# Wired Identities: Retention and Destruction of Personal Health Information in an Electronic World[*]

Elaine Gibson

> In my view, self-identity is central to human existence…the essence of this discussion is that privacy mechanisms define the limits and boundaries of the self. When the permeability of those boundaries is under the control of a person, a sense of individuality develops. But it is not the inclusion or exclusion of others that is vital to self-definition; it is the ability to regulate contact when desired…Thus privacy mechanisms serve to help define me.[1]

## Introduction

Our identities are to a significant degree both embedded in and shaped by personal information concerning ourselves. Health information concerns arguably the most sensitive and intensely personal aspects of ourselves, and thus is a fundamental aspect of identity. How we choose to be known or not known, the health information we reveal or don't reveal based on how we think others will identify or 'label' us, and the ways in which we reinvent ourselves over time are all powerful ways in which we control aspects of our identity. The topic of retention has received considerable attention within Canadian legislation and policies designed to ensure the protection of personal health information. The flip side of retention, i.e. that of destruction, has received very little attention to date. Statutes and policies mention destruction in passing, but its parameters and the reasons for requiring it have not been supplied, and there has been a dearth of discussion at a conceptual level in the academic literature. Yet the issue of destruction of personal information is of vital importance to the ability to control the shaping of our identity.

The world is changing dramatically as information shifts to electronic form. The value of personal health information has increased significantly in both monetary and non-monetary terms in recent decades. And with the digitization of information, pragmatic aspects of indefinite retention become solveable. There are a number of arguments that favour indefinite retention for the benefit of ourselves, our offspring, and future society. However, it is the premise of this paper that, especially in light of the shift to digitization, the need to protect privacy and confidentiality requires a greater emphasis on destruction as an important aspect of the safeguarding of personal health information. This in turn, I argue, is a necessary ingredient in the preservation of identity.

The first part of this paper briefly outlines the need for and importance of retention of personal health information, followed by examination of the need for destruction. It then provides an overview of laws and policies in Canada pertaining to retention and destruction of personal health information. This is followed by a discussion of the impact of digitization and its profound alteration of the world of personal health information. My analysis covers autonomy, information as a public good, inequality, and privacy

---

[*] I am grateful to be recipient of the Charles D. Gonthier Fellowship from the Canadian Institute for the Administration of Justice. Financial support from the CIAJ aided in the development of this paper. I am also grateful for the excellent research assistance provided by Ilana Luther.

[1] Irwin Altman, *The Environment and Social Behaviour: Personal Space, Privacy, Crowding and Territory* (Monterey: Brooks/Cole Publishing Company, 1975) at 50.

as a social good. I then offer tentative proposed directions for setting destruction policies, developed through the lens of identity.

The substance of this discussion is confined to physicians and surgeons, but suffice to say that the various health professions have similarly vague and differing provisions in their governing legislation as to retention and destruction.[2] Also note that throughout this paper I am discussing personal health information, i.e., information that is identifiable or potentially identifiable in combination with other information. Information that is anonymized[3] is not imbued with identical privacy concerns; however, once information is truly anonymized, it loses much of its value.[4] Genetic information presents a particular conundrum in the context of anonymization in that it is unique to the individual and therefore can never be truly anonymized.[5] Furthermore, information considered to be anonymized can sometimes be de-anonymized through electronic-information-savvy endeavours.[6] As a last point, even if truly anonymized, the information is still embedded with a remote yet discernable privacy aspect.[7]

---

[2] For example, pharmacists in Canada have retention requirements ranging from 2 years (*Pharmacy Act*, RSPEI 1988, c P-6.1, s 29(a)) to 15 years (New Brunswick College of Pharmacists, *Regulations of the New Brunswick College of Pharmacists* (May 2014) at s 17.22(1), online: New Brunswick College of Pharmacists: <http://www.nbpharmacists.ca/>), with no stated requirement in Nova Scotia.

[3] See definition of anonymized information in Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (December 2010) at 57: "Anonymized information – the information is irrevocably stripped of direct identifiers, a code is not kept to allow future re-linkage, and risk of re-identification of individuals from remaining indirect identifiers is low or very low".

[4] Identifiable personal health information may be required, however, in order to fully understand reasons behind certain patient behaviors: see William Crown, "Characteristics of the Marketplace for Medical Care Data" in "Chapter 4: Healthcare Data: Public Good or Private Property?" in Claudia Grossman, ed, *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good* (Washington, National Academies Press, 2010) at 147-149.

[5] See Bahrad A Sokhansanj, "Beyond Protecting Genetic Privacy: Understanding Genetic Discrimination Through Its Disparate Impact on Racial Minorities" (2012) 2 Colum J Race & L 279 at 282-286; Amy L McGuire, "Identifiability of DNA Data: The Need for Consistent Federal Policy" (2008) 8:10 Amer J of Bioethics 75 at 75. McGuire explains:

> DNA is itself uniquely identifiable (McGuire and Gibbs 2006a, 2006b). In 2004, Zhen Lin and colleagues illustrated that access to just 30–80 statistically independent single nucleotide polymorphisms (SNPs) was sufficient to uniquely identify an individual (Lin, Owen, and Altman 2004). Recently, Homer and colleagues demonstrated that an individual's SNP profile could potentially be identifiable even when it is aggregated with 1,000 or more other samples (Homer et al. 2008).

[6] Amitai Etzioni, "A Liberal Communitarian Conception of Privacy" (2012) 29:3 J Marshall J Comp & Info L 419 at 459-60.

[7] Elaine Gibson, "Is There a Privacy Interest in Anonymized Personal Health Information?" (2003) Health LJ at 97. This conversation is taken further by Bahrad A Sokhansanj, who discusses how the use of even anonymized information for research purposes can impact negatively on African Americans, see Bahrad A Sokhansanj, "Beyond Protecting Genetic Privacy: Understanding Genetic Discrimination Through Its Disparate Impact on Racial Minorities" (2012) 2 Colum J Race & L 279.

Retention and Destruction

Retention of personal health information is a positive undertaking for individuals and for society in a number of ways. First, health professionals have an ethical obligation toward their patients to hold their information in trust for an extended period of time.[8] This obligation attempts to ensure that a historical record of one's health status, tests ordered, and treatments received is available for the subsequent provision of care.[9] Retention also enables review for purposes of billing, quality assurance, and regulation.[10] As well, records have become highly valuable to enable the conduct of research and epidemiology or tracking of health and disease.[11] The information may also be required for purposes of litigation, and a substantial period of time may elapse before an injury that may be the cause of a lawsuit comes to light or the full extent of the injury is revealed.[12] Our present societal preoccupation with genetic and social influences on our lives leads to claims of the need to know our family histories and influences, including the health status of family members.[13] Also there is archival significance in our health records. These significant factors lean toward retention of information for as long as possible if not in perpetuity.

Reasons for retention are manifest and plentiful. The justifications in favour of destruction are fewer in number but nevertheless powerful. I will discuss two: cost and privacy. First, there is a cost to retaining information in that it requires space – historically, with paper records, a great deal of space. Second are issues of privacy and confidentiality.[14] In a nutshell, the longer information is retained, the greater the likelihood that it will be accessed by and/or disseminated to a range of individuals and organizations,

---

[8] *McInerney v MacDonald*, [1992] 2 SCR 138 at para 22.

[9] Lorne Elkin Rozovsky & Noela J Inions, *Canadian Health Information: A Practical Legal and Risk Management Guide*, 3d ed (Markham: Butterworths, 2002) at 7.

