Dalhousie Law Journal

Volume 38 | Issue 2 Article 4

10-1-2015

Wired Identities: Retention and Destruction of Personal Health Information in an Electronic World

Elaine Gibson
Dalhousie University

Elaine Gibson*

Wired Identities: Retention and Destruction of Personal Health Information in an Electronic World

This article examines the issue of the retention and destruction of personal health information. While legislation in Canada shows some attention to the issue of retaining health records, very little consideration has been given to their destruction. As technological advances have made indefinite retention feasible, serious privacy issues are now being raised by the lack of a standard related to the destruction of health records. The author argues that this issue needs to be explicitly addressed. The author analyzes this problem by looking at issues of autonomy, public good, inequality, and privacy as a social good before offering thoughts on the shape that policies around the destruction of personal health information should take.

L'article examine les enjeux qui entourent la rétention et la destruction de renseignements personnels sur la santé. Alors qu'au Canada, les mesures législatives semblent porter une certaine attention à la rétention des dossiers de santé, la question de leur destruction n'est que peu ou pas abordée. À mesure que les progrès technologiques ont rendu possible la rétention des dossiers pour des périodes indéfinies, de grands problèmes liés à la protection de la vie privée sont aujourd'hui provoqués par l'absence de normes concernant la destruction des dossiers de santé. L'auteure affirme que ces problèmes doivent être abordés de manière explicite. Pour les analyser, elle examine les questions d'autonomie, de bien public, d'inégalité et de respect de la vie privée en tant que bien social avant de réfléchir sur la forme que pourraient prendre les politiques entourant la destruction des dossiers de santé.

* Schulich School of Law, Dalhousie University. I am grateful to have been selected as recipient of the Charles D Gonthier Fellowship from the Canadian Institute for the Administration of Justice and the Dr. Robert F Maudsley Memorial Research/Study Grant from the College of Physicians & Surgeons of Nova Scotia. Financial support from these awards aided in the development of this paper. I am also grateful for the excellent research assistance provided by Ilana Luther.

> 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 contains 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 been addressed in Canadian legislation and policies designed to ensure the protection of personal health information. The flip side of retention—destruction—has received little attention to date. Statutes and policies mention destruction

1. Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding* (Monterey, CA: Brooks/Cole, 1975) at 50 [emphasis added].

in passing, but the parameters of destruction 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 solvable; indeed, we have entered an era in which it is more expedient to retain than to destroy information. A number of arguments favour indefinite retention for the benefit of us, 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 the retention and destruction of personal health information. 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, the rapid and increasing digitization of this information has profoundly altered the situation, creating a firestorm of problems with privacy. This leads to the question of determining how this problem should best be addressed. The following section analyzes the topic in the contexts of autonomy, information as a public good, inequality, and privacy as a social good. I then offer tentative proposed directions for setting destruction policies.

The specific focus of this discussion is physicians and surgeons, but suffice it 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 the focus of this paper is personal health information, that is, information that is identifiable or potentially identifiable in combination with other information. Information that is

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

anonymized[3] is not imbued with identical privacy concerns; however, once information is truly anonymized, it loses much of its value.[4] Genetic information is within the scope of this paper due to the health information inevitably contained therein. Genetic information presents a particular conundrum in the context of anonymization in that it is unique to the individual and therefore can never truly be anonymized.[5] Furthermore, information considered to be anonymized can sometimes be de-anonymized through electronic-information-savvy endeavours.[6] Finally, even if truly anonymized, a remote yet discernable privacy interest subsists.[7]

I. *Rationales for retention and destruction*

The 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, such as tests ordered and treatments received, is available for the subsequent provision of care.[9] Retention also enables review for purposes of billing, quality assurance,

3. See definition of anonymized information in Secretariat on Responsible Conduct of Research, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (Ottawa: Secretariat on Responsible Conduct of Research, 2014) at 59, online: PRE <http://www.pre.ethics.gc.ca/pdf/eng/tcps2-2014/TCPS_2_FINAL_Web.pdf>: "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, for instance, in order to fully understand reasons behind certain patient behaviours: see William Crown, "Characteristics of the Marketplace for Medical Care Data" in Claudia Grossmann et al, eds, *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary* (Washington, DC: National Academies Press, 2010) 143 at 147-149.

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

> DNA is itself uniquely identifiable. 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. 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.

6. Amitai Etzioni, "A Liberal Communitarian Conception of Privacy" (2012) 29:3 John Marshall J Computer & Info L 419 at 459-460 [Etzioni, "Communitarian Conception of Privacy"].

7. Elaine Gibson, "Is There a Privacy Interest in Anonymized Personal Health Information?" (2003) Health LJ 97. Sokhansanj elaborates on this topic, discussing how the use of even anonymized information for research purposes can impact negatively on African Americans, see Sokhansanj, *supra* note 5.

8. *McInerney v MacDonald*, [1992] 2 SCR 138 at 150-151, 93 DLR (4th) 415 [*McInerney*].

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

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 also may 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 fascination with genetic and social influences on our lives leads to claims of the need to know one's 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 or in perpetuity.

