Protection of Health Information Privacy: The Challenges and Possibilities of Technology

FEATURE ARTICLE

BARBARA VON TIGERSTROM RECEIVED HER L.L.B. FROM THE UNIVERSITY OF TORONTO. BEFORE ATTENDING LAW SCHOOL, SHE COMPLETED HER B.A. AT THE UNIVERSITY OF ALBERTA AND HER M.A. AT THE UNIVERSITY OF TORONTO. SHE IS CURRENTLY CLERKING AT THE SUPREME COURT OF CANADA.

Taylor Jordan Chafetz (Vancouver) is pleased to sponsor the 1998 Appeal Award for Outstanding Student Legal Writing and congratulates winning author Barbara von Tigerstrom.

Legal and philosophical interest in the right to privacy has intensified in recent years along with the rapid development of new technologies. Even the famous early article by Warren and Brandeis[1] was written in response to concerns about technological innovations of the day – photography and surveillance technologies – and their use to invade the private lives of individuals.

A century later, these concerns remain, but many others have joined them. Advances in information and communications technology have increased our ability to collect, store and transmit data about individuals. While these advances are useful in many positive ways, some see them as bringing us closer to an Orwellian dystopia where "Big Brother" can watch and record the actions of every individual, and where the individual has lost control over information about herself and thus over her very life. As a reaction to these concerns, lawyers and academics have been attempting to formulate theories and policies to define the rights of individuals and the limits on the use of technology by government and other organizations with respect to personal information.

Among the categories of personal information which may be at issue in these analyses, health information is of particular interest for a number of reasons. First of all, it is widely recognized that the information which may be contained in a person's medical records is among the most sensitive kinds of personal data,[2] and thus carries serious risks for personal privacy. In addition, the privacy of health information is a universal concern which, to a greater or lesser extent, affects every member of society. In part because of these two points, the medical profession and the law has traditionally placed a high value on the confidentiality of medical information and the relationship between health care providers and their patients. Recently, this ethic has been challenged by developments in information and communications technology and by

1 S. D. Warren & Louis D. Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193.

2 "Health care information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual." L. O. Gostin et al., "Privacy and Security of Personal Information in a New Health Care System" (1993) 270:20 Journal of the American Medical Association 2487 at 2487.

...it is widely recognized that the information which may be contained in a person's medical records is among the most sensitive kinds of personal data, and thus carries serious risks for personal privacy.

changes in the structure of the health care system. The issue is all the more difficult because there are many legitimate and important reasons for the use and disclosure of health information, including the provision of health care, monitoring and improving quality of care, promotion of public health and the efficient administration of costly health care systems.

As a result of this tension, the past few years have seen intensified academic and legislative activity related to the issue of confidentiality in health care. The challenge is not only to clarify the extent and the bearers of duties to safeguard privacy, and to reconcile these duties with the efficient and effective delivery of health care services – these concerns, while difficult and in need of resolution, are not new. Concerned persons are also now struggling to identify and deal with the effects of developments in

3 See e.g. S. B. Petersen, "Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?" (1995) 48 Federal Communications Law Journal 163 at 164: "Information privacy is the right to control how information about oneself is used by those to whom it is disclosed." Westin defines privacy as the "claim of individuals, groups and institutions to determine for themselves when, how and to what extent information about them is communicated to others." A. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 32.

4 Contemporary knowledge of genetics also means that human tissue and the genetic information it contains may be traced to the individual, making the concept of "non-identifiable" samples or genetic data essentially obsolete (L. O. Gostin, "Genetic Privacy" (1995) 23 Journal of Law, Medicine & Ethics 320 at 322). This is one of the ways in which advances in genetics pose unique challenges for the privacy of health information – a fascinating topic which would require a paper of its own to do it justice. See e.g. the article by Gostin cited above and others in the same volume; R. Wachbroit, "Rethinking Medical Confidentiality: The Impact of Genetics" (1993) 27 Suffolk University Law Review 1391.