[10] Elaine Gibson, "Health Information: Confidentiality and Access" in Jocelyn Grant Downie, Timothy A Caulfield and Colleen M Flood, eds *Canadian Health Law and Policy*, 4th ed (Markham: LexisNexis Canada, 2011).

[11] Don Willison, Elaine Gibson & Kim McGrail, "A Roadmap to Research Uses of Electronic Health Information" in Colleen M Flood, ed, *Data Data Everywhere: Access and Accountability?* (Montreal: McGill-Queen's University Press, 2011) at 233-251.

[12] John J Morris & Cynthia D Clarke, *Law for Canadian Health Care Administrators*, 2d ed (Markham: LexisNexis Canada, 2011) at 102.

[13] See, for example, Juliet Ruth Guichon, Ian Mitchell, and Michelle Giroux, eds, *The Right to Know One's Origins: Assisted Human Reproduction and the Best Interests of Children* (Brussels: Academic and Scientific Publishers, 2012); Michelle Giroux and Mariana De Lorenzi, "Putting the Child First": A Necessary Step in the Recognition of the Right to Identity, (2011) 27 Can J Fam L 53; Vanessa Gruben and Daphne Gilbert, "Donor Unknown: Assessing the Section 15 Rights of Donor-Conceived Offspring," (2011) 27 Can J Fam L 247.

[14] For purposes of this discussion, privacy may be considered the entitlement of the individual or group to keep aspects of themselves away from being exposed. Confidentiality is the obligation of another to keep secret information that has been conveyed to him/her. These definitions are elaborated on in Elaine Gibson, "Public Health Information Privacy and Confidentiality" in Tracey M Bailey, Timothy Caulfield & Nola M Ries, eds, *Public Health Law & Policy in Canada*, 2d ed (Markham: LexisNexis Canada, 2008) 91-132 at 92-93.

and the possibility that it will be inappropriately used multiplies. This gives rise to acute privacy concerns. And one's assessment of the relative value of privacy implicitly informs one's view as to the nature and rigour of destruction requirements.

Late in the 19th century Warren and Brandeis published a foundational piece on privacy law.[15] They outlined what they viewed as then-modern incursions into one's private life. The incursions that were the subject of concern included 'instantaneous cameras', 'numerous mechanical devices', and the widespread circulation of newspapers, the latter's social gossip columns being seen as particularly egregious. In response, they developed the concept of a nascent right to privacy, identified broadly as the 'right to be let alone'.

Warren and Brandeis published their article in 1890. A somewhat similar contemporary formulation is the newly-established 'right to be forgotten'.[16] The European Court earlier this year determined that there is value in being able to choose not to have personal information available to others in perpetuity.[17]

The ability to control the shaping of our identity in significant respects, including the right to be let alone, the right to be forgotten, and other significant aspects of the right to privacy and confidentiality militate against the retention of personal health information indefinitely or in perpetuity. And destruction is the sole guaranteed method of preventing a breach of confidentiality.

Laws and Policies

The federal government first enacted legislation with the aim of ensuring the protection of information held by public institutions, and the provinces followed suit. Private sector legislation has since been enacted at both the federal and provincial levels regulating either personal health information specifically or personal information more broadly. The legislation provides for the retention of information but, as we shall see, contains little guidance on the need for destruction of health records. The remainder of this discussion focusses on private sector legislation and policies.

Physicians and surgeons in private practice in Canada fall under the auspices of the federal Personal Information Protection and Electronic Documents Act (PIPEDA) by virtue of their engagement in

[15] Samuel D Warren and Louis D Brandeis, "The Right to Privacy" (Dec 15, 1890) 4:5 Harvard LR 193-220.

[16] *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12), online: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

[17] Discussed further *infra* in section on 'Privacy as a Social Good'.

commercial activity.[18] Physicians and surgeons are also[19] subject to provincial legislation that has been enacted to regulate private sector information, either healthcare-specific or private-sector information more broadly, in all jurisdictions with the exception of P.E.I. and the territories.[20]

Schedule 1 Principle 5 of PIPEDA indicates that information is to be retained only for so long as is necessary to fulfil the purposes for which it was collected,[21] following which it is to be "destroyed, erased, or made anonymous".[22] Organizations are responsible for the development of guidelines and procedures for retention and destruction.[23] Note that these provisions within PIPEDA are ambiguous and contain no suggested time frames. Instead of providing clear guidance in the legislation and regulations, decision-making as to how to operationalize the responsibilities of retention and destruction is downloaded to individual organizations.

Provincial legislatures have adopted varying requirements and approaches to retention and destruction. Most provincial information legislation in Canada either authorizes the making of regulations concerning retention[24] or mandates that organizations are to develop policies and implement procedures.[25] Thus,

---

[18] Commercial activity is defined in the Act as "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": SC 2000, c 5, s 2(1) [*PIPEDA*]. Note that hospitals are presumptively excluded from PIPEDA: Canada, Industry Canada, *PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector: Questions & Answers*, at 1, online: Industry Canada <https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/PARTS_QandA-e.pdf/$FILE/PARTS_QandA-e.pdf>.

[19] If provincial legislation has been declared substantially similar to PIPEDA, PIPEDA applies only to information going into and out of the province and to information collected, used or disclosed in connection with the operation of a federal work, undertaking or business. See *PIPEDA*, s 26(2)(b).

[20] Alberta *Personal Information Protection Act*, SA 2003, c P-6.5; Alberta *Health Information Act*, RSA 2000, c H-5; British Columbia *Personal Information Protection Act*, SBC 2003, c 63; Saskatchewan *Health Information Protection Act*, SS 1999, c H-0.021; Manitoba *Personal Health Information Act*, CCSM c P33.5; Quebec *An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR, c P-39.1; Ontario *Personal Health Information Protection Act,* SO 2004, c 3, Schedule A; New Brunswick *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; Nova Scotia *Personal Health Information Act*, SNS 2010, c 41; Newfoundland and Labrador *Personal Health Information Act*, SNL 2008, c P-7.01.

[21] That is, unless there has been a request for personal information; see *PIPEDA*, s 8(8).

[22] *PIPEDA*, Schedule 1, s 5, 4.5.3.

[23] *PIPEDA*, Schedule 1, s 5, 4.1.4.

[24] Alberta *Health Information Act*, RSA 2000, c H-5, s 108(1)(o); Saskatchewan *Health Information Protection Act*, SS 1999, c H-0.021, s 63(1)(i); ; Quebec *An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR, c P-39.1, s 90. Note that such regulations have rarely been made.

[25] Alberta *Personal Information Protection Act*, SA 2003, c P-6.5, s 35; British Columbia *Personal Information Protection Act*, SBC 2003, c 63, s 35; Manitoba *Personal Health Information Act*, CCSM c P33.5, s 17(1); Ontario *Personal Health Information Protection Act,* SO 2004, c 3, Schedule A, s10; New Brunswick *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s 55(1); Nova Scotia *Personal Health Information Act*, SNS 2010, c 41, s 50; Newfoundland and Labrador *Personal Health Information Act*, SNL 2008, c P-7.01, s 13(2).

similarly to in PIPEDA, primary responsibility is shifted from the provincial government level to the organizations themselves. I will first discuss regulations/policies concerning retention and then destruction.

a) Retention

Each province has legislation establishing a governing College for physicians and surgeons, and every College has provisions requiring the retention of records. The basic time period for mandated retention ranges from 5 years from date of last entry in Quebec[26] through 6 in Saskatchewan[27] to 10 in most provinces.[28] British Columbia is the clear outlier, having increased its requirements in 2014 from 5 to 16 years.[29] These periods are increased for minors, for whom varying additional times are added for retention, ranging from 2 years past age of majority in Alberta and Saskatchewan[30] to 16 additional years past age of majority in British Columbia.[31] Quebec has no requirement for additional retention in case of minors. The rationale for this high degree of variance from province to province is unclear other than the fact that retention needs to at minimum mirror limitation periods for bringing civil action, which also differ between provinces. Note that these retention periods are identified as minimums; by

---

[26] *Regulation Respecting Records, Places of Practice and the Cessation of Practice by a Physician*, RRQ, c M-9, r 20.3, s 12.