Reasons for retention are manifest and plentiful. The justifications in favour of destruction are fewer in number but nevertheless mighty. 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] The longer information is retained, the greater the likelihood that it will be accessed by or disseminated to a range of individuals and organizations, and the possibility that it will be inappropriately used multiplies. This gives rise to acute privacy concerns. 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

---

10. Elaine Gibson, "Health Information: Confidentiality and Access" in Jocelyn Downie, Timothy Caulfield & Colleen M Flood, eds, *Canadian Health Law and Policy*, 4th ed (Markham, ON: LexisNexis Canada, 2011) 253.

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) 233.

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

13. See, e.g., Juliet R Guichon, Ian Mitchell & Michelle Giroux, eds, *The Right to Know One's Origins: Assisted Human Reproduction and the Best Interests of Children* (Brussels: Academic & Scientific, 2012); Michelle Giroux & Mariana De Lorenzi, "'Putting the Child First': A Necessary Step in the Recognition of the Right to Identity" (2011) 27:1 Can J Fam L 53; Vanessa Gruben & Daphne Gilbert, "Donor Unknown: Assessing the Section 15 Rights of Donor-Conceived Offspring" (2011) 27:2 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 or 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*, 2nd ed (Markham, ON: LexisNexis Canada, 2008) 91 at 92-93.

15. Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193 at

incursions into one's private life. The incursions that were the subject of concern included "instantaneous photographs," "numerous mechanical devices," and the widespread circulation of newspapers, with 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 of Justice 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, militates against the indefinite retention of personal health information. Destruction is the sole guaranteed method of preventing a breach of confidentiality.

II. *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.

In the year 2000, Parliament invoked the federal trade and commerce power to enact the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[18] *PIPEDA* covers information used, collected, or disclosed in the course of commercial activity. Industry Canada has declared that physicians and surgeons in private practice fall under the auspices of *PIPEDA* by virtue of their engagement in commercial activity.[19] Hospitals, on the other hand, are presumptively excluded from

---

195.

16. *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317, [2014] 3 CMLR 1247 [*Google v AEPD*].

17. Discussed further below in section on Privacy as a social good.

18. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

19. Industry Canada, *PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector: Questions & Answers*, (Ottawa: Industry Canada, 25 February 2013) 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>. Commercial activity is defined 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,

PIPEDA.[20] All provinces have enacted legislation to regulate private sector information, either health care-specific[21] or private-sector more broadly.[22]

PIPEDA permits provinces and territories to have their information legislation declared substantially similar to *PIPEDA*, and in that circumstance, that legislation takes the place of *PIPEDA* for information which stays within the province.[23] Legislation in Alberta, British Columbia, Ontario, New Brunswick, and Newfoundland and Labrador has been declared substantially similar.[24] Where substantially similar, *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.

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,[25] following which it is to be "destroyed, erased, or made anonymous."[26] Organizations are responsible for developing guidelines and procedures for retention and destruction.[27] Note that these provisions within *PIPEDA* are ambiguous and contain no suggested time frames. Instead of providing clear guidance in the legislation and regulations,

---

membership or other fundraising lists": *PIPEDA*, *supra* note 18, s 2(1).

20. Industry Canada, *supra* note 19 at 3.

21. Health care-specific legislation is as follows: Manitoba's *Personal Health Information Act*, SM 1997, c 51, CCSM c P33.5 [MB *PHIA*]; New Brunswick's *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05 [NB *PHIPAA*]; Newfoundland and Labrador's *Personal Health Information Act*, SNL 2008, c P-7.01 [NL *PHIA*]; Nova Scotia's *Personal Health Information Act*, SNS 2010, c 41 [NS *PHIA*]; Ontario's *Personal Health Information Protection Act*, SO 2004, c 3, Schedule A [ON *PHIPA*]; Prince Edward Island's *Health Information Act*, SPEI 2014, c 31 [PEI *HIA*] (not yet in force); Saskatchewan's *Health Information Protection Act*, SS 1999, c H-0.021 [SK *HIPA*].

22. Broad private sector legislation is as follows: British Columbia's *Personal Information Protection Act*, SBC 2003, c 63 [BC *PIPA*]; Quebec's *An Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 [QC *PPIPS*]. Alberta is unique in having broad private sector legislation and health care-specific legislation: Alberta *Personal Information Protection Act*, SA 2003, c P-6.5 [AB *PIPA*]; Alberta *Health Information Act*, RSA 2000, c H-5 [AB *HIA*].

23. *PIPEDA*, *supra* note 18, s 26(2)(b).

24. The following provinces have had their health information legislation declared substantially similar: British Columbia (*Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220); Ontario (*Health Information Custodians in the Province of Ontario Exemption Order*, SOR/2005-399); Quebec (*Organizations in the Province of Quebec Exemption Order*, SOR/2003-374); New Brunswick (*Personal Health Information Custodians in New Brunswick Exemption Order*, SOR/2011-265); Newfoundland and Labrador (*Personal Health Information Custodians in Newfoundland and Labrador Exemption Order*, SI/2012-72). Alberta's general private sector legislation has been declared substantially similar (*Organizations in the Province of Alberta Exemption Order*, SOR/2004-219), but its health-information-specific legislation has not (i.e., AB *HIA*, *supra* note 22).

