mirror similar requirements found in the PIPEDA. Support for this position may be found in the fact that it has been argued, at least in Ontario, that "[m]ost physicians who have developed privacy policies to comply with PIPEDA will only have to make minor adjustments to them as a result of PHIPA."[106] Each piece of legislation attempts to vest in the individual some degree of control over personal health information by implementing consent requirements before others may collect, use or disclose personally identifiable information. Such consent requirements notwithstanding, beyond protecting the privacy of an individual's medical information, each of the statutes outlines an additional purpose: fostering information exchange within an increasingly diverse health care system. Indeed, each provincial law, like the PIPEDA, contains multiple provisions that provide for the use and disclosure of information without the consent of the data subject. A number of these provincial exemptions are motivated by other public policy concerns, such as permitting the exchange of information in order to provide medical treatment, allowing for the collection of data that can be used for performance evaluation of the health care system, facilitating research, and detecting fraud, among other things.

But individuals, given the rather personal nature of health information, usually perceive a substantial interest in maintaining the privacy of this type of information. One of the dilemmas for legislative schemes that regulate health information is therefore how to guard personal information, when its protection runs up against access interests and requirements, in a manner that reconciles these competing policy goals. In this context Gostin has concluded, "one of the burdens of achieving cost effective and accessible [health] care is a loss of privacy".[107] Though certainly present in the PIPEDA, the provincial Acts demonstrate a greater tension between access to information and the privacy of personal health information that appears characteristic of personal data protection legislation.

One area of the debate particularly demonstrative of this strain revolves around medical research and the fears that a requirement to obtain informed and written consent will stymie research through higher costs and greater administrative burden. Indeed, Gostin has argued that increased amounts of available, accurate health information would facilitate research.[108] This would be accomplished through the reduced cost of collecting and analyzing secondary data and through the increased trustworthiness and generalizability of the data given the wider scope of collection. However, as Simitis has explained, personal information for research purposes will very often entail a use that does not correspond to the original purpose for which the data were collected.[109] For this reason, he believes that, in such cases, legislation must ensure that data subjects completely preserve their rights, meaning that personal information collected for one purpose and subsequently used for research purposes should require informed consent. As a proponent of informational self-determination, Simitis asserts that individuals should have the right to determine whether their information may be used for research and he is critical of approaches to data protection that privilege research. He questions, as lacking credible empirical proof, the oft-repeated mantra by the research community that a consent requirement would increase the costs of research and potentially skew results through reduced sample size and selection bias. On the contrary, he cites experiences in Germany where such protection for the data subject increased both cooperation rates and data reliability.[110]

The deliberate balance between privacy and access, legislated into the provincial health information Acts and the federal PIPEDA, which reflects the tension found within the Hippocratic Oath, discussed at the outset of this paper, demonstrates that all are closer to personal data protection than to privacy. Indeed, it is quite telling that all of these statutes regulate how information may be collected, used, and disclosed, rather than whether such actions should be permitted in the first place.[111] After all, if they were motivated exclusively by a desire to safeguard privacy, they would contain extremely limited access provisions based on explicit consent by the information subject. Put another way, if these statutes were concerned predominantly with privacy, they would privilege this goal, to the near exclusion of access. However, to varying degrees, they all seek to strike a balance between the protection of personal information and access, which is, in fact, consistent with Neill's model. Indeed, although Neill does not explicitly employ the language of access, she does assert, that personal information, including health information, that is not protective of the "sacred self" may legitimately be used for decision-making purposes. Thus, Neill's model helps to explain and make sense of the nature of contemporary medical information protection legislation, including the trade-offs contained within. The relative youth of these Acts means that we currently lack convincing empirical evidence to determine whether the legislated balance goes too far in either direction. Proponents of increased access to medical information forecast improvements to the overall health of the community.[112] Again, however, more rigorous investigation is necessary if we are to determine whether the benefits that purportedly accrue through greater access would offset the potential disadvantages that might adhere to the corresponding necessary reduction in autonomy and control over personal information.

It should be clear from the foregoing analysis and discussion of these federal and provincial enactments that the provincial Acts go beyond the PIPEDA in protecting personal health information. Nonetheless, there are similarities between these federal and provincial laws, in terms of consent requirements and trade-offs between protection and access, which undoubtedly are motivated by desires to keep the broader economy and health sector functioning. For this reason, these statutes might better be considered more about personal data protection than about privacy.