[27] College of Physicians & Surgeons of Saskatchewan, *Bylaw 23.1 Medical Records*, s (f), online: College of Physicians & Surgeons of Saskatchewan <http://www.sma.sk.ca/data/1/rec_docs/696_CPSS_Bylaw_23.pdf>.

[28] See for example, *Medicine Act*, General O Reg 114/94, s 19(1); The College of Physicians and Surgeons of Prince Edward Island, *The Application of the Principles of Privacy*, "Preservation of Information", online: The College of Physicians and Surgeons of Prince Edward Island <http://cpspei.ca/wp-content/uploads/2013/11/Privacy-Principles-P-Apr-2004.pdf>; College of Physicians & Surgeons of Nova Scotia, *Guidelines for Medical Record-Keeping,* (6 June 2008) at s 8.1, online: College of Physicians & Surgeons of Nova Scotia <http://www.cpsns.ns.ca/portals/0/guidelines-policies/2008-medical-record.pdf>.

[29] College of Physicians & Surgeons of British Columbia, Bylaws (1 June 2009) at s 3-6(2), online: College of Physicians and Surgeons of British Columbia <https://www.cpsbc.ca/files/pdf/HPA-Bylaws.pdf>.

[30] College of Physicians & Surgeons of Alberta, *Administration of Practice: Patient Records* (3 April 2014) at s 9, online: College of Physicians & Surgeons of Alberta: <http://www.cpsa.ab.ca/Libraries/standards-of-practice/patient-records.pdf?sfvrsn=2>; College of Physicians and Surgeons of Saskatchewan, *Bylaw 23.1 Medical Records*, at (f), online: College of Physicians and Surgeons of Saskatchewan <http://www.sma.sk.ca/data/1/rec_docs/696_CPSS_Bylaw_23.pdf>.

[31] College of Physicians & Surgeons of British Columbia, Bylaws (1 June 2009) at s 3-6(2), online: College of Physicians and Surgeons of British Columbia <https://www.cpsbc.ca/files/pdf/HPA-Bylaws.pdf>. This mandated time frame far exceeds the Canadian Medical Protective Association (medical liability defence organization) general recommendation of a minimum ten-year retention (plus ten years from age of majority).

inference, unless there is a specified requirement for destruction following the retention period, the information may be held for a longer period of time.[32]

This variability in guidance may simply reflect confusion, or it may be seen to reflect differing conceptions of privacy informing the legislature or organization. The extending of minimum retention periods is clearly and understandably driven by the need for evidence in case of an eventual civil claim. However, the fact that this extension is justifiable does not in turn provide justification for a lack of specificity in the eventual need for destruction.

b) Destruction

Despite wide variation and ambiguity, at least the requirements for retention are addressed in every jurisdiction, unlike for destruction. Most of the Colleges of Physicians and Surgeons outline the required methods for destruction if the records are being destroyed. However, in terms of whether destruction is actually required in and of itself, requirements of the various Colleges vary widely. The Colleges of Physicians and Surgeons in Alberta[33] and Saskatchewan[34] have no provisions concerning destruction. New Brunswick, Ontario, and Quebec provide that information 'may' be destroyed; there is no requirement for destruction. Manitoba's legislation[35] refers physicians over to the Personal Health Information Act, which states: "A trustee shall establish a written policy concerning the retention and destruction of personal health information and shall comply with that policy."[36] Thus, trustees of information are to develop their own policies.

The College in Prince Edward Island indicates that "(p)aper records no longer needing to be maintained should be destroyed by burning or shredding…electronic records are to be erased and physically

---

[32] The Canadian Medical Association (the primary national advocacy organization for physicians) states in its *Principles for the Protection of Patients' Personal Health Information Policy (2011*) that information should be retained "…at least for the period required by the provincial or territorial regulatory authority (College) or by any applicable legislation. It may be necessary to maintain personal health information beyond the applicable period where there is a pending or anticipated legal proceeding related to the care provided to the patient." See Canadian Medical Association, *Principles for the Protection of Patients' Personal Health Information* (2011) at 4, online: Canadian Medical Association <http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf>.

[33] College of Physicians & Surgeons of Alberta, *Administration of Practice: Patient Records* (3 April 2014), online: College of Physicians & Surgeons of Alberta: <http://www.cpsa.ab.ca/Libraries/standards-of-practice/patient-records.pdf?sfvrsn=2>.

[34] College of Physicians and Surgeons of Saskatchewan, *Bylaw 23.1 Medical Records*, online: College of Physicians and Surgeons of Saskatchewan <http://www.sma.sk.ca/data/1/rec_docs/696_CPSS_Bylaw_23.pdf>.

[35] The College of Physicians & Surgeons of Manitoba, By-law #1, (1 December 2008), online: The College of Physicians & Surgeons of Manitoba <http://cpsm.mb.ca/cjj39alckF30a/wp-content/uploads/By-Law-1.pdf>.

[36] *Personal Health Information Act*, CCSM c P33.5, s 17(1).

destroyed."[37] This provision could be interpreted either as a requirement for destruction or as simply mandating that if records are to be destroyed, one must follow the stated methods.

Legislative provisions, bylaws and policies in Nova Scotia, British Columbia, and Newfoundland and Labrador contain the strongest and least ambiguous requirements for destruction. Nova Scotia's College policy merely indicates that "When the obligation to store medical records comes to an end, the records should be destroyed in a way that is in keeping with the obligation of maintaining confidentiality."[38] However, this requirement is buttressed by a provision in the Personal Health Information Act, which provides as follows:

> 49(2) At the expiry of the relevant retention period, personal health information that is no longer required to fulfil the purposes identified in the retention schedule must be securely destroyed, erased or de-identified.[39]

The British Columbia Personal Information Protection Act states:

> An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that
>
> (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and
>
> (b) retention is no longer necessary for legal or business purposes.[40]

And a bylaw under Newfoundland and Labrador's Medical Act is clear in its requirement:

> Following the applicable period of retention…, medical records which are not required to be retained in accordance with this By-Law must be destroyed in such a way that reconstruction of the record is not reasonably foreseeable in the circumstances.[41]

---

[37] The College of Physicians and Surgeons of Prince Edward Island, *The Application of the Principles of Privacy*, "Destruction of Records", online: The College of Physicians and Surgeons of Prince Edward Island <http://cpspei.ca/wp-content/uploads/2013/11/Privacy-Principles-P-Apr-2004.pdf>.

[38] College of Physicians & Surgeons of Nova Scotia, *Guidelines for Medical Record-Keeping,* (6 June 2008), online: College of Physicians & Surgeons of Nova Scotia <http://www.cpsns.ns.ca/portals/0/guidelines-policies/2008-medical-record.pdf>.

[39] SNS 2010, c 41, s 49(2).

[40] SBC 2003, c 63, s 35(2).

[41] The College of Physicians and Surgeons of Newfoundland and Labrador, By-Law 6: Medical Records (30 April 2012), s 29, online: The College of Physicians and Surgeons of Newfoundland and Labrador <http://www.cpsnl.ca/default.asp?com=Bylaws&m=292&y=&id=9>.