25. That is, unless there has been a request for personal information: see *PIPEDA*, *supra* note 18, s 8(8).

26. *Ibid*, Schedule 1, ss 5, 4.5.3.

27. *Ibid*, Schedule 1, ss 5, 4.1.4.

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[28] or mandates that organizations are to develop policies and implement procedures.[29] Thus, similarly to under *PIPEDA*, primary responsibility is shifted from the provincial government level to the organizations themselves.

1. *Retention*

In addition to information legislation, each province has legislation establishing a governing college for physicians and surgeons, and each college has provisions requiring the retention of records. The basic time period for mandated retention ranges from five years from the date of last entry in Quebec,[30] through six years in Saskatchewan,[31] to ten years in most provinces.[32] British Columbia is the clear outlier, having increased its requirements in 2014 from five to sixteen years.[33] These periods are increased for minors, for whom varying additional times are added for retention, ranging from two years past the age of majority in Alberta and Saskatchewan[34] to sixteen years past the age of majority in British Columbia.[35] Quebec does not require additional retention for minors. The

28. AB *HIA*, *supra* note 22, s 108(1)(o); SK *HIPA*, *supra* note 21, s 63(1)(i); QC *PPIPS*, *supra* note 22, s 90. Note that such regulations have rarely been made.

29. AB *PIPA*, *supra* note 22, s 35; BC *PIPA*, *supra* note 22, s 35; MB *PHIA*, *supra* note 21, s 17(1); ON *PHIPA*, *supra* note 21, s 10; NB *PHIPAA*, *supra* note 21, s 55(1); NS *PHIA*, *supra* note 21, s 50; NL *PHIA*, *supra* note 21, s 13(2).

30. *Règlement sur les dossiers, les lieux d'exercise et la cessation d'exercise d'un médecin* CQLR c M-9, r 20.3, s 12 [QC *Regulation on Records*].

31. College of Physicians and Surgeons of Saskatchewan, *Regulatory Bylaws* (CPSS, April 2015), s 23.1(f), online: CPSS <https://www.cps.sk.ca/Documents/Legislation/Legislation/Regulatory%20Bylaws%20-%20April%202015.pdf>.

32. See, e.g., Ontario's *General*, O Reg 114/94, s 19(1); College of Physicians and Surgeons of Prince Edward Island, "The Application of the Principles of Privacy" (CPSPEI, April 2004), online: CPSPEI <cpspei.ca/wp-content/uploads/2013/11/Privacy-Principles-P-Apr-2004.pdf>; College of Physicians and Surgeons of Nova Scotia, "Policy on the Content and Maintenance of Medical Records" (CPSNS, 18 October 2013), online: CPSNS <www.cpsns.ns.ca/DesktopModules/Bring2mind/DMX/Download.aspx?PortalId=0&TabId=129&EntryId=42>.

33. College of Physicians and Surgeons of British Columbia, *Bylaws* (CPSBC, 12 March 2015), s 3-6(2), online: CPSBC <https://www.cpsbc.ca/files/pdf/HPA-Bylaws.pdf>.

34. College of Physicians and Surgeons of Alberta, "Administration of Practice: Patient Records" (CPSA, 3 April 2014), s 9, online: CPSA <www.cpsa.ab.ca/Libraries/standards-of-practice/patient-records.pdf?sfvrsn=2>; College of Physicians and Surgeons of Saskatchewan, *supra* note 31.

35. College of Physicians and Surgeons of British Columbia, *supra* note 33. This mandated time frame far exceeds the Canadian Medical Protective Association (medical liability defence organization)'s general recommendation of a minimum ten-year retention (plus ten years from age of majority).

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, and these limitation periods also differ between provinces. Note that these retention periods are identified as minimums; by inference, unless there is a specified requirement for destruction following the retention period, the information may be held for a longer period of time.[36]

This variability and dearth of specificity in guidance may simply reflect confusion, or it may reflect differing conceptions of privacy informing the legislature or organization. The need for flexibility to accommodate the extension 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 in certain circumstances does not in turn justify a lack of specificity in the eventual need for destruction.

2. *Destruction*

Despite wide variation and ambiguity, at least the requirements for retention are addressed in every jurisdiction, unlike those for destruction. Most of the colleges of physicians and surgeons outline the required procedures if the records are being destroyed.[37] However, in terms of whether destruction is actually required in and of itself, the colleges' requirements vary widely. The colleges of physicians and surgeons in Alberta[38] and Saskatchewan[39] have no provisions concerning destruction. New Brunswick,[40] Ontario,[41] and Quebec[42] provide that information "may" be destroyed; there is no requirement to do so. Manitoba's legislation[43] refers physicians to the

36. The Canadian Medical Association (the primary national advocacy organization for physicians) states 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, "CMA Policy: Principles for the Protection of Patients' Personal Health Information" (CMA, 2011) at 4, online: CMA <policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf>.

37. See, e.g., *British Columbia bylaws under the Health Professions Act*, RSBC 1996, c 183, College of Physicians and Surgeons of British Columbia, *supra* note 33, s 3-7(1), which outlines the methods by which various types of records are to be destroyed.