Reconciling Canadian Legislation with Neill's Model

Having established that the Canadian legislation examined in this paper is more aptly considered protective of personal data than privacy, and that the provincial Acts offer more protection of personal health information than does the PIPEDA, a concomitant question arises as to whether the federal and provincial statutes are aligned with Neill's model? If so, where would they be situated on the privacy–personal data protection continuum, that was developed based upon Neill's ontology of privacy rights?

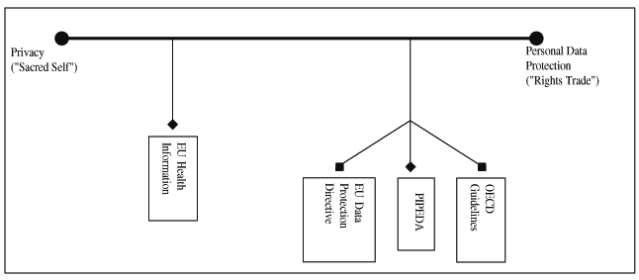
While the PIPEDA does bestow the force of Canadian law upon "fair information practices", it is here argued that the rights outlined by the Act are void of the moral legitimation integral to Neill's privacy model. They do not derive from absolute, static norms based on the innate natural properties of the "sacred self". Instead, the federal Act is strongly motivated by commercial imperatives. This is made most evident by the Act's reliance on the CSA Code, which closely resembles the OECD Guidelines in the latter's attempt to strike a balance between personal data protection and the free flow of information for business purposes. Similarly, the fact that the development and passage of the Act was in large part motivated by concerns about trade between Canada and the EU, as discussed previously, offers further evidence of the commercial elements driving the PIPEDA. Indeed, the preamble to the Act states that the PIPEDA is "[a]n Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances. . . .".[113] Moreover, the stated purpose of Part 1 (Protection of Personal Information in the Private Sector) of the Act is:

> … to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right to privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[114]

Federal privacy protection for personal information in the private sector, therefore assumes an instrumental character, in service of the true legislative goal of facilitating electronic commerce.

The PIPEDA is thus quite candid about its intended purpose and does not presume to safeguard privacy under the rubric of the "sacred self". It is clear that the trade-offs in the legislation endeavour to satisfy competing public policy goals in an attempt to ensure that Canada continues to profit in the "information economy". Rather than appealing to a fundamental sense of privacy and the necessity of ensuring its protection, the Act specifies a purpose of balancing personal data protection against commercial interests. As such, the provisions of the federal Act revolve around what Neill would classify as broad rights to a private life and trade transgressions, and thus, more aptly, are considered protective of personal data rather than the privacy of the "sacred self". Indeed, the rights enumerated by the PIPEDA are certainly not protective of Neill's conception of the "sacred self", but neither do they make that claim. The attempt by the Act to legislate some level of data protection without couching it in terms of a fundamental appeal to the dignity of privacy is certainly in line with Neill's model. For these reasons the PIPEDA would clearly not be positioned at the left side of the privacy–personal data protection continuum. Nonetheless, there remains the question of where to situate this statute *vis-à-vis* the OECD Guidelines and EU Data Protection Directive. Since the federal Act is so closely allied with the OECD Guidelines, the obvious choice for the placement of the former on the continuum is parallel to the latter, as outlined in Figure 4.

Figure 4 — Location of the PIPEDA on the Privacy–Personal Data Protection Continuum



In contrast, the provincial legislative protections offered in respect of personal health information in Canada, are more difficult to align with Neill's model. Moreover, an argument could be advanced that differences in protection between the four statutes warrant separate placement of each, although a systematic explication of the differences between the four provincial Acts goes beyond the scope of this paper. Indeed, since they ultimately all seek to balance protection of personal health information with other policy objectives, it seems realistic to group them together for purposes of this paper.