The Canadian Medical Association simply indicates that disposal should be in a safe and secure manner; it does not address the topic of need for destruction.[42] The Canadian Medical Protective Association advises its members that "Once the retention period has expired, records should be destroyed in a manner that maintains confidentiality."[43]

As the preceding discussion illustrates, provisions in the various provinces regarding destruction differ markedly. Only three provinces have a clear and unambiguous provision which mandates destruction of records. Others use language such as 'should' or 'may', or leave responsibility to organizations to develop a policy, or are completely silent as to the need for destruction. The main guidance provided in most provinces is how to destroy if destroying, not whether destruction is required, and even less often, the legislation addresses when to destroy. It may be concluded that legislative provisions and guidance by regulatory bodies and advocacy organizations regarding the obligations of retention and destruction of personal health information are problematically vague.

When this legislation was being drafted, the preoccupation was with retention. This was due to the fact that organizations wished to get rid of personal information as soon as possible due to space and weight limitations, and destruction was not remotely the primary focus. Rather, the legislators sought to ensure that records were retained for a suitably lengthy period of time for the purposes for which they had been collected. The need for and specifics as to how to meet the obligation of destruction have not received sufficient attention by legislators or regulatory authorities. The recent and ongoing shift to the digitization of information presents a number of challenges to meeting the obligations of retention and destruction that need to be addressed.

Import of the Digitization of Health Information

I have identified that relevant legislative provisions and policies are deficient due to vagueness, inconsistency, and sheer lack of guidance regarding the retention and destruction of health information. These deficiencies increase in significance when information is rendered electronic due to the enhanced value of the information itself, and also due to the complexities in attempting to ensure destruction.

Historically, health information was collected and stored on paper in manila folders in the context of healthcare delivery in order to ensure quality patient care and for billing purposes. Paper charts had a range of limitations, one of which was the volume of storage space required to retain them. The sheer weight and volume of paper-based records resulted in destruction being a necessary part of running a health-care service. These records also had a form of built-in confidentiality protection in that they were stored in what Nicolas Terry refers to as "innumerable data silos"[44], presumably by virtue of the fact that files needed to be kept in close physical proximity to the care provider or other institution.

---

[42] Canadian Medical Association, *Principles for the Protection of Patients' Personal Health Information* (2011) at s 12, online: Canadian Medical Association <http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf>.

[43] Canadian Medical Protective Association, A Matter of Records: Retention and Transfer of Clinical Records (rev June 2013), "storage and disposal", online: Canadian Medical Protective Association <https://www.cmpa-acpm.ca>.

[44] Nicolas P Terry, "Legal Issues Related to Data Access, Pooling, and Use" in "Chapter 4: Healthcare Data: Public Good or Private Property?" in Claudia Grossman et al, eds, *Clinical Data as the Basic Staple of*

But the storage of personal health information has gradually been transformed from paper-based to electronic medical records (EMRs).[45] Governments in Canada crave information as they grapple with burgeoning healthcare expenditures. A primary mechanism for controlling budgets is to base decision-making on solid evidence so as to increase efficiencies. This need for evidence results in strong and intensifying demands for information for purposes of research, planning, and evaluation of health care services and systems.[46] Thus, the federal government has invested $2.1 billion since 2001 through Canada Health Infoway[47] to facilitate the development and adoption of electronic health records in healthcare facilities, pharmacy networks, and physician offices. A majority of physicians' offices in Canada now use EMRs as part of their practice.[48]

This signals a shift in the very nature of health information. First, vast quantities of information are being created and stored. The problems with retention due to physical storage limitations are virtually absent. One 8 GB flash drive, for instance, can store 160,000 word-document-type pages' worth of information.[49] In the year 2000, storage costs had dropped to approximately $0.01 per megabyte,[50] which was 1/50,000$^{th}$ the amount they had been in 1980. By 2008, the cost was $0.0001.[51] Thus, the primary motivation of the custodian of information to destroy it, i.e. the need to gain space, is greatly diminished. Data can be retained forever in theory; as Bennett et al. identify, "…it is just easier to retain

---

*Health Learning: Creating and Protecting a Public Good: Workshop Summary* (Washington, U.S.: National Academies Press, 2010) at 159.

45 The EMR has been defined by the Canadian Medical Association as an electronic version of the paper record, which may be part of an office-based system or a broad integrated network. See Canadian Medical Association, *Principles for the Protection of Patients' Personal Health Information* (2011) at 5, online: Canadian Medical Association <http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf>.

46 Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada* (Saskatoon: Commission on the Future of Health Care in Canada, 2002); see also, Elaine Gibson, "Jewel in the Crown? The Romanow Commission Proposal to Develop a National Electronic Health Record System" (2003) 66:2 Sask LR 647.

47 Canada Health Infoway, Summary Corporate Plan 2012-2013 at 1, online: Canada Health Infoway <https://www.infoway-inforoute.ca/index.php/resources/infoway-corporate/business-plans/doc_download/80-summary-corporate-plan-2012-2013>.

48 Health Council of Canada, *Progress Report 2013: Health Care Renewal in Canada* (2013), Health Council of Canada at 13, online: Health Council of Canada <http://www.healthcouncilcanada.ca>.

49 CFgear Blog, "How much data can a USB flash drive hold?" (5 April 2010), online: CFgear Blog <http://cfgearblog.blogspot.ca/2010/04/how-much-data-can-usb-flash-drive-hold_5.html>.

50 A megabyte can contain approximately 500 pages of double-spaced plain-text: http://pc.net/helpcenter/answers/how_much_text_in_one_megabyte

51 Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009) at 63.

data than to get rid of it."[52] Indeed, it is argued by Viktor Mayer-Schonberger that the very act of deciding whether to retain or delete information has become more expensive than simply retaining it.[53]

Second, the information has transmorphed from something primarily or exclusively for patient care to something of high value for other purposes. The electronic era has veritably exploded the possibilities for uses of personal health information, ushering in a new currency in the information itself, both figuratively and in financial terms. The collection of information in databases, combined with the ability to merge various databases, results in a range of possibilities for exploitation of electronic information for secondary purposes. To take one example, a database of information concerning women recipients of social assistance may be matched with a database containing children's medical records in order to examine whether children born to mothers on social assistance have relatively poor health outcomes. In this way the identities of these women and children in society are powerfully shaped based on the findings of the research. Another example is the purchase by pharmaceutical corporations of information as to prescriptions issued to patients in order to target marketing to particular physicians based on their prescribing patterns. These are illustrations of this newfound 'currency' in health information.

EMRs may be compatible with and integrated into broader networks of interoperable (i.e., regional or provincial) electronic health record (EHR) systems. EHR systems have incredibly rich potential in that the information contained therein can be used to enhance the quality of patient care (multiple points of access to diagnosis and care information, for instance); also the information may be mined for purposes of research,[54] surveillance, audit, planning, and evaluation of health care services and systems. Further, the actual financial value of health information may be illustrated by the Icelandic government's sale of access to its health sector database to a corporation called deCODE. The contract provided for payments of between $950,000 and $1,900,000 per year.[55]

Authors Blanchette and Johnson analyze the shift to electronic information in the contexts of bankruptcy law, young offender records, and credit reports. They identify primary reasons that in their

---

[52] Colin J Bennett, Christopher Parsons & Adam Molnar, "Chapter 3: Forgetting, Non-Forgetting and Quasi Forgetting in Social Networking: Canadian Policy and Corporate Practice" in S Gutwirth et al, eds, *Reloading Data Protection* (Springer Science and Business Media, 2014) at 41. For a more fulsome exploration of this topic, see Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009).

[53] Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009) at 68.