38. College of Physicians and Surgeons of Alberta, *supra* note 34.

39. College of Physicians and Surgeons of Saskatchewan, *supra* note 31.

40. College of Physicians and Surgeons of New Brunswick, "Guidelines: The Patient Medical Record" (CPSNB, June 2010), online: CPSNB <www.cpsnb.org/english/Guidelines/guidelines-7.html>.

41. College of Physicians and Surgeons of Ontario, "Policy Statement #4-12: Medical Records" (CPSO, May 2012), online: CPSO <www.cpso.on.ca/CPSO/media/uploadedfiles/policies/policies/policyitems/medical_records.pdf>.

42. QC *Regulation on Records*, *supra* note 30.

43. College of Physicians and Surgeons of Manitoba, *By-law #1* (CPSM, 1 December 2008), online: CPSM <cpsm.mb.ca/cjj39alckF30a/wp-content/uploads/By-Law-1.pdf>.

Manitoba *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."[44] Thus, Manitoban 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 destroyed."[45] This provision could be interpreted either as requiring 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. The Nova Scotia College policy discusses the method but not the need for destruction; however, it also refers the reader to the province's *Personal Health Information Act*,[46] which provides:

> 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.[47]

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.[48]

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.[49]

---

44. MB *PHIA*, *supra* note 21, s 17(1).
45. College of Physicians and Surgeons of Prince Edward Island, *supra* note 32.
46. College of Physicians and Surgeons of Nova Scotia, *supra* note 32.
47. NS *PHIA*, *supra* note 21 s 49(2).
48. BC *PIPA*, *supra* note 22, s 35(2).
49. College of Physicians and Surgeons of Newfoundland and Labrador, "By-Law 6:

The Canadian Medical Association simply indicates that disposal should be in a safe and secure manner; it does not address the need for destruction.[50] The Canadian Medical Protective Association advises its members that "[o]nce the retention period has expired, records should be destroyed in a manner that maintains confidentiality."[51]

As the preceding discussion illustrates, provisions in the various provinces regarding destruction differ markedly. Only three provinces have a clear and unambiguous provision that mandates destruction of records. Others use language such as "should" or "may," 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, and not whether destruction is required per se. It is even less common that 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.

In the era in which most of the relevant 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 therefore destruction was not remotely the primary focus. Rather, the emphasis was on insisting that records be retained for a suitably lengthy period of time for the purposes for which they had been collected.[52] 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 must be addressed.

3. *Digitization*

It has been suggested 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 due

Medical Records" (CPSNL, 30 April 2012), s 29, online: CPSNL <www.cpsnl.ca/default.asp?com=Bylaws&m=292&y=&id=9>.

50. Canadian Medical Association, *supra* note 36.

51. Canadian Medical Protective Association, "A Matter of Records: Retention and Transfer of Clinical Records" (CMPA, June 2013), online: <https://www.cmpa-acpm.ca/en/web/guest/-/a-matter-of-records-retention-and-transfer-of-clinical-records>.

52. Jean-François Blanchette & Deborah G Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness" (2002) 18:1 Information Society 33 at 34.

to the complexities in attempting to ensure destruction of digitized information.

Historically, health information was collected and stored on paper in manila folders in the context of health care 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,"[53] presumably by virtue of the fact that files needed to be kept in close physical proximity to the care provider or other institution.

The storage of personal health information has been transformed gradually from paper-based to electronic medical records (EMRs).[54] Governments in Canada crave information as they grapple with burgeoning health care expenditures. A primary mechanism for controlling budgets is increasing efficiency by making decisions based on solid evidence. This need for evidence results in strong and intensifying demands for information for the purposes of research, planning, and evaluation of health care services and systems.[55] The federal government has invested $2.1 billion since 2001 through Canada Health Infoway[56] to facilitate the development and adoption of electronic health records in health care facilities, pharmacy networks, and physicians' offices. A majority of physicians' offices in Canada now use EMRs as part of their practice.[57]

This signals a shift in the very nature of health information. First, vast quantities of information are being created and stored. Problems

53. Nicolas P Terry, "Legal Issues Related to Data Access, Pooling, and Use" in Grossmann et al, *supra* note 4, 151 at 159.

54. 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, *supra* note 36 at 5.

55. 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 L Rev 647.

56. Canada Health Infoway, "Summary Corporate Plan 2012–2013" (Canada Health Infoway, 31 January 2012) 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>.

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

with retention due to paper-based storage limitations are virtually absent. An eight-gigabyte flash drive, for instance, can store 160,000 word-document-type pages' worth of information.[58] In the year 2000, storage costs had dropped to approximately $0.01 per megabyte,[59] which was 1/50,000th the amount they had been in 1980. By 2008, eight years later, the cost had been reduced to a mere $0.0001 per megabyte.[60] Thus, the primary motivation of the custodian of information to destroy information—the need to gain space—has been greatly diminished. Theoretically, data can be retained in perpetuity; as Bennett, Parsons, and Molnar note, in the present era, "it is just easier to retain data than to get rid of it."[61] Indeed, Viktor Mayer-Schönberger posits that the very act of deciding whether to retain or delete information has become more expensive than simply retaining it.[62]

Second, information has transformed from something primarily or exclusively for patient care to something of 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. 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 uses. To take one example, a database of information concerning women who receive 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.[63] 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

58. CFgear Blog, "How Much Data Can a USB Flash Drive Hold?" (5 April 2010), CFgearblog (blog), online: <cfgearblog.blogspot.ca/2010/04/how-much-data-can-usb-flash-drive-hold_5.html>.