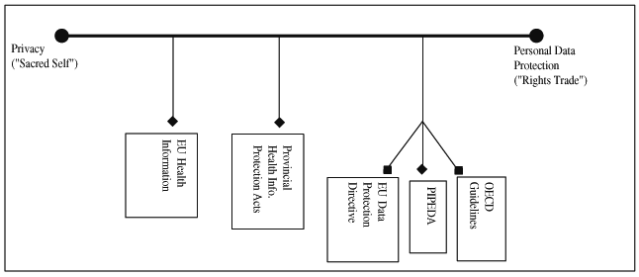
As discussed above, Neill asserts that only information *of* the body, which is considered to reflect the "sacred self", deserves privacy protection. Yet, the medical information that is safeguarded by each of the provincial Acts includes both mental and physical information and is therefore both *of* and *about* the body. According to Neill, however, only the mental health information, *of* the body, would warrant privacy protection based upon an appeal to the "sacred self". Again, it is important to recall that Neill does not argue against providing any protection for physical health information (*about* the body), rather she argues that the justification for any such safeguards must be made with reference to values other than privacy protection. Indeed, the multiple, and seemingly incongruous, policy goals of these provincial health information protection Acts appear to attempt to strike a balance between access and privacy, making it clear that protection of the "sacred self" is not the overarching objective. Instead, each Act appears to consider privacy in terms of its instrumental value. The various provisions of the statutes are premised on utilitarian concerns about maintaining the patient–health care provider relationship, advocating and offering autonomy to individuals over their own information, and perhaps preventing economic harm and the humiliation of individual patients. The exemptions and limitations written into each piece of legislation, which actually reduce privacy protection, are ostensibly designed to benefit society by facilitating information flow within the health care system. Insofar as this concerns physical health information, the provincial Acts align with Neill's model. But the provincial health information protection Acts fail to differentiate between mental and physical health information. Thus, the instrumental treatment of mental health information under the provincial Acts fails to align with a position close to the "sacred self" that Neill would afford this type of information in her model. Based upon the overall wording and effects of the provincial Acts, it can be argued that health protection legislation in Canada finds a place at the fluctuating norms and protection of broad privacy rights level of Neill's ontology. While this allies with Neill's model in terms of the treatment of physical health information, the inclusion of mental health information at this level of protection is difficult to reconcile with her ontology of privacy rights.

Since the provincial health Acts treat both mental and physical health information without making a distinction, it is also difficult to assign them on the privacy–data protection continuum *vis-à-vis* the PIPEDA, EU Data Protection Directive, and OECD Guidelines. A

seemingly obvious solution would be to separate and place physical and mental health information protection at different points on the spectrum, as was done with the EU Data Protection Directive. However, the provincial Acts treat both types of health information similarly, whereas the EU Data Protection Directive confers a distinct status upon health and sex life information. It would therefore be analytically incorrect to split the provincial Acts into different places on the continuum.

Since we have established that none of the provincial laws completely protect the privacy of the "sacred self", although this would be appropriate for mental health information according to Neill's model, an alternative solution might be to locate the provincial Acts at a position adjacent to the other data protection instruments scrutinized in this paper. Indeed, based upon Neill's typology there is nothing about the *physical* health information that these provincial Acts strive to protect that would merit a greater claim to privacy than the commercial information safeguarded by the PIPEDA, EU Data Protection Directive, or OECD Guidelines. Therefore, situating the provincial Acts closer to the data protection side of the continuum would avoid ascribing a special status to *physical* medical information that is not justified by Neill's model. This placement would also certainly account for the competing policy goals of the legislation, which are reflected in the numerous exemptions designed to facilitate access to personal information. However, such a resolution would ignore the provincial protection afforded *mental* health information, which in Neill's model merits privacy protection due to its association with the "sacred self". Given this, and despite the utilitarian nature of the provincial statutes, I would situate the provincial Acts closer to the European Union treatment of health information than to the PIPEDA, EU Data Protection Directive, or OECD Guidelines. By way of qualification, however, the equal treatment given to *physical* health information by the provincial legislation and the fact that the protection afforded *mental* health information is subject to exemptions, militates against placing these Acts to the left side of the European Union health information. In other words, placing the provincial Acts too far to the left on the continuum would seem motivated by an implicit assumption that medical information warrants special attention and protection, as compared to "commercial" information. But according to Neill's model such an assumption would, in general, be wrong and could only be defended in respect of *mental* health information. Yet, precisely because the provincial statutes offer qualified protection to *mental* health information, they must be positioned closer to the privacy protection of the "sacred self" than the other statutes and guidelines already situated on the continuum. To the extent that the provincial Acts cover mental health information but also permit qualified exceptions, they should be positioned between the European Union treatment of health information and the European Union–PIPEDA–OECD Guidelines grouping, as outlined in Figure 5.

Figure 5 — Location of the Provincial Health Information Protection Acts on the Privacy–Personal Data Protection Continuum



Conclusion

This paper has sought to explore the relationship and tension between the privacy and access interests inherent in contemporary legislative mechanisms that regulate the collection, use, and disclosure of personal information in Canada. Elizabeth Neill's ontology of privacy rights provided the theoretical underpinnings to analyze and situate certain Canadian legislation currently involved in regulating this relationship. The explication of Neill's model demonstrated that she considers human dignity to be a metaphor that assumes a dual role; it reflects the innate natural properties of privacy and autonomy, and, based on these original, innate properties, it provides the moral justification for constructing societal norms protective of privacy. This conceptual construct allows Neill to differentiate between the broad right to a private life and narrow rights to inherent privacy and human dignity. The former are protected through conventional fluctuating norms, while the latter are safeguarded by natural, conventional static norms. Transgressions of these static norms, based upon narrow rights, represent violations of innate privacy and the individual dignity of the "sacred self". According to Neill, it is only these rights that warrant protection based upon an appeal to privacy. Broader rights, although certainly susceptible to transgression, may not be defended through reference to privacy. It is precisely this distinction that provided the basis for developing the privacy–data protection continuum, upon which the various legislative devices examined in the paper were situated.