5 Gostin points out that in some cases information need not be traced to a particular individual for it to be considered sensitive; the disclosure of information about a "discrete population" such as a small community or a racial or ethnic group may also affect valid interests. L. O. Gostin, "Health Information Privacy" (1995) 80 Cornell Law Review 451 at 520. See also E. W. Clayton, "Panel Comment: Why the Use of Anonymous Samples for Research Matters" (1995) 23 Journal of Law, Medicine & Ethics 375. It is still personal information, however, which poses the greatest threat to privacy.

communications and especially information technology on patients' privacy. Despite the increased attention these matters have received, there is (perhaps predictably) as yet no firm consensus on how we should proceed. The uncertainty is no doubt due in part to the range of competing interests and objectives to be balanced, but also reflects long-standing disagreements about the nature and value of privacy, and the relationship between technology and society. It will be the aim of this article, after a very brief review of existing laws and policies on privacy, to examine some of the technological challenges to privacy in health care and proposed responses in the context of some of these larger debates about privacy and technological progress.

I. Data Protection: Legal and Philosophical Perspectives

A. The Concept of Privacy

Privacy is a broad concept which has been defined in many different ways. It may encompass a number of aspects, but generally, refers to the right or capacity to shield some aspects of one's life from the scrutiny of others, to draw a boundary between the public and private spheres of one's existence. The particular aspect of privacy which is at issue here is sometimes referred to as "information privacy": the right to control when, how and by whom personal information about oneself is communicated to and used by others.[3] Personal information, in turn, can be defined as any information about an individual which may be identified with that individual in some way. This identification need not be by name or even by anything so obvious as an identification number; there are many ways in which information may be traced to its subject, and technology is increasing the number of ways in which this may be done, by facilitating the matching of data sets, for example.[4] Whenever data may be traced to its subject, it has the potential to reveal private information about that person and is thus considered sensitive.[5]

When we speak of invasion of privacy, there are two categories of actions and actors we may be concerned with. The first, which is perhaps the one that springs first to mind, is the unauthorized collection, use or disclosure of information, which may occur when the security intended to protect the data is inadequate, and persons who are not authorized to do so obtain access to personal information. Unauthorized access may also occur when staff members breach their own duties of confidentiality and allow access by others, who then use the information for various purposes.[6] Although such violations have received much public attention, the second category, involving authorized uses, may be equally important. Some maintain that "the most serious threats to privacy come from authorized users of health information."[7] The sheer number and variety of authorized users means that widespread dissemination of personal information is inevitable, and this makes it difficult to control the use of such information.[8]

Opinions differ as to the interests and values that are protected by a right to privacy. One view sees privacy as crucial to the protection of human dignity and personality, while the other major perspective emphasizes the importance of privacy to society and social relationships.[9] An example of the former is the well-known early article on "The

6 *The Report of the Commission of Inquiry into the Confidentiality of Health Information* by H. Krever (Toronto: Queen's Printer for Ontario, 1980) [hereinafter Krever Commission] was initially ordered in response to public outcry following reports that police officers, private investigators, and others had improperly gained access to confidential health information from hospitals and the Ontario Health Insurance Plan; see vol. 1 at 1 and c. 5-13.

7 "Health Information Privacy," see note 5 at 485.

8 See above. "The Institute of Medicine found that the number of authorized users of the computer-based record is too exhaustive to list, and would parallel the complete list of individuals and organizations associated directly or indirectly with health care." See above at 485-86.

9 F. D. Schoeman, "Privacy: Philosophical Dimensions in the Literature" in F. D. Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984) 1 at 8.

10 See note 1 at 205, 211.

11 See above at 205, 211; and at 213: "the principle … is in reality not the principle of private property, unless that word be used in an extended and unusual sense."

12 See above at 197.

13 See e.g. E. J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" in Schoeman, ed., see note 9, 156 (originally published in (1964) 39 New York University Law Review 962).

Right to Privacy" by Warren and Brandeis, in which the interest protected was referred to as "inviolate personality,"[10] an interest distinct from that of private property[11] and broader than that protected by the law of slander and libel which "are in their nature material rather than spiritual."[12] Other authors have similarly emphasized the importance of privacy as respect for the dignity, integrity and autonomy of individuals.[13]

The second view is a more instrumentalist one. According to this view, without the protection of privacy, there is no possibility of intimacy, nor, therefore, of interpersonal relationships based on love and trust.[14] Privacy also plays an important role in the relationship between the individual and the state, and restraining the power of the government to gather and use information about the private lives of individuals is seen as an important means of curbing totalitarian tendencies of the state.[15] Recent articles have also emphasized the value of privacy for ensuring the participation of autonomous persons in a democratic society.[16]

The concept of privacy encompasses a variety of different interests, and some have questioned whether there is such a thing as a coherent interest in privacy as such.[17] They have also argued that the interests promoted by privacy, though important, are not unique, but rather are interests common to and protected by other areas of the law.[18] Various laws also offer protection against some of the harms that might follow from violations of privacy, such as the prohibition of discrimination on the basis of personal characteristics. The ongoing debate concerns the question of whether there are also distinct interests and harms which can only be protected by an independent right to privacy.