[54] See Patricia Kosseim & Megan Brady, "Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes" (2008) 2 McGill J of L & H 5, for an explique of the difficulties in providing access to EHRs to researchers in light of the approach taken by Canada Health Infoway to their development.

[55] See deCODE genetics, Prospectus (Reg File No 333-31984), online: NASDAQ <http://www.nasdaq.com/markets/ipos/filing.ashx?filingid=1223935>. Due to a ruling of the Icelandic Supreme Court on November 27, 2003, however, the company had to abandon its attempt to establish the Health Sector Database after the Court found the company's attempt to establish the database unconstitutional. See Icelandic Supreme Court, R*agnhildur Gumundsddttir v. The State of Iceland*, No 151/2003.

view head American society toward what they refer to as a 'panoptic society'.[56] First, the quantity of data being collected has mushroomed. Indeed, Science Daily reported in 2013 that half of the world's data had been generated in the previous two years,[57] and one organization has estimated a growth rate of approximately 30 percent per year in the global accumulation of information.[58] Second, the granularity of the information being collected has greatly increased such that its value is greatly enhanced. Third, the information can be aggregated with other databases and types of information such that it provides "a much finer resolution of the digital persona than each [piece of information] can by itself."[59] When these factors – quantity, granularity, and the ability to cross-correlate or aggregate – are combined, there is high predictive power in the information generated. Mayer-Schonberger would add to this list the assets of easy retrieval[60] and global accessibility.[61] Blanchette and Johnson indicate that there is much excitement about the potential for this information to be used as an asset, and little concern at present as to the harmful effects that can result from data retention – hence the prediction of a panoptic, or 'all-seeing', society.

Provincial governments in Canada hold a cornucopia of health information in comparison to most other jurisdictions due to our publicly-funded healthcare system. [62] Information has been collected and collated by the provinces for billing and other administrative purposes in electronic format for at least forty years.[63] Consider trying to garner parallel information in a country like the U.S. with its widely disparate range of healthcare providers in the private and public sectors. This means that provincial-

---

[56] Drawing on Jeremy Bentham's formulation of a system in which prisoners could be observed constantly at little expense; Michel Foucault expanded from the prison context on the potential application of the panopticon concept to society more broadly and used to wield power in *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books, 1995).

[57] See SINTEF, "Big Data, for better or for worse: 90% of the world's data generated over last two years" (22 May 2013) ScienceDaily, online: ScienceDaily <www.sciencedaily.com/releases/2013/05/130522085217.htm>.

[58] Lyman and Varian, "How Much Information?", as cited in Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009) at 52.

[59] Jean-Francois Blanchette & Deborah G Johnson, "Data Retention and the Panoptic Society: The Benefits of Forgetfulness" (2002) 18 The Information Society 33 at 39.

[60] Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009) at 72.

[61]Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009) at 79.

[62] Don Willison, Elaine Gibson & Kim McGrail, "A Roadmap to Research Uses of Electronic Health Information" in Colleen M Flood, ed, *Data Data Everywhere: Access and Accountability?* (Montreal: McGill-Queen's University Press, 2010) at 233.

[63] Pat Martens, "How and Why Does it 'Work' at the Manitoba Centre for Health Policy?" in Colleen M Flood, ed, *Data Data Everywhere: Access and Accountability?* (Montreal: McGill-Queen's University Press, 2010) at 137.

government-held personal health information is rich in value in comparison to most jurisdictions outside of Canada.

There are heightened privacy risks associated with electronic information. EHRs can provide superior privacy protection in a number of respects, including the ability to trace all employees who have accessed one's health record. However, the fact that they can be accessed from multiple points, conveyed virtually instantaneously to many parts of the world, and carried on one's person in a flash drive or hard drive, renders them highly amenable to sharing in various contexts. This, combined with the fact that millions of pieces of information can be combined, leads to the risk of massive breaches of confidentiality as compared to when information existed in paper files. As just one egregious recent example, in July 2013, the theft of 4 unencrypted computers at a US facility led to the compromise of the personal health information of over 4 million people.[64] The fact that information is stored in EHRs leads to substantially heightened risk of broad breaches of confidentiality.

Risks to privacy are further heightened by technical obstacles to destruction of EMRs. Depending on the software used, the information often rests with a third party vendor.[65] This means that, unless covered in a contract between the healthcare provider and the vendor, the healthcare provider may lose control of for how long, and how, the data is to be retained or destroyed. Also EMRs must be backed up on a regular basis, usually off-site.[66] Consider a system that backs up daily or weekly – there may be dozens or even hundreds of copies of the information in existence. As former federal Privacy Commissioner Jennifer Stoddart stated in the context of online information:

> Once personal information goes online, it may be difficult to delete. While you may be able to delete it in one place, there may be cached versions or copies stored elsewhere that you cannot control. Digital storage is cheap and computer memory is plentiful – and unlike people, the Net never forgets.[67]

The physical ability to destroy the information is also problematic. Deletion of the EMR does not actually destroy the data; it merely removes it from the graphical user interface (essentially, the way we view the information). A joint report by Ann Kavoukian, then Privacy Commissioner for Ontario, and the National Association for Information Destruction, Inc., suggests the following as sole proven methods for destruction of electronic information:

---

[64] Advocate Health Care, Press Release, "Advocate Medical Group Notifies Patients, Offers Protection Following Office Burglary" (2013), online: Advocate Health Care <http://www.advocatehealth.com>.

[65] Written correspondence with Brad MacDonald, President, TimeAcct Information Systems, December 9, 2014.

[66] Written correspondence with Brad MacDonald, President, TimeAcct Information Systems, December 9, 2014.

[67] Canada, Office of the Privacy Commissioner of Canada, Archived News Release, "Protect your personal information because the Internet never forgets, Privacy Commissioner of Canada says" (27 January 2011) online: Office of the Privacy Commissioner of Canada: <https://www.priv.gc.ca/media/nr-c/2011/nr-c_110127_e.asp>. Stoddart was presumably drawing for this concept on a piece by JD Lasica: See JD Lasica, "The Net Never Forgets" (25 Nov 1998) Salon, online: Salon <http://www.salon.com/1998/11/25/feature_253/>.

> The method of destruction for electronic media includes mechanical destruction to render it unusable, degaussing, and sanitization (including secure erase), and should involve removing all labels or markings that indicate previous use. Simply deleting computer files or reformatting a disk does not securely destroy the data because even deleted files may be subject to data recovery efforts.
>
> For all personal hand-held computing or processing devices (such as PDAs and mobile phones) storing sensitive contact information, calendars, documents, e-mail correspondence and other information, methods of destruction may include mechanical destruction of the entire unit, or destruction of the replaceable memory circuits or card so that the device can be redeployed with a new memory component. [68]

A further challenge regarding destruction is that different records on the drive will carry different time frames for retention, and so the destruction dates will correspondingly be variable. If the hard drive is destroyed at the earliest date of expiry of an EMR's retention period, data that needs to be retained will also be destroyed. If it is destroyed at the latest date, other EMRs are de facto being retained too long.

The fact that more and more personal information is in the form of EMRs does not alter the historical obligations of retention and destruction; the obligations persist, but a physician who attempts to honour them is greatly challenged by these developments.[69] The risks associated with EHRs are viewed as sufficiently high by the Canadian Medical Association that it has taken the remarkable step of instructing physicians to advise their patients that they cannot control access nor guarantee confidentiality of information once it is part of such a system.[70]

B.C. Privacy Commissioner Elizabeth Denham referred to the need for greater privacy protections in the context of developments in information technologies as follows:

> The public expects there to be adequate safeguards to protect personal information, both in the delivery of health care and research using health data. Advances in information technology necessitate a much more comprehensive approach to privacy and security risk management than ever before.[71]

---

[68] Ontario, Information and Privacy Commissioner, Ontario and National Association for Information Destruction, Inc, *Get rid of it Securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information* (October 2009), online: Information and Privacy Commissioner, Ontario <http://www.ipc.on.ca/images/Resources/naid.pdf>.