It was found that the privacy protection offered by the OECD Guidelines, the EU Data Protection Directive, and the PIPEDA cannot claim to protect the privacy of the "sacred self". In fact, with perhaps the exception of the European Union treatment of health and sex life information, none of these three data protection instruments asserts a fundamental appeal to the dignity of

privacy as its predominant justification and purpose, which is very much in line with Neill's model. All seek to establish some level of personal data protection while also facilitating trade and commerce. Thus, these statutory devices align more closely with broader claims to privacy, whose ontological status would place them nearer to the data protection side than to the privacy side of the continuum. All were therefore characterized as more protective of personal data than of privacy.

The comparative examination of the PIPEDA and the four provincial Acts in respect of health information demonstrated that while there are similarities, the provinces go further in protecting personal health information than does the federal legislation. Nonetheless, each of the provincial statutes, similar to the PIPEDA, also demonstrated concern with policy goals beyond the protection of privacy. The analysis made it clear that the provincial Acts attempt to balance the protection of personal information against competing policy goals that oftentimes require access to information. Although the provincial Acts demonstrated a utilitarian nature with regard to privacy that aligns with Neill's model, and is similar to the PIPEDA, their dual treatment of mental and physical health information rendered their placement on the privacy–data protection continuum somewhat problematic. Neill's model, which does not privilege medical information *about* the body, would generally require that the provincial Acts be situated closer to personal data protection than to the privacy side of the continuum. However, since all of the provincial statutes offer qualified protection to mental information *of* the body, they also safeguard an element of the "sacred self" and thus privacy. For this reason the provincial Acts were ultimately situated on the left side of the privacy–data protection continuum.

The overall analysis revealed an inherent tension between privacy and access in all data protection laws, although it was most pronounced in the medical information protection statutes. Part of this tension stems from the nature of the medical environment, which depends upon accurate, current and complete health data in order to function effectively. Indeed, patients, health care providers, researchers, policymakers and all others with a stake in the system require quality information in order to make informed decisions. It thus becomes obvious that access to information is an integral part of the health care system in order to facilitate more effective health care provision, to evaluate the quality and cost effectiveness of health services, to monitor abuse and fraud, to track disease, and to research patterns of disease for prevention and treatment purposes. Although such a perspective, which encompasses significant communitarian elements, might perhaps reify system values at the expense of patient rights to privacy, the tension between privacy and access is not as absolute as one might think, since both individual and social imperatives will often intersect in the realm of health information protection.[115]

In this context it became clear that the epistemic strength of Neill's ontology of privacy rights rests with its ability to disentangle the conceptual underbrush associated with the notion of privacy. The guidance offered by her model for determining valid privacy claims helps illustrate whether contemporary privacy legislation is motivated more by privacy or personal data protection concerns. This, in turn, helps to explain why society might accept the trade-offs between data protection and access inherent in all these legislative devices. By effectively identifying the boundaries of what is and what is not privacy, Neill's model helps to debunk some of the rhetoric about the presumed absolute nature of privacy rights that invariably gets caught up in policy discussions about legislative protections. Indeed, by cutting through the rhetoric involved in the debate, Neill helps to bring clarity to the complexity of information policy and its development in the "information age". Perhaps by accepting that privacy has a rather narrow conceptual justification, we can better comprehend the nature and value of the personal data protection legislation being enacted around us. While a libertarian might bristle at the degree to which communitarians, like Etzioni, emphasize social virtue at the expense of individual autonomy, this type of analysis does highlight an important aspect of public policy development; namely, that societies are almost always unable to make perfect choices since there will usually be a degree to which one interest trumps another. This is the area where Elizabeth Neill's work could prove most useful; by delineating the bounds of what qualifies as a legitimate privacy claim, her model might bring clarity to the public policy process in which legislators must respond to competing demands for protection and access.