59. A megabyte can contain approximately 500 pages of double-spaced plain-text: Per Christensson, "How Many Pages of Text Will One Megabyte Hold?" (3 July 2005), online: <pc.net/helpcenter/answers/how_much_text_in_one_megabyte>.

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

61. Colin J Bennett, Christopher Parsons & Adam Molnar, "Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice" in Serge Gutwirth, Ronald Leenes & Paul De Hert, eds, *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Dordrecht: Springer, 2014) 41 at 41. For a more fulsome exploration of this topic, see Mayer-Schönberger, *supra* note 60.

62. Mayer-Schönberger, *supra* note 60 at 68.

63. From 2002–2005 I served on the Family Benefits Database Advisory Committee, which reviewed proposals to merge the family benefits database for Nova Scotia with other health-related and socioeconomic-related databases.

patterns.[64] These are just a few 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 rich potential in that the information they contain can be used to enhance the quality of patient care (for example, multiple points of access to diagnosis and care information); also the information may be mined for purposes of research,[65] surveillance, audit, planning, and evaluation of health care services and systems. As one example of the actual dollar value of health information, the government of Iceland sold 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.[66]

Blanchette and Johnson analyzed the shift to electronic information in the contexts of bankruptcy law, young offender records, and credit reports. They identified primary reasons that American society, in their view, is headed toward what they refer to as a "panoptic society."[67] First, the quantity of data being collected has mushroomed. Indeed, *ScienceDaily* reported in 2013 that 90 per cent of the world's data had been generated in the previous two years,[68] and one research group has estimated a growth rate of approximately 30 per cent per year in the global accumulation of information.[69] Second, the granularity of the information being collected has greatly increased, such that its value is significantly

64. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2001–14" (Ottawa: Office of the Privacy Commissioner of Canada, 2001), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/cf-dc/2001/cf-dc_010921_e.asp>.

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

66. See deCODE genetics, "Prospectus Registration File No 333-31984," online: NASDAQ <www.nasdaq.com/markets/ipos/filing.ashx?filingid=1223935>. Due to a ruling of the Icelandic Supreme Court on 27 November 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, Ragnhildur *Guðmundsdóttir v The State of Iceland*, No 151/2003, online: <https://epic.org/privacy/genetic/iceland_decision.pdf>.

67. 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 Michael Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books, 1995).

68. See SINTEF, "Big Data, for Better or for Worse: 90% of the World's Data Generated over Last Two Years," *ScienceDaily* (22 May 2013), online: <www.sciencedaily.com/releases/2013/05/130522085217.htm>.

69. Peter Lyman & Hal R Varian, "How Much Information?" (2003) at 5, online: <groups.ischool.berkeley.edu/archive/how-much-info-2003/printable_report.pdf>, cited in Mayer-Schönberger, supra note 60 at 52.

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."[70] 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-Schönberger would add to this list the assets of easy retrieval[71] and global accessibility.[72] 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[73]—hence their prediction of a panoptic society.

Provincial governments in Canada hold a veritable cornucopia of health information in comparison with most other jurisdictions due to our publicly-funded health care system.[74] The provinces have collected and collated information for billing and other administrative purposes in electronic format for at least forty years.[75] Consider trying to garner parallel information in a country like the U.S. with its widely disparate range of health care providers in the private and public sectors. The implication is that the personal health information held by provincial governments is rich in value in comparison with the information available in most jurisdictions outside of Canada.

EHRs can provide superior privacy protection in a number of respects, including the ability to trace the identities of all employees within an institution who have accessed a person's health records. However, there are also heightened privacy risks associated with electronic information. EHRs 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. These factors render the information highly amenable to sharing in various contexts. This, coupled with the fact that millions of pieces of information can be combined, leads to the risk of massive breaches of confidentiality compared with when information existed only in paper files. As one egregious recent example, in July 2013, the theft of four unencrypted computers at a U.S. facility compromised the personal health information of over four million people.[76] The fact that

70. Blanchette & Johnson, *supra* note 52 at 39.
71. Mayer-Schönberger, *supra* note 60 at 72.
72. *Ibid* at 79.
73. Blanchette & Johnson, *supra* note 52 at 39.
74. Willison, Gibson & McGrail, *supra* note 11 at 233.
75. Pat Martens, "How and Why Does It 'Work' at the Manitoba Centre for Health Policy? A Model of Data Linkage, Interdisciplinary Research, and Scientist/User Interactions" in Flood, *supra* note 11, 137 at 137.
76. Advocate Health Care, Press Release, "Advocate Medical Group Notifies Patients, Offers

information is stored in EHRs leads to a substantially heightened risk of broad breaches of confidentiality.