B. Legal Protection of Personal Information

The law relating to the protection of personal information is very complex,[19] and varies considerably among jurisdictions. For example, United States courts have recognized a limited cause of action in tort for invasion of privacy.[20] American judges have also found that a right of privacy, while not explicitly stated in the Constitution, is implicit in some of its provisions.[21] In Canada, however, only a narrow category of cases have protected an individual's "reasonable expectation of privacy" in the context of the right in section 8 of The Charter of Rights and Freedoms to be "secure against unreasonable search and seizure."[22] There have been some suggestions that the section 7 guarantee of life, liberty and security of the person may include privacy interests, but "the Supreme Court seems reluctant to make more than vague pronouncement on the matter."[23] Canadian courts have also been unwilling to recognize an independent tort of invasion of privacy, although they have applied other categories such as trespass, nuisance, libel, slander, injurious falsehood or passing off to provide remedies to plaintiffs in many of the same types of cases.[24]

In several provinces in Canada, provincial statutes create a civil cause of action in tort for the invasion of privacy,[25] and various federal and provincial statutes protect privacy in specific contexts.[26] Information held by the government is treated separately under the federal Privacy Act[27] and provincial freedom of information acts,[28] which

14 C. Fried, "Privacy" in Schoeman, ed., see note 9, 203 (originally published in (1968) 77 Yale Law Journal 475); R. S. Gerstein, "Intimacy and Privacy" in Schoeman, ed., see note 9, 265 (originally published in (1978) 89 Ethics 76).

15 See e.g. P. M. Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States" (1995) 80 Iowa Law Review 553 at 560.

16 See above; S. Simitis, "Reviewing Privacy in an Information Society" (1987) 135 University of Pennsylvania Law Review 707.

17 Schoeman, see note 9 at 5.

18 E.g. W. L. Prosser, "Privacy" in Schoeman, ed., see note 9, 104; J. J. Thomson, "The Right to Privacy" in Schoeman, ed., see note 9, 272.

19 The law on privacy was once compared to "a haystack in a hurricane" (*Ettore* v. *Philco Broadcasting Co.,* 229 F. 2d 481 (3d Circuit 1956), quoted in Prosser, see above at 117.) This survey, necessarily brief, will not attempt to untangle all the various strands of the law relating to privacy, nor does it pretend to be exhaustive.

20 The common law cause of action in the United States is based on four categories set out in an article by Dean Prosser: intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; public disclosure of embarrassing facts; publicity which places the plaintiff in a false light; and appropriation of the plaintiff's name or likeness, see note 18 at 107.

21 See e.g. *Griswold* v. *Connecticut*, 381 United States [Reports] 479 [1965] (Supreme Court); *Whalen* v. *Roe*, 429 United States [Reports] 589 [1976] (Supreme Court).

provide protection against the disclosure of personal information and allow an individual to access information about herself (as well as other publicly held information). Quebec is unique in that it provides an explicit right to privacy in its Charter of Human Rights and Freedoms,[29] limits the right of persons to collect, use and disclose personal information about others in the Civil Code,[30] and, most notably, is the only province with legislation protecting personal information held by the private sector.[31]

Internationally, the past few decades have seen the development of standards for the protection of personal information. The right to privacy is recognized in several international agreements on human rights, including the International Covenant on Civil and Political Rights[32] and the European Human Rights Convention.[33] Canada has also formally adopted the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)[34] which were developed in 1980 to help harmonise national privacy legislation and thereby facilitate the international flow of data.[35] Although the OECD Guidelines are not binding, they have been extremely influential in the development of laws and policies on personal information throughout the world, including New Zealand's Privacy Act 1993.[36] The Guidelines set out eight basic principles:[37]

Collection limitation – data should be collected by fair and lawful means, and should be limited.

Data quality – data should be relevant, accurate, complete, and up to date.