Notes:

[1] cf. Paul S. Appelbaum, "Privacy in Psychiatric Treatment: Threats and Responses" (2002) 159 American Journal of Psychiatry 1809, in which Appelbaum discusses the importance of privacy in the context of psychiatric counselling. Lawrence Gostin discusses the tension between ensuring patient privacy and the goals and needs of the health care system in Lawrence O. Gostin, "Health Information Privacy" (1995) 80 Cornell L. Rev. 451. Peter Jacobson has also analyzed the difficulty of balancing patient privacy and the information needs of the medical system in Peter D. Jacobson, "Medical Records and HIPAA: Is It Too Late To Protect Privacy?" (2002) 86 Minn. L. Rev. 1497.

[2] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1981) [OECD Guidelines].

[3] EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data*, [1995] O.J. L. 281/31 [EU Data Protection Directive].

[4] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [PIPEDA].

[5] Elizabeth Neill, *Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self* (Montreal: McGill Queen's University Press, 2001).

[6] *Ibid.* at 5.

[7] *Ibid.* at 7.

[8] *Ibid.*

[9] *Ibid.* at 26.

[10] *Ibid.* at 55.

[11] Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 N.Y.U.L. Rev. 962.

[12] Neill, *supra* note 5 at 126.

[13] Neill, *supra* note 5 at 135.

[14] Neill, *supra* note 5 at 133–139.

[15] Neill, *supra* note 5 at 148.

[16] Margaret Ann Wilkinson, "Privacy and Personal Data Protection: Albatross for Access?" in Karen G. Adams & William F. Birdsall, eds., *Access to Information in a Digital World* (Ottawa: Canadian Library Association, 2004) 109. Wilkinson has concluded that Canadian legislation is best characterized as protective of personal data protection rather than privacy. For this reason, she opines that confidentiality, rather than privacy, may provide the more appropriate conceptual framework for interpreting personal data protection legislation in this country.

[17] cf. Colin J. Bennett & Charles D. Raab, "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response" (1997) 13 The Information Society 245; Simon Davies, "Spanners in the Works: How the Privacy Movement is Adapting to the Challenge of Big Brother" in Colin J. Bennett & Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) 244.

[18] Philip E. Agre & Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (Cambridge, Mass.: MIT Press, 1997); Colin J. Bennett & Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).

[19] OECD Guidelines, *supra* note 2.

[20] The knowledge or consent provisions of the first principle are not absolute in order to allow for cases where consent is impracticable, such as in police investigations or to allow for the possibility of a data subject being represented by another party.

[21] OECD Guidelines, *supra* note 2.

[22] EU Data Protection Directive, *supra* note 3.

[23] Spiros Simitis, "From the Market to the Polis: The EU Directive on the Protection of Personal Data" (1995) 80 Iowa L. Rev. 445.

[24] Bennett & Raab, *supra* note 17.

[25] EU Data Protection Directive, *supra* note 3, art. 2.

[26] Bennett & Raab, *supra* note 17.

[27] EU Data Protection Directive, *supra* note 3, art. 3(2).

[28] EU Data Protection Directive, *supra* note 3, art. 6(1)(*b*).

[29] EU Data Protection Directive, *supra* note 3, arts. 6(1)(*d*)-(*e*).

[30] EU Data Protection Directive, *supra* note 3, art. 7.

[31] EU Data Protection Directive, *supra* note 3, art. 14(*a*).

[32] EU Data Protection Directive, *supra* note 3, art. 14(*b*).

[33] EU Data Protection Directive, *supra* note 3, art. 17(1).

[34] EU Data Protection Directive, *supra* note 3, arts. 17(2)-(3).

[35] EU Data Protection Directive, *supra* note 3, arts. 10(*a*)–(*c*).

[36] EU Data Protection Directive, *supra* note 3, art. 18(1).

[37] EU Data Protection Directive, *supra* note 3, art. 12(*a*).

[38] EU Data Protection Directive, *supra* note 3, art. 12(*b*).

[39] EU Data Protection Directive, *supra* note 3, art. 12(*c*).

[40] EU Data Protection Directive, *supra* note 3, art. 8(1).

[41] EU Data Protection Directive, *supra* note 3, arts. 8(2)-(3).

[42] EU Data Protection Directive, *supra* note 3, art. 8(4).

[43] *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221 [ECHR].

[44] European Data Protection Supervisor, *Public access to documents and data protection* (Brussels: European Communities, 2005).

[45] Although the ECHR is ostensibly concerned with offering protection against state transgressions of human rights, Bygrave marshals a number of other works that support his assertion that article 8 of the ECHR covers data processing activities executed in the private sector. Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties" (1998) 6 Int'l J.L. & I.T. 247.

[46] EU Data Protection Directive, *supra* note 3, art. 28(3).