Risks to privacy are further heightened by technical obstacles to the destruction of EMRs. Depending on the software used, the information often rests with a third-party vendor.[77] This means that, unless covered in a contract between the health care provider and the vendor, the health care provider may lose control of how and for how long the data is to be retained or destroyed. Also, EMRs must be backed up on a regular basis, usually off-site.[78] Consider a system that routinely backs up daily or weekly—dozens or even hundreds of copies of the information may exist. The federal Office of the Privacy Commissioner discussed this concept 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," Commissioner Stoddart says.[79]

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 report produced jointly by Ann Cavoukian, then Privacy Commissioner for Ontario, and the National Association for Information Destruction, suggests the following as the sole proven methods for destruction of electronic information:

> 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

---

Protection Following Office Burglary" (26 August 2013), online: Advocate Health Care <www.advocatehealth.com/body_full.cfm?id=12&action=detail&ref=293>. For a recent Canadian example in which the personal health information of 620,000 Albertans was compromised, see "Laptop Stolen with Health Information of 620,000 Albertans," *CBC News* (23 January 2014), online: <www.cbc.ca/news/canada/edmonton/laptop-stolen-with-health-information-of-620-000-albertans-1.2507161>.

77. Letter from Brad MacDonald (President, TimeAcct Information Systems) to Elaine Gibson (9 December 2014), on file with author.

78. *Ibid.*

79. Office of the Privacy Commissioner of Canada, 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," *Salon* (25 November 1998), online: Salon <www.salon.com/1998/11/25/feature_253/>.

> 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.[80]

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 vary correspondingly. 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 the hard drive 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.[81] 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 or guarantee confidentiality of information once it is part of such a system.[82]

British Columbia's 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.[83]

---

80. Ontario, Information and Privacy Commissioner & National Association for Information Destruction, "Get Rid of It *Securely* to Keep It Private: Best Practices for the Secure Destruction of Personal Health Information" (Information and Privacy Commissioner, Ontario, October 2009) at 8, online: IPC ON <https://www.ipc.on.ca/images/Resources/naid.pdf>.

81. Nola M Ries & Geoff Moysa, "Legal Protections of Electronic Health Records: Issues of Consent and Security" (2005) 14:1 Health L Rev 18.

82. See Canadian Medical Association, *supra* note 36 at 4.

83. Office of the Information and Privacy Commissioner for British Columbia, "Investigation Report F13-02, Ministry of Health," (OIPC BC, 26 June 2013), online: OIPC BC < https://www.oipc.bc.ca/investigation-reports/1546>. 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) based on the claim that he had accessed personal data without proper authorization in the context of pharmaceutical research: See "Roderick MacIsaac Suicide: B.C. Government Apologizes to Researcher's Family," *CBC News* (3 October 2014), online: <http://www.cbc.ca/news/canada/british-columbia/roderick-

Specifically, the need for destruction was addressed in a privacy impact assessment conducted on the Canada Health Infoway (CHI) blueprint for EHRs.[84] The CHI blueprint had referred to a need for indefinite retention in some cases. The impact assessment critiqued this suggestion on the basis that it violated both the privacy principle of limiting retention and at times Canadian laws. In response, CHI agreed to remove this statement from its blueprint.[85]

Thus far, 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. In light of the need to address destruction of information, the next section examines a range of rationales that suggest different mechanisms for examining the topic.

III. *Normative and public policy rationales*

> [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.[86]

This passage by Nicolas Terry indicates that laws follow and instantiate public policy. If this is so, or if it is ia value worth striving for, it would be important that our laws and policies be amended to reflect developments in the area of health information. This takes us to the question of the rationales to be applied to provide guidance.

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,[87] and those who argue that information is a collective asset and should be used for the

---

macisaac-suicide-b-c-government-apologizes-to-researcher-s-family-1.2787048>.

84. Canada Health Infoway, *A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2* (Canada Health Infoway, 12 February 2008) at 29, online: Canada Health Infoway <https://www.infoway-inforoute.ca/en/component/edocman/resources/reports/privacy/13-a-conceptual-privacy-impact-assessment-of-the-ehrs-blueprint-version-2>.

85. *Ibid* at 30.

86. Terry, *supra* note 53 at 152.

87. For a general discussion of privacy as control see Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967); Louis Lusky, "Invasion of Privacy: A Clarification of Concepts" (1972) 72:4 Colum L Rev 693; Charles Fried, "Privacy" (1968) 77:3 Yale LJ 475 at 493; Richard A Wassertrom, "Privacy: Some Arguments and Assumptions" in Ferdinand D Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984) 317.

public good.[88] These viewpoints contrast sharply and do not leave much room for common ground.[89] 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.

1. *Autonomy*

A fundamental tenet of our legal system is respect for individual autonomy. This respect is manifested in recent years in Canada primarily in jurisprudence under section 7 of the *Charter of Rights and Freedoms*.[90] Based squarely in liberalism, it attempts to ensure that the individual is able to exercise free will in choosing his or her destiny, and specifically in having his or her privacy respected. The necessary implication is that individuals should be able to control the use and retention of their personal information to the greatest extent possible.[91]

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.[92] 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 abilities to exclude others from accessing it, to trade in such information, and to profit from its use. Whoever is viewed as owning the information is conceived of as having the ability to act autonomously with regard to it.