Purpose specification – the purposes for which data is collected should be specified at the time of collection and use should be limited to those and compatible purposes.

Use limitation – personal data should not be used or disclosed for other than specified and compatible purposes except with consent or by legal authority.

Security safeguards – personal data should be secured against loss, unauthorized access, etc.

Openness – policies and practices should be open, and people should be able to find out what information is being kept and used for what purposes and by whom.

Individual participation – the individual should have the right to know whether a data controller has information about him; to have timely, affordable and effective access to that information; and to challenge its accuracy.

Accountability – the data controller is accountable for compliance with these principles.

The principles, which have come to be called, collectively, "fair information practices," include some protection for personal privacy but also a number of other related concerns, for example ensuring the accuracy of information and transparency of policies and procedures.

C. Privacy of Health Information

Health law has always placed a high value on the autonomy of individual patients. This shows itself mostly in the requirement of informed consent and the idea, expressed most famously by Justice Cardozo in *Schloendorff* v. *Society of New York Hospital* that

22 Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c.11 [hereinafter Charter]. See e.g. *R.* v. *Duarte* [1990] 1 Supreme Court Reports 30 (Supreme Court); *R.* v. *Dyment* [1988] 2 Supreme Court Reports 417 (Supreme Court of Canada).

23 D. C. Kratchanov, "Personal Information and the Protection of Privacy" in *Ensuring Privacy Protection on the Information Highway* (Toronto: Insight Press, 1995) 97 at 108.

24 G. H. L. Fridman, *The Law of Torts in Canada*, vol. 2 (Toronto: Carswell, 1990) at 192.

25 Privacy Act, Revised Statutes of British Columbia 1996, c. 373; Privacy Act, Revised Statutes of Saskatchewan 1978, c. P-24; Privacy Act, Re-enacted Statutes of Manitoba 1987, c. P-125; Privacy Act, Revised Statutes of Newfoundland 1990, c. P-22.

26 See Fridman, see note 24 at 197-98. See also Kratchanov, see note 23 at 110-11.

27 Revised Statutes of Canada 1985, c. P-21.

28 E.g. Freedom of Information and Protection of Privacy Act, Statutes of Alberta 1994, c. F-18.5.

29 R.S.Q. 1977, c. C-12 (Supp. 1993), section 5.

30 S.Q. 1991, c. 64, sections 35-41.

31 Act Respecting the Protection of Personal Information in the Private Sector, S.Q. 1993, c. 17. For a discussion of the Quebec legislation, see P.-A. Comeau & A. Ouimet, "Freedom of Information and Privacy: Québec's Innovative Role in North America" (1995) 80 Iowa Law Review 651.

32 16 December 1966, 999 United Nations Treaty Series 171, article 17(1): "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

"every human being of adult years and sound mind has a right to determine what shall be done with his own body."[38] Respect for the patient as an autonomous individual is also implicated in the physician's duty not to breach the confidence of her patient and the patient's ability to claim a measure of control over her own health information.[39] The instrumental value of privacy in the health care setting involves the importance of a patient's trust in his care providers. If a patient fears disclosure of personal information, he may avoid seeking treatment[40] or offer false information, potentially harming both his own health and that of others.[41]

Much of the law on personal data is also applicable to medical information; for example in Canada medical records held by public institutions such as hospitals and health boards may be covered under provincial information and privacy legislation.[42] In the health care context there are additional sources of ethical and legal obligations to respect patients' privacy, however, and several jurisdictions have found it appropriate to pass separate legislation specific to health information.

Physicians have obligations to preserve confidentiality under the Hippocratic Oath and the codes of conduct of professional bodies.[43] Breach of these obligations may leave a physician open to disciplinary proceedings by those bodies. A common law action may also be brought on a number of bases,[44] including breach of confidence, negligence, breach of contract[45] and breach of fiduciary duty.[46] These actions may not be effective ways of enforcing a patient's rights,[47] and are subject to exceptions and gaps in protection.[48] Perhaps the most serious problem is that most of these duties, even if they can be effectively enforced, apply only to physicians. Dozens if not hundreds of other people may have access to any one person's health records, and the nature and extent of their duties may be unclear. Computerization of records exacerbates this problem since it may make it difficult to determine who "holds" the record and thus bears the responsibility of protecting it.[49]