[47] S.C. 1976-77, c. 33.

[48] S.C. 1980-81-82-83, c. 111, Sch. II.

[49] On July 1, 1983, the same day that the *Privacy Act* was proclaimed effective, Part IV of the *Canadian Human Rights Act* was repealed. The entire ambit of rights protected by the latter Act was codified in the new *Privacy Act* and the *Access to Information Act*, R.S.C. 1980-81-83-83, c. 111, Sch. I, which also came into force on July 1, 1983. See Shirish Pundit Chotalia, *The 1999 annotated Canadian Human Rights Act* (Scarborough: Thomson, 1998).

[50] British Columbia passed its *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 in 1992. Alberta passed the *Freedom of Information and Protection of Privacy Act*, S.A. 1994, c. F-18.5, in 1994, which was subsequently included in the Revised Statutes of Alberta in 2000: R.S.A. 2000, c. F-25. Saskatchewan passed its own *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, in 1990. Manitoba assented to its *Freedom of Information and Protection of Privacy Act*, S.M. 1997, c. 50, C.C.S.M. c. F175, in 1997, which replaced *The Freedom of Information Act*, S.M. 1985-86, c. 6. Ontario passed its *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, in 1987. Public sector privacy in Quebec is safeguarded by *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, R.S.Q. c. A-2.1, adopted in 1982. New Brunswick has enjoyed public sector privacy protection since 1998 when its *Protection of Personal Information Act*, S.N.B. 1998, c. P-19.1, was passed. Prince Edward Island passed its *Freedom of Information and Protection of Privacy Act*, S.P.E.I. 2001, c. 37, in 2001. Nova Scotians are protected by their provincial *Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, c. 5, passed in 1993. With the exception of Part IV (Protection of Privacy), which has yet to be proclaimed, Newfoundland's *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1, went into force in January 2005. The Northwest Territories and Nunavut are protected by the *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20, passed in 1994 and which went into effect on December 31, 1996. Under section 76.05 of the *Nunavut Act*, S.C. 1993, c. 28, Nunavut adopted the same Act under its own jurisdiction as of April 1, 1999. The Yukon, in 1995, also passed an *Access to Information and Protection of Privacy Act*, S.Y. 1995, c. 1, that was proclaimed on July 1, 1996. This Act was repealed and replaced by R.S.Y. 2002, c. 1.

[51] Canada, Parliament, "Bill C-6: Personal Information Protection and Electronic Documents Act: Legislative History of Bill C-6" by John Craig in *Library of Parliament (Legislative Summaries)* LS-344E (1999-2000) at para. 8, online: Parliament of Canada <http://www.parl.gc.ca/common/Bills_ls.asp?lang=E&Parl=36&Ses=2 &ls=C6&source=Bills_House_Government>.

[52] EU Data Protection Directive, *supra* note 3.

[53] EC, *2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, [2002] O.J. L. 002/13, online: Europa <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002D0002&model=guichett>.

[54] Standing Senate Committee on Social Affairs Science and Technology, *Proceedings of the Standing Senate Committee on Social Affairs, Science and Technology: Issue 6 — Second and Third Reports of the Committee* (Ottawa: Public Works and Government Services Canada, 1999).

[55] Section 91(2) of the *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5, which confers responsibility for inter-provincial trade and commerce upon the federal government, is often referred to as the so-called "commercial clause".

[56] The province of Quebec initiated a constitutional challenge against the PIPEDA on December 17, 2003. Although, as of writing, the Quebec Court of Appeal had not yet issued a ruling, it seems reasonable to

assume that, given the nature of this challenge, it will make its way up to the Supreme Court of Canada.

[57] PIPEDA, *supra* note 4, s. 2(1).

[58] Canadian Institutes of Health Research, *Personal Information Protection and Electronic Documents Act: Questions and Answers for Health Researchers* (Ottawa: Public Works and Government Services Canada, 2001), online: Canadian Institutes of Health Research <http://www.cihr-irsc.gc.ca/e/pdf_14391.htm>.

[59] Paragraph 26(2)(*b*) of the PIPEDA states that "[t]he Governor in Council may, by order, if satisfied that legislation of a province that is substantially similar to this Part [1 — Protection of Personal Information in the Private Sector] applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province": PIPEDA, *supra* note 4.