[69] Nola M Ries & Geoff Moysa, "Legal Protections of Electronic Health Records: Issues of Consent and Security" (2005) 14:1 Health LR 18.

[70] See Canadian Medical Association, *Principles for the Protection of Patients' Personal Health Information* (2011) at 4, online: Canadian Medical Association <http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf>.

[71] British Columbia, Office of the Information & Privacy Commissioner for British Columbia, *Investigation Report F13-02, Ministry of Healt*h (26 June 2013), online: Office of the Information & Privacy Commissioner for British Columbia <https://www.oipc.bc.ca/report/investigation-reports/>. This report resulted from the tragic suicide of a health researcher who had been fired from his position in 2012 (along with six other government employees) on the basis that he had accessed personal data without proper authorization in the context of pharmaceutical research: See "Roderick MacIsaac Suicide: B.C. Government

Specifically, the need for destruction was addressed in a privacy impact assessment conducted on the Canada Health Infoway (CHI) blueprint for EHRs.[72] The CHI blueprint had referred to a need for indefinite retention at times. The assessment critiqued this suggestion on the basis of this violating the privacy principle of limiting retention and at times Canadian laws, and CHI in its response agreed to remove this statement from its blueprint.[73]

It may be seen that the failure of legislation to adequately address the topic of destruction of personal health information has not been of major import over the years. However, its rapid and increasing digitization has created a firestorm of problems with privacy that lead to the question of determining how this problem should best be addressed. In the following section I seek to answer this question.

Analysis

> [I]n this debate (as to whether clinical data is a public good or private property) the legal system is neither a spectator nor an independent actor. Legal models enter the equation because they reflect and so perpetuate the intended or perceived current state of public policy.[74]

Thus far in this paper I have outlined the basic arguments for the competing forces of retention and destruction and reviewed present laws and policies. I then examined the move to digitization of personal health information, and posited its creating a tremendous shift in the ability to retain information indefinitely, as well as greatly enhancing the worth of the information itself. Privacy concerns are thereby heightened. This gives rise to the question of whether greater attention needs to be paid to the need for destruction of information. The quote by Nicolas Terry that opens this section of the paper suggests that law may be seen to reflect and perpetuate public policy. If this is so, should laws and policies be changed to reflect these developments? And what framework should be applied to provide guidance in attempting to answer this question?

Perhaps the most prominent line of debate in the area of health information is between those who argue that autonomy of the individual is foremost and requires respect for individual choice,[75] and those

---

Apologizes to Researcher's Family", *CBC News* (3 October 2014) online: CBC News <http://www.cbc.ca/news/canada/british-columbia/roderick-macisaac-suicide-b-c-government-apologizes-to-researcher-s-family-1.2787048>.

[72] Canada Health Infoway, *A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2* (12 February 2008) at 29, online: Canada Health Infoway <https://www.infoway-inforoute.ca>.

[73] *Ibid* at 30.

[74] Nicolas P Terry, "Legal Issues Related to Data Access, Pooling, and Use" in "Chapter 4: Healthcare Data: Public Good or Private Property?" in Claudia Grossman et al, eds, *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary* (Washington, U.S.: National Academies Press, 2010) at 152.

[75] For a general discussion of privacy as control see Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967); Louis Lusky, "An Invasion of Privacy: A Clarification of Concepts" (1972) 72 Colum LR 693; Charles Fried, "Privacy" (1968) 77 Yale LJ 475 at 493; RA Wassertrom, "Privacy: Some Arguments and Assumptions" in F Schoeman, ed., *Philosophical Dimensions: an Anthology* (Cambridge: Cambridge University Press, 1984).

who argue that information is a collective asset and should be used for the public good.[76] These viewpoints contrast sharply and don't leave much room for common ground.[77] Following an analysis of the limitations of the individual choice/public good debate, I will briefly explore what an equality-based analysis adds to an understanding of the value of privacy in the context of personal health information. The final section analyzes privacy as a public good, and ends with some suggestions for reform.

Autonomy

A fundamental tenet of our legal system is respect for autonomy of the individual. This respect is manifested in recent years in Canada primarily in jurisprudence under s. 7 of the Charter of Rights and Freedoms.[78] Based squarely in liberalism, it attempts to ensure that the individual is able to exercise free will in choosing his/her destiny, and specifically in having her or his privacy respected. The necessary implication is that individuals should be able to control the use and retention of their personal information to the extent possible.

One concept that might be considered part of a liberal framework is that of data as property. Much of the American analysis of data revolves around who owns – and who should own - the information. This frame of reference implicitly sets up contesting claims on the part of the individual who is the source of the information and others who claim an entitlement to at minimum possess the information by virtue of its having been passed on to them, or somehow surrendered, or through interpretation of the relevant legislation. Viewing information through a property lens leads to conceptualization of the ensuing rights as including the ability to exclude others from accessing it, to trade in such information, and to profit from its use.

Autonomy is of fundamental importance, but there are two basic problems with its realization in the area of health information. First, the information is inevitably conveyed to others in the course of seeking health care services. Once this happens, the only mechanism that might ensure respect for autonomy is if the individual consents to subsequent uses. However, there is growing consensus that consent does not function adequately for a range of reasons, including the following: It does not apply when we are incompetent; it is inoperative when it comes to issues of public health, wherein societal needs take precedence; it cannot include third-party information conveyed by an individual because getting consent of the third party is impractical; and it is frequently given under circumstances of duress

---

[76] See, for example, Don E Detmer and Elaine B Steen, "Shoring up Protection of Personal Health Data" (Summer 1996) Issues in Science and Technology 73.

[77] For a discussion, see Jeroen Van den Hoven, "Information Technology, Privacy and the Protection of Personal Data" in eds Jeroen Van den Hoven and John Weckert Information Technology and Moral Philosophy (Cambridge: Cambridge University Press, 2008) at 301. See also "Chapter 4: Healthcare Data: Public Good or Private Property?" in Claudia Grossman et al, eds, *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary* (Washington, U.S.: National Academies Press, 2010) at 137-170.

[78] For example, see *R v Morgentaler*, [1988] 1 SCR 30; *Rodriguez v British Columbia (Attorney General)*, [1993] 3 SCR 519; *Cuthbertson v Rasouli*, 2013 SCC 53, 3 SCR 341. Note that the jurisprudence on autonomy is not exclusively Charter-based; see, for example, *Malette v Shulman* et al (1990), 72 OR (2d) 417 (CA).

or weakness.[79] The second problem is that we have little actual 'control' of our information in a number of significant ways. Legislation, common law and policies grant custodians the opportunity to engage in a wide range of uses without consent.[80] In some circumstances, the individual can explicitly opt out of its use, but the ability to do so is infrequent. More importantly, the individual is generally unaware of the range of uses nor of the ability to opt out. Therefore the individual does not control uses of information in any meaningful sense.

Clearly autonomy is important but in significant respects not actualisable, and therefore is inadequate as a complete frame of reference for the safeguarding of personal health information.

Public Good

Health information is often argued as constituting a public good for two principal reasons. First is that there are major benefits in pooling information and making it available for a range of uses.[81] This

---

[79] See Onora O'Neill, "Some Limits of Informed Consent" (2003) 29.1 J of Med Ethics 4; Neil C Manson & Onora O'Neill, *Rethinking Informed Consent in Bioethics* (Cambridge: Cambridge University Press, 2007).