In response to concerns raised by the incomplete protection provided by the common law and intensified by technological developments, several jurisdictions have developed specific laws for the protection of health data. New Zealand issued the Health Information Privacy Code 1994[50] under its Privacy Act 1993[51] which sets out twelve health information privacy rules, incorporating the OECD principles as well as more detailed provisions on use and disclosure, and limits on the use of unique identifiers. The past few years have seen a number of proposed acts in the United States, including the Fair Health Information Practices Act 1997,[52] the Medical Privacy in the Age of New Technologies Act[53] and the Medical Records Confidentiality Act of 1995.[54] In Canada, no similar legislation yet exists, although a number of provinces are considering the possibility of enacting health information legislation.[55] In June 1997 a proposed Health Information Protection Act was introduced in the Alberta Legislature.[56] The bill is currently being studied by a government committee, and the government has invited public comment in anticipation of the bill being reintroduced in 1999. More recently, in

33 Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 United Nations Treaty Series 221, article 8(1): "Everyone has a right to repect for his private and family life, his home and his correspondence."

34 Reproduced as Appendix 1 in J. Michael, *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (Paris: UNESCO Publishing, 1994) at 139-44. (OECD is the Organization for Economic Cooperation and Development.)

35 Kratchanov, see note 23 at 112. Canada adhered to the Guidelines in 1984.

36 Statutes of New Zealand 1993, No. 28.

37 The principles appear as articles 7 to 14 of the OECD Guidelines, see note 34.

38 (1914), 105 North Eastern Reporter 92 (New York Court of Appeal) at 93.

39 *McInerney* v. *MacDonald*, [1992] 2 Supreme Court Reports 138 (Supreme Court of Canada) at 148: Health information is "information that goes to the personal integrity and autonomy of the patient." The patient "has a 'basic and continuing interest in what happens to this information, and in controlling access to it.'"

40 S. E. Corsey, "The American Health Security Act and Privacy: What Does it Really Cost?" (1994) 12 Journal of Computer and Information Law 585 at 599.

41 This is a major issue in public health policy, since it is feared that mandatory reporting of communicable and sexually transmitted diseases, while important for public health authorities, may deter people from seeking diagnosis and treatment.

late 1997 the Ontario Ministry of Health released a draft Personal Health Information Protection Act, 1997,[57] which is similar to the Alberta bill in many respects.

II. Technological Developments and Their Impact on Privacy

Although concerns about privacy are common to all societies at various stages of technological development,[58] advances which have taken place over the last few decades are seen as greatly increasing the potential for the invasion of privacy. It is increasingly difficult to draw strict boundaries between various types of technology, but two broad categories, communications and information technology, will be examined here.

A. Communications Technology

Although most attention has been focussed on information technology, "a revolution in communications technology has redirected policy attention to another issue that has long been pertinent – the protection of personal communication channels."[59] New technologies such as the facsimile (fax), cellular communications and various types of computer networks have increased the ease and speed of transmitting information in numerous forms and in unprecedented quantities. The benefits of these for improving the quality and efficiency of medical care are unquestionable: they allow convenient and accurate communication for consultations among health care providers, and between care providers and their increasingly mobile patients. A whole field, known as "telemedicine," is developing to make use of communications technology to provide better care to patients in remote locations, and to allow consultation with specialists without the necessity of costly and difficult travel.[60] Telemedicine is also increasingly being used in the education of health practitioners.[61] All of these uses are important in improving the quality of care and access to care, and in reducing costs – it has been estimated that "America's health care expenses might be reduced by more than $36 billion annually with more efficient use of telecommunications."[62]

Confidentiality concerns have been raised with respect to a number of aspects of such communications. For example, do transfers of data for specialty consultations require the consent of the patient?[63] What about transmission of images or other information for teaching purposes? In addition to these deliberate disclosures, there is always the potential for interception and use of data by unauthorized persons.[64] Cellular telephones, for instance, are particularly vulnerable to interception.[65] Interception may occur through the intentional efforts of the unauthorized persons or by mistake, as, for example, when information is accidentally sent by fax to someone other than the intended recipient. Policies will have to be developed to deal with these potential threats to privacy.