[60] Section 72 of the PIPEDA states that "[p]arts 1 to 5 or any provision of those Parts come into force on a day or days to be fixed by order of the Governor in Council made on the recommendation of (a) in the case of Parts 1 [Protection of Personal Information in the Private Sector] and 2 [Electronic Documents] or any provision of those Parts, the Minister of Industry; and (b) in the case of Parts 3 to 5 or any provision of those Parts, the Minister of Justice": PIPEDA, *supra* note 4. Similarly, the process outlined in the *Canada Gazette* for determining "substantially similar" legislation, though not a rule of law, does make it quite clear that the Governor in Council will only issue orders based upon recommendations made by the Minister of Industry: Personal Information and Protection of Electronic Documents Act: Process for the Determination of Substantially Similar Provincial Legislation by the Governor in Council, C. Gaz. 2002. I. 2385 [*Canada Gazette*, "Substantially Similar"].

[61] Under the system of "responsible government" in Canada, the cabinet is in most cases the supreme executive authority. Moreover, since it draws its ministers from the legislative branch (Parliament) and controls the Parliament, "responsible government" in Canada does not entail a "separation of powers". The Prime Minister, who is able to appoint, promote, demote, and dismiss ministers, ultimately controls the cabinet. The cabinet plans the legislative agenda for each session of Parliament, with significant power being exercised by the Prime Minister. The cabinet or one of its committees makes decisions, which are then sent as "orders" or "minutes" to the Governor General for signature. In the case where a particular act, such as the PIPEDA, requires that a specific minister make a decision, it is still the cabinet that makes the decision, which is then formally authenticated by the specified minister. Although the cabinet will often delegate a number of issues to individual ministers for the sake of expediency, every minister accepts that the cabinet may exercise its supreme authority if it so chooses. It thus becomes clear, that the executive branch and not the legislative branch, has the right to designate which minister will be responsible for which act: Peter W. Hogg, *Constitutional law of Canada*, 2003 student ed. (Scarborough, Ont.: Thomson Carswell, 2003).

[62] *Canada Gazette*, "Substantially Similar", *supra* note 60.

[63] *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sch. A [PHIPA].

[64] Personal Information and Protection of Electronic Documents Act: Health Information Custodians in the Province of Ontario Exemption Order, C. Gaz. 2005. I. 331 [*Canada Gazette*, "Health Information Custodians"].

[65] Although Alberta's *Health Information Act*, R.S.A. 2000, c. H-5 [HIA], has not been recognized as being "substantially similar", the province's broader *Personal Information Protection Act*, S.A. 2003, c. P-6.5, has been deemed equivalent to the PIPEDA. Therefore, the health care sector must abide by this latter Act until the former is recognized as being "substantially similar".

[66] *Canada Gazette*, "Substantially Similar", *supra* note 60; *Canada Gazette*, "Health Information Custodians", *supra* note 64.

[67] Canadian Standards Association, *Model Code for the Protection of Personal Information* (Toronto: CSA, 1996) CAN/CSA-Q830-96.

[68] PIPEDA, *supra* note 4.

[69] PIPEDA, *supra* note 4, s. 7(1).

[70] PIPEDA, *supra* note 4, s. 7(2).

[71] The exemptions for use and disclosure of information without consent for statistical, or scholarly study or research also require that the information can only be used or disclosed if 1) the purposes cannot otherwise be achieved, 2) it is impracticable to obtain consent, and 3) the organization informs the Privacy Commissioner before using or disclosing the information. The notification requirement notwithstanding, the Privacy Commissioner has no power to prevent use or disclosure.

[72] PIPEDA, *supra* note 4, s. 7(3).

[73] PIPEDA, *supra* note 4, s. 9.

[74] PIPEDA, *supra* note 4, ss. 11-12.

[75] *Health Information Act*, R.S.A. 2000, c. H-5 [HIA].

[76] *Health Information Protection Act*, S.S. 1999, c. H-0.021 [HIPA].

[77] *Personal Health Information Act*, S.M. 1997, c. 51, C.C.S.M. c. P33.5 [PHIA].

[78] PHIPA, *supra* note 63.

[79] *Canada Gazette*, "Health Information Custodians", *supra* note 64.

[80] HIA, *supra* note 75, s. 2; HIPA, *supra* note 76, Preamble; PHIA, *supra* note 77, s. 2; PHIPA, *supra* note 63, s. 1.

[81] In Alberta's statute, "non-identifying" information is defined in paragraph 1(1)(*r*) as health information from which "the identity of the individual who is the subject of the information cannot be readily ascertained from the information". This type of information can generally be collected, used, and disclosed without restrictions as the majority of the Act applies to "individually identifying" information. The other provincial statutes actually define personal health information and although the definition set forth in paragraph 2(*m*) of Saskatchewan's HIPA is fairly broad, paragraph 3(2)(*a*) limits the scope of the Act so that it does *not* apply to "statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified". Subsection 1(1) of Manitoba's PHIA defines "personal health information" as "information about an identifiable individual . . ." and section 3 of the Act states that "[t]his Act does not apply to anonymous or statistical health information that does not, either by itself or when combined with other information available to the holder, permit individuals to be identified". Similarly, Ontario's PHIPA defines "personal health information" in section 4 as ". . . identifying information about an individual. . . .".