[80] For example, Ontario's *Personal Health Information Protection Act*, SO 2004, c 3, Schedule A, s 37(1) provides for the following permitted uses without the requirement of consent:

> **37.** (1) A health information custodian may use personal health information about an individual,
> ...
> (b) for a purpose for which this Act, another Act or an Act of Canada permits or requires a person to disclose it to the custodian;
> (c) for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them;
> (d) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian;
> (e) for educating agents to provide health care;
> (f) in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual;
> (g) for the purpose of seeking the individual's consent, or the consent of the individual's substitute decision-maker, when the personal health information used by the custodian for this purpose is limited to the name and contact information of the individual and the name and contact information of the substitute decision-maker, where applicable;
> (h) for the purpose of a proceeding or contemplated proceeding in which the custodian or the agent or former agent of the custodian is, or is expected to be, a party or witness, if the information relates to or is a matter in issue in the proceeding or contemplated proceeding;
> (i) for the purpose of obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services;
> (j) for research conducted by the custodian, subject to subsection (3), unless another clause of this subsection applies; or
> (k) subject to the requirements and restrictions, if any, that are prescribed, if permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada.

[81] David Blumenthal, "Characteristics of a Public Good and How They are Applied to Healthcare Data" in "Chapter 4: Healthcare Data: Public Good or Private Property?" in Claudia Grossman et al eds, *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary* (Washington, U.S.: National Academies Press, 2010) at 139.

argument conforms closely to the spirit of communitarianism in that it priorizes the public good over the individual right over the uses that should be made of one's information.[82] A second argument is that health information is collected and/or rendered useful in electronic form by virtue of government funding; thus, we all contribute to the health care system by virtue of payment of taxes, and are entitled to reap the benefits of public use of information collected by the system.[83] While the latter argument has been made primarily in the American context, it may be all the more salient in Canada given the universal coverage of basic physician and hospital services through our health care system.

This model is not without its detractors. Amitai Etzioni, generally a champion of communitarian values/approaches, posits that health care information is exceptional in that it is the most highly personal and intimate of all information, and also may be used to discriminate against individuals, thus shaping their identities in problematic ways. [84] He is particularly concerned that the electronicization of information has given rise to major and multiple breaches of confidentiality.[85] Therefore he argues in favour of enhanced privacy protections vis-à-vis health information in contrast to other types of information.

Further, not all uses of information serve the public good. It is questionable whether the public good is a generic and readily-definable concept. For instance, who gets to decide whether something is in the public good? Is it in the public good for a particular drug to be developed? Does it matter if the pharmaceutical corporation stands to make a substantial profit from it? Does it matter if they have acted in violation of laws in their activities?[86]

It can be seen that neither the autonomy nor the communitarian/public good perspective provides a complete answer. The individual choice/public good debate is further problematized when viewed through an equality analysis. The risks of a violation of privacy may be heightened for, and one's access to privacy and confidentiality may be dependent upon, one's status in society. Privacy may be experienced differently by persons from disabled, racialized, and otherwise socially and economically marginalized groups. Any discussion as to solutions must include an analysis of the dynamic of equality.

Inequality

---

[82] Don E Detmer and Elaine B Steen, "Shoring up Protection of Personal Health Data" (Summer 1996) Issues in Science and Technology 73 at 77-78.

[83] David Blumenthal, "Characteristics of a Public Good and How They are Applied to Healthcare Data" in "Chapter 4: Healthcare Data: Public Good or Private Property?" in Claudia Grossman et al eds, *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary* (Washington, U.S.: National Academies Press, 2010) at 142-43.

[84] Amitai Etzioni, *The Spirit of Community: Rights, Responsibilities, and the Communitarian Agenda*. (New York: Crown, 1993); Amitai Etzioni, "A Liberal Communitarian Conception of Privacy" (2012) 29:3 J Marshall J Comp & Info L 419 at 450-453.

[85] Amitai Etzioni, "A Liberal Communitarian Conception of Privacy" (2012) 29:3 J Marshall J Comp & Info L 419 at 450-453.

[86] http://www.forbes.com/sites/erikakelton/2012/05/10/more-pharma-companies-to-join-the-dishonor-roll-pay-billions-for-fraud-following-abbotts-settlement/

The sensitivity of personal health information varies with its nature and context. For example, the fact that an individual is myopic (near-sighted) may not be experienced as sensitive by most, but if one seeks certain types of employment, e.g. with a police force, it may be highly sensitive if it prevents entry to the profession. More importantly, the disclosure of information that may not be of high sensitivity to an upper-class or middle-class individual can have a devastating impact if one lives in poverty; for example, it may result in the intervention of child protective services.

Genetic information presents particular problems. Marsha Hanen identifies the problematic impact of probabilistic genetic disease predisposition in the contexts of employment and insurance, areas in which knowledge of the predisposition can result in discriminatory treatment.[87] Karen Eltis examines the use of genetic predisposition research to draw inaccurate, distorted, and stereotyped conclusions about members of ethnic and racial minorities on the basis of intelligence.[88]

One's access to privacy and confidentiality is also dependent upon one's status in society. Catherine Frazee et al. conducted a series of focus groups with disabled women in Ontario to examine issues of privacy and confidentiality when accessing health care services.[89] They found that, in the experience of women with disabilities, confidentiality is routinely denied in comparison to the able-bodied. They further explore the fact that disabled women disproportionately receive social assistance and other forms of government income support. A requirement of these programs is the gathering of health care information devoid of treatment of the individual; in other words, the physician or other health care provider is in effect an agent of the state and not of the patient. Women recipients surveyed indicated that they feel constantly scrutinized, even by their own physicians, and the confidential nature of their relationship is seriously undermined by the need of the physician to report to government agencies. Thus, poverty, gender and disability intersect to deny these women– some of the most economically disadvantaged members of Canadian society - the level of confidentiality that those with greater privilege take for granted.

It may be seen that the collection, use and disclosure of health information has varying impact depending on one's position in society. Those most disadvantaged have the least control over the shaping of their identities and are most likely to experience adversely the effects of inappropriate – or even legitimate - uses of their information. And, as outlined above, the longer the information is retained, the more likely it will indeed be used in a way that impacts adversely on the person or group.

Privacy as a Social Good

---

[87] Marsha Hanen, "Chapter 10: Genetic Technologies and Medicine: Privacy, Identity and Informed Consent," in Carole Lucock, Valerie Steeves and Ian Kerr, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009).

[88] Karen Eltis, "Genetic Determinism and Discrimination: A Call to Re-orient Prevailing Human Rights Discourse to Better Comport with the Public Implications of Individual Genetic Testing" (2007) J of Law, Med & Ethics 282.

[89] Catherine Frazee, Joan Gilmour & Roxanne Mykitiuk, *The Legal Regulation and Construction of the Gendered Body and of Disability in Canadian Health Law and Policy* (2 March 2011), online: <http://ssrn.com/abstract=1775204>.