---

88. See, e.g., Don E Detmer & Elaine B Steen, "Shoring up Protection of Personal Health Data" (1996) 12:4 Issues in Science & Technology 73.

89. Jeroen van den Hoven, "Information Technology, Privacy and the Protection of Personal Data" in Jeroen van den Hoven & John Weckert, eds, *Information Technology and Moral Philosophy* (Cambridge: Cambridge University Press, 2008) at 301. See also "Healthcare Data: Public Good or Private Property?" in Grossmann et al, *supra* note 4, 137.

90. *Canadian Charter of Rights and Freedoms*, s 7, being Schedule B to the Canada Act 1982 (UK), 1982, c 11. For examples, see *R v Morgentaler*, [1988] 1 SCR 30, 44 DLR (4th) 385; *Rodriguez v British Columbia (AG)*, [1993] 3 SCR 519, 107 DLR (4th) 342; *Cuthbertson v Rasouli*, 2013 SCC 53, [2013] 3 SCR 341. Note that the jurisprudence on autonomy is not exclusively *Charter*-based; see, e.g., *Malette v Shulman* (1990), 72 OR (2d) 417, 67 DLR (4th) 321 (CA).

91. *McInerney*, *supra* note 8.

92. See, e.g., Paul M Schwartz, "Property, Privacy, and Personal Data" (2004) 117:7 Harv L Rev 2056; James B Rule, "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions" (2004) 54:2 UTLJ 183; Thomas M Lenard & Paul H Rubin, "In Defense of Data: Information and the Costs of Privacy" (2010) 2:1 Policy & Internet 149.

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 does not operate when it comes to issues of public health, wherein societal needs take precedence; it cannot include third-party information conveyed by an individual because obtaining consent of the third party is impractical; and it is frequently given under circumstances of duress or weakness.[93] In addition to consent not functioning adequately, a second problem is that we have little actual control of our information in a number of significant ways. Legislation, common law, and organizational policies grant custodians the opportunity to engage in a wide range of uses without consent.[94] In some circumstances,

93. See O O'Neill, "Some Limits of Informed Consent" (2003) 29:1 J Medical Ethics 4; Neil C Manson & Onora O'Neill, *Rethinking Informed Consent in Bioethics* (Cambridge: Cambridge University Press, 2007).

94. For example, Ontario's *PHIPA*, *supra* note 21, s 37(1) provides for the following permitted uses without the requirement of consent:

> 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

the individual can explicitly opt out of its use, but the ability to do so is infrequent. More importantly, the individual is generally neither aware of the range of uses, nor of the ability to opt out.[95] Therefore, the individual does not control the uses of information in any meaningful sense.

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.

2. *Public good*

Health information is often argued as constituting a public good for two principal reasons. First, there are major benefits in pooling information and making it available for a range of uses.[96] This argument conforms closely to the spirit of communitarianism in that it prioritizes the public good over the individual right with respect to the uses that should be made of one's information.[97] A second argument revolves around the fact that health information is collected and rendered useful in electronic form by virtue of government funding; thus, we all contribute to the health care system by virtue of paying taxes, and therefore are entitled to reap the benefits of the public use of information collected by the system.[98] 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 and 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.[99] He is particularly concerned that the electronicization of information has given rise to major and multiple breaches of confidentiality.[100] Therefore, he argues in favour

---

Canada.

95. Jennifer Barrigar, Jacquelyn Burkell & Ian Kerr, "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information" (2006) 44:1 Can Bus LJ 54. The authors posit that consent is intended to be ongoing, and explore the psychological reasons people are reluctant to withdraw consent. However, they do not discuss the fundamental starting point that most are unaware of their ability to withdraw consent; unawareness of the entitlement disenfranchises a person of the option to withdraw.

96. David Blumenthal, "Characteristics of a Public Good and How They Are Applied to Healthcare Data" in Grossmann et al, *supra* note 4, 139.

97. Detmer & Steen, *supra* note 88 at 77-78.

98. Blumenthal, *supra* note 96 at 142-143.

99. Amitai Etzioni, *The Spirit of Community: Rights, Responsibilities, and the Communitarian Agenda* (New York: Crown, 1993); Etzioni, "Communitarian Conception of Privacy," *supra* note 6 at 450-453.

100. *Ibid.*

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 their activities have violated the law?[101]

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 lens. The risks of a violation of privacy may be heightened, and one's access to privacy and confidentiality may be more limited, depending on 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 inequality.

3. *Inequality*

The sensitivity of personal health information varies with its nature and context. For example, the fact that an individual is myopic may not be experienced as sensitive by most, but if one seeks certain types of employment, for example, 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- 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.[102] 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.[103]

---

101. Erika Kelton, "More Drug Companies to Pay Billions for Fraud, Join the 'Dishonor Roll' after Abbott Settlement," *Forbes* (10 May 2012), online: <www.forbes.com/sites/erikakelton/2012/05/10/more-pharma-companies-to-join-the-dishonor-roll-pay-billions-for-fraud-following-abbotts-settlement/>.