[82] HIA, *supra* note 75, paragraphs 1(1)(*i*), 1(1)(*k*); HIPA, *supra* note 76, paragraph 2(*m*); PHIA, *supra* note 77, s. 1(1); PHIPA, *supra* note 63, s. 4(1).

[83] HIA, *supra* note 75, ss. 19, 26, 32. In cases of disclosure to a non-custodian, the Information and Privacy Commissioner must be notified before any data matching procedures may be executed.

[84] HIA, *supra* note 75, paragraph 1(1)(*t*).

[85] HIPA, *supra* note 76, paragraph 2(*t*); PHIA, *supra* note 77, s. 1(1).

[86] PHIPA, *supra* note 63, s. 3.

[87] HIA, *supra* note 75, ss. 60-61; HIPA, *supra* note 76, ss. 16–22; PHIA, *supra* note 77, ss. 16–19; PHIPA, *supra* note 63, ss. 10–14.

[88] HIA, *supra* note 75, s. 22(2); PHIA, *supra* note 77, s. 15.

[89] HIPA, *supra* note 76, s. 6; PHIPA, *supra* note 63, ss. 8, 29.

[90] See *supra* note 81 and accompanying text.

[91] See *supra* note 83 and accompanying text.

[92] HIA, *supra* note 75, ss. 25–27; HIPA, *supra* note 76, s. 26; PHIA, *supra* note 77, s. 21; PHIPA, *supra* note 63, s. 37.

[93] HIA, *supra* note 75, s. 27.

[94] HIPA, *supra* note 76, paragraph 27(4)(*g*); PHIA, *supra* note 77, paragraph 21(*d*);PHIPA, *supra* note 63, ss. 45(1), 47(2).

[95] David T.S. Fraser (McInnes Cooper), *The Application of PIPEDA to Personal Health Information* (2004) at 5, online: Dalhousie University: University Computing and Information Services <http://myweb.dal.ca/fraserdt/privacy/pipeda_and_personal_health_information.pdf>.

[96] Ontario Information and Privacy Commissioner, *Submission to the Standing Committee on General Government: Bill 159, Personal Health Information Privacy Protection Act, 2000* (2001) at 11, online: Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca/userfiles/page_attachments/phipa-01.pdf>.

[97] Mary Marshall & Barbara von Tigerstrom, "Health Information" in Jocelyn Downie, Timothy Caulfied & Colleen M. Flood, eds., *Canadian Health Law and Policy*, 2d ed. (Toronto: Butterworths, 2002) 157.

[98] PHIA, *supra* note 77, paragraph 22(2)(*a*).

[99] PHIPA, *supra* note 63, paragraph 38(1)(*a*).

[100] HIPA, *supra* note 76, paragraph 27(4)(*j*).

[101] HIPA, *supra* note 76, s. 27(6).

[102] HIPA, *supra* note 76, paragraph 29(2)(*c*).

[103] PHIA, *supra* note 77, s. 24; PHIPA, *supra* note 63, s. 44.

[104] HIA, *supra* note 75, s. 7–17; HIPA, *supra* note 76, ss. 31–40; PHIA, *supra* note 77, ss. 5–12; PHIPA, *supra* note 63, ss. 51–55.

[105] Ontario Information and Privacy Commissioner, *supra* note 96.

[106] Richard Steinecke, "More Workable Consent Procedures Under New Privacy Legislation" *Dialogue* (September/October 2004) at para. 3, online: The College of Physicians & Surgeons of Ontario <http://www.cpso.on.ca/publications/dialogue/0904/privacy.htm>.

[107] Lawrence O. Gostin, "Health Information Privacy" (1995) 80 Cornell L. Rev. 451.

[108] *Ibid.*

[109] Simitis, *supra* note 23.

[110] *Ibid.*

[111] Wilkinson, *supra* note 16.

[112] cf. Gostin, *supra* note 107; Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999).

[113] PIPEDA, *supra* note 4.

[114] PIPEDA, *supra* note 4.

[115] Mark Weitz *et al.*, "In Whose Interest? Current Issues in Communicating Personal Health Information: A Canadian Perspective" (2003) 31 J.L. Med. & Ethics 292.