There is a line of argument that says: we need not set up this sharp dichotomy between privacy on the one hand, and social utility of uses of information on the other. Rather, we need to appreciate privacy itself as a public good - as something that we as a society cherish. This theory does not take issue with the communitarian conceptualization that information is a public good, but posits that so too is privacy a social good.[90]

The concept of privacy as a social good takes us into the nascent area of emerging law being referred to as the 'right to be forgotten'. In May 2014 the European Court ordered that Google remove from its search engine information concerning an auction notice on the complainant's repossessed home from many years prior.[91] This has led to a fair amount of discussion as to whether it is ever appropriate for personal information to no longer be available, with a range of views expressed.[92]

Blanchette and Johnson analyze the impact of long-term data retention in three domains – bankruptcy, young offenders, and credit reports.[93] They review the increasing trend to priorize data retention over destruction in these domains. In this context, they argue in favour of the social benefits of forgetfulness, of the ability for a person to have a fresh start in life – in other words, to shape and reshape one's identity over time. There is a benefit in being able to shed one's past that is rendered impossible with long-term retention of data. Arguments for destruction of data in these domains in particular – of special interest to socio-economically marginalized groups – also takes account of an equality analysis.

Mayer-Schonberger provides a stark example of the dangers in collecting and retaining information in the Netherlands in the 1930s.[94] A citizen registry had been created in order to facilitate administrative functioning and welfare planning. When the Nazis invaded, they confiscated the registry and had the ability to identify citizens of Jewish and Gypsy origin. This resulted in much higher rates of targeting these particular populations for attempted eradication than in most other European Nazi-controlled countries. Even the Jewish refugee population in the Netherlands fared better than citizens by virtue of the former's non-inclusion in the registry. What commenced as a beneficent endeavour toward Dutch citizens – the creation of the registry – became a malevolent force after the passage of a period of years.

---

[90] Valerie Steeves, "Chapter 11: Reclaiming the Social Value of Privacy" in Carole Lucock, Valerie Steeves and Ian Kerr, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009).

[91] *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12), online: <http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065>.

[92] See for example, Jeffrey Rosen, "The right to be forgotten" (2012) Stan LR Online: <http://www.stanfordlawreview.org>; Paul Bernal, "Chapter 4: The EU, the US and the Right to be Forgotten" in S Gutwirth et al, eds, *Reloading Data Protection* (Springer Science and Business Media, 2014); Steven C Bennett, "The Right to be Forgotten: Reconciling EU and US Perspectives" (2012) 30 Berkeley J Int L 161.

[93] Jean-Francois Blanchette & Deborah G Johnson, "Data Retention and the Panoptic Society: The Benefits of Forgetfulness" (2002) 18 The Information Society 33.

[94] Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009) at 141.

This is an example of group harm caused by retention of information. A Canadian example of potential individual harm has led to a decision to destroy vast quantities of personal information, including much health information, in the context of Aboriginal residential school survivors.[95] Under the Indian Residential Schools Settlement Agreement, an Independent Assessment Process (IAP) was established to provide compensation for abuse suffered by survivors of the school system. The Truth and Reconciliation Commission (TRC) was also established to establish a historical record of the treatment of Aboriginal children at church-run residential schools and to ensure that this record is made available to the Canadian public. In accordance with the IAP, compensation applicants provided documentation and oral evidence of the veracity of their claims. Health information was a substantial component of this evidence. The TRC sought to archive the evidence for posterity in a national research centre:

> For its part, the TRC submits that the IAP Documents are the single-most comprehensive collection of documents that evidence the harms suffered by residential school survivors. The TRC submits that the IAP Documents contain a unique aggregation of items, which taken as a whole provide the most comprehensive understanding of the abuses that took place in the Indian Residential School system. The TRC and the NCTR [National Centre for Truth and Reconciliation] submit that the IAP Documents are essential to the creation of "as complete an historical record as possible of the IRS system and legacy."[96]

In contrast, IAP chief adjudicator Dan Shapiro argued on behalf of the IAP in Ontario Superior Court that the archiving of these records would breach the confidentiality of the survivors' information, which had been provided for purposes of claims adjudication and not for purposes of the TRC. Justice Perell ruled in August 2014 that, subject to individual consent, the records should be destroyed after a period of fifteen years from the date of conclusion of the adjudication process. In the interim, claimants are to be given the option of consenting to the retention and archiving of their redacted records, failing which the records are to be destroyed.

The case serves as an interesting example on a number of levels. First, it directly pits individual privacy as against the perceived public good in having the information available in perpetuity. Second, it engages a question of equality in light of the concepts of group privacy and potential group harms – is it better for Aboriginal groups to have the information retained so that the best documentation of the devastating legacy of the schools is readily available? This question is answered by Justice Perell essentially in individual choice and consent terms as follows: It's up to the individual claimants to make their own decisions in this regard by giving their consent should they so choose; no-one else can or should make the decision for them. Third, it is an affirmation of the importance of forgetting – the societal interest in retention of the information is overshadowed by the right of individuals to walk away from their past, at least to a limited extent.

What does all this have to do with identity? One could argue that retaining information indefinitely or in perpetuity preserves our identities. That's an attractive but superficial formulation. Our health information can be interpreted and used by others in shaping their sense of our identity in ways that we don't find desirable. This in turn shapes our own sense of our identity. If we have control of the

---

[95] *Fontaine v Canada (Attorney General)*, 2014 ONSC 4585, 122 OR (3d) 1.

[96] *Fontaine v Canada (Attorney General)*, 2014 ONSC 4585, 122 OR (3d) 1 at para 238.

information we can control this shaping of identity; but to the extent that this takes place outside of our control, it can be problematic and indeed destructive. In a multitude of ways we have already lost control of decision-making surrounding our personal health information. And it's not likely that we will regain control, especially in this electronic era. Yet our identities are very much shaped by our ability to control information about ourselves and to whom such information is released.

It is my contention that a multi-faceted approach is required. In the first instance, it is important that we retain control over our information to the extent possible. The decision on Aboriginal residential school claimants was brilliant in this way – it gave control back to the claimants to make their own choices. But to the extent that control is not possible, the analysis needs to go further. A granular approach to retention is required that should be based on the type of information, reason for collection, intended use or uses, and risks of disclosure. There is no one-size-fits-all solution. For example, retention in order to conduct public health surveillance or epidemiological research serves a high value to society, and so retaining the information for these purposes would certainly deserve a relatively high degree of tolerance as compared to retention of information as a general default. One must also look to the sensitivity of the information should inappropriate disclosure occur, as well as the level of risk in the way that the information is stored – this includes both the degree of identifiability and the security mechanisms in place.

I also propose that destruction after a set period of time should be the default position. Laws at present focus on retention time frames but a preferable system would be to have set times for destruction unless the case can be made out that retention is in the longer-term interest. As discussed above, there is a range of reasons that this could be appropriate. These would need to be clearly justified as worthy of retention in the longer term despite the fact that privacy risks would accompany their retention but because of their very high social value. Part of the assessment should be the potential impact on groups/segments of society as well as on individuals.[97] Rigid provisions for long-term security of the information need to be in place, including succession plans for organizations holding the data. Finally, there appears to be little justification for the wide variation in laws at present. We need to develop a national model framework which provincial jurisdictions can draw on for guidance and adopt as appropriate.

Justice Windeyer of the High Court of Australia aptly referred to "[l]aw, marching with medicine but in the rear and limping a little".[98] It appears that the health professions have been embracing electronic technologies, and laws have not kept up with the rapid pace of reform. It is time for this problem to be addressed such that control over the shaping of our individual and group identities is not swept away in the tide of our wired selves.

---

[97] In this respect the judgment of Perell J in *Fontaine v Canada (Attorney General)*, 2014 ONSC 4585, 122 OR (3d) 1 may arguably have been deficient. The Truth and Reconciliation Commission had opposed destruction of the documents. The judgment rested on individual choice while burying the inherent group interest in retention.

[98] *Mount Isa Mines v Pusey* (1970, 125 CLR 383 at 395 (HCA), in the context of a claim for psychiatric illness in negligence law.