102. Marsha Hanen, "Genetic Technologies and Medicine: Privacy, Identity, and Informed Consent" in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009) 173.

103. Karen Eltis, "Genetic Determinism and Discrimination: A Call to Re-Orient Prevailing Human

One's access to privacy and confidentiality also depends upon one's status in society. Catherine Frazee and her colleagues conducted a series of focus groups with disabled women in Ontario to examine issues of privacy and confidentiality when accessing health care services.[104] They found that in the experience of women with disabilities, confidentiality is routinely denied in comparison with the able-bodied. They further explored the fact that disabled women disproportionately receive social assistance and other forms of government income support. These programs require 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, not of the patient. Women surveyed indicated that they feel constantly scrutinized, even by their own physicians, and the confidential nature of their relationship is seriously undermined when the physician is required 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 greater the potential that it will indeed be used in a way that impacts adversely on the person or group.

4. *Privacy as a social good*

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 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 sprivacy is likewise a social good.[105]

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

Rights Discourse to Better Comport with the Public Implications of Individual Genetic Testing" (2007) 35:2 JL Med & Ethics 282.

104. Catherine Frazee et al, "The Legal Regulation and Construction of the Gendered Body and of Disability in Canadian Health Law and Policy" (2011) National Network on Environments and Women's Health Working Paper, online: SSRN <ssrn.com/abstract=1775204>.

105. Valerie Steeves, "Reclaiming the Social Value of Privacy" in Kerr, Steeves & Lucock, *supra* note 102, 191.

May 2014, the European Court of Justice ordered that Google remove from its search engine information concerning an auction notice on the complainant's repossessed home from many years prior.[106] This has led to a considerable range of views as to whether it is ever appropriate for personal information to no longer be available.[107]

Blanchette and Johnson review the increasing trend to prioritize long-term data retention over destruction in a number of domains.[108] 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.

Mayer-Schönberger provides a stark example of the dangers in collecting and retaining information in the Netherlands in the 1930s.[109] A citizen registry had been created in order to facilitate administrative functioning and welfare planning. When the Germans invaded, they confiscated the registry and were therefore able to identify citizens classified by the Dutch government as Jewish or "Gypsy." This resulted in much higher rates of targeting of these particular populations for attempted eradication than in most other 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 with benevolent intentions toward Dutch citizens—the creation of the registry—later became a powerful malevolent force.

This example illustrates group harm caused by the 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.[110] Under the Indian Residential Schools Settlement Agreement, an Independent Assessment Process (IAP) was established to compensate survivors for abuse inflicted by the school system. The Truth and Reconciliation Commission (TRC) was also founded 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

106. *Google v AEPD*, *supra* note 16.
107. See e.g., Jeffrey Rosen, "The Right to Be Forgotten" (2012) 64 Stan L Rev Online 88, online: <www.stanfordlawreview.org>; Paul Bernal, "The EU, the US and Right to be Forgotten" in Gutwirth, Leenes & De Hert, *supra* note 61, 61; Steven C Bennett, "'The Right to Be Forgotten': Reconciling EU and US Perspectives" (2012) 30:1 BJIL 161.
108. Blanchette & Johnson, *supra* note 52.
109. Mayer-Schönberger, *supra* note 60 at 141.
110. *Fontaine v Canada (AG)*, 2014 ONSC 4585, 122 OR (3d) 1 [*Fontaine*].

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."[111]

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 the purposes of claims adjudication, 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.[112] In the interim, claimants are to be given the option of consenting to the retention and archiving of their redacted records, failing which, their records are to be destroyed.

This case serves as an interesting example on a number of levels. First, it directly pits individual privacy 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? Justice Perell answered this question essentially in individual choice and consent terms as follows: it is 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 affirms the importance of forgetting—the right of individuals to walk away from their past, to a limited extent, overshadows the societal interest in retention of the information.

111. *Ibid* at para 238.
112. *Ibid* at para 362.

Conclusion

A multi-faceted approach to the need for destruction is required. In the first instance, it is important that we retain control over our information to the greatest extent possible. This facilitates control of the shaping of our respective identities. 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 in a multitude of ways we have already lost control of decision-making surrounding our personal health information. And in this electronic era it is unlikely that we will regain control. To the extent that control is not possible, the analysis needs to go further. A granular approach to retention needs to be applied 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 has a high value to society, and so retaining the information for these purposes would deserve a relatively high degree of tolerance as compared to retaining 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.

Destruction after a set period of time should be the default position. At present, laws focus on retention time frames but a preferable system would have set times for destruction unless a case can be made that retention is in the longer-term interest. One arguing for the retention of personal health information would need to show that its high social value outweighs the privacy risks that accompany the data's retention. Part of the assessment should focus on the potential impact on groups/segments of society as well as on individuals.[113] 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."[114] The

113. In this respect the judgment of Perell J in *Fontaine*, *supra* note 110 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.

114. *Mount Isa Mines v Pusey* [1970] HCA 60, 125 CLR 383 at 395, in the context of a claim for psychiatric illness in negligence law.

health professions have been embracing electronic technologies, but 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 identities.