B. Information Technology

Most of the recent discussions about the protection of personal information and in particular health information have focussed on the impact of developments in information technology and the increasing use of computerized record systems. "The health care industry is in the midst of an era of unprecedented computerization of medical records

42 See e.g. Freedom of Information and Protection of Privacy Act, above note 28, section 1(1)(g), (j). The British Columbia Freedom of Information and Protection of Privacy Act, Statutes of British Columbia 1992, c.61, since 1995 has covered, in addition, professional governing bodies such as the College of Physicians and Surgeons. Freedom of Information and Protection of Privacy Act (Amendment), Statutes of British Columbia 1993, c.46, section 28(6), section 30. E. Shaw, J. Westwood & R. Wodell, *The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them* (Vancouver: B.C. Civil Liberties Association, 1994) at 103. A similar amendment is proposed for Alberta; see "Information and Privacy Legislation Being Extended First to Education and Health Care," Government of Alberta News Release, August 27, 1997.

43 W. H. Minor, "Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections" (1995) 28 Columbia Journal of Law & Social Problems 253 at 278-79; Shaw, Westwood & Wodell, see above at 100.

44 Shaw, Westwood & Wodell, see note 42 at 102; "Health Information Privacy," see note 5 at 509.

45 Courts may incorporate a duty of confidentiality into an implied contract between physician and patient; "Health Information Privacy," see note 5 at 509 n. 292; S. Rodgers-Magnet, "Common Law Remedies for Disclosure of Confidential Medical Information," "Appendix 1" in Krever Commission, see note 6, vol. 3, 297 at 323.

46 *McInerney* v. *MacDonald*, see note 39 at 148-50.

47 Shaw, Westwood & Wodell, see note 42 at 102.

and data."[66] Computerizing records is part of many health care reform proposals, since it would not only increase efficiency but also significantly cut costs.[67] However, the general public is apparently nervous about the potential effects of these changes: in recent polls 85 per cent of people said that protecting confidentiality of medical records was very important to them, and 90 per cent believed that computers make it easier for someone to improperly obtain personal information.[68] While there is some disagreement about the exact nature and extent of the impact of technology on the protection of privacy, there is no doubt that "pervasive use of computers has enhanced society's ability to collect, store, retrieve, process, and disseminate data on individuals, quite often without the individual's knowledge and consent."[69]

For instance, the ease of recording and storing information in computer databases may mean that information will be collected and retained that might not have been otherwise.[70] The centralized storage of large amounts of information also increases the likelihood and severity of breaches of privacy. Traditionally, records have been kept in manual form in a number of different (and usually secure) locations, making it difficult to obtain information and especially to obtain and combine a wide range of data from various sources.[71] Unless special protections are built into the system, access to a database can provide an authorized or unauthorized user with an unprecedented amount of information. Even when different sets of data are held in different systems, it is often possible to "link" or "match" the data for a particular individual using some identifier. This practice, known as computer matching, presents a serious threat to personal privacy since it allows a user to compile a detailed dossier or profile on an individual by linking data from many different sources,[72] and thereby acquire extensive knowledge about that person,[73] without the individual's knowledge or consent. Matching may also detach information from its context and lead to the proliferation of false or misleading information.[74]

As a result, the means by which health information is identified in a computer system has become extremely important. In health care, the use of unique identifiers (a name, number or other unique marker for each individual)[75] would allow a comprehensive record for each patient to be compiled from information scattered geographically and over the years. These "patient-based longitudinal records," which would contain "all data relevant to the health of an individual … collected over a lifetime,"[76] would carry obvious benefits for quality of care and administrative efficiency. However, the additional threat to privacy means that limits on the use of unique identifiers may be appropriate.[77] Of special concern is the use of an identifier that would allow links to be made between health records and other forms of personal data. For example, privacy advocates in the United States strongly resisted the proposed use of the social security number (SSN) as an identification number for the reformed health care system.[78] Because of the widespread use of the SSN by both government and private entities, the SSN may be used to access and link information about many aspects of a person's life.[79] Those concerned about privacy are alarmed at the prospect of this pool of information

48 "Health Information Privacy," see note 5 at 509-11.

49 See above at 511.

50 New Zealand Privacy Commissioner, Health Information Privacy Code 1994 (Auckland, N.Z.: Privacy Commissioner, 1994). Found at http://www.knowledge basket.co.nz/privacy/health/hipcnc.htm.

51 See note 36.

52 H.R. 52, 105th Congress, 1st Session. Found at ftp:/ftp.loc.gov.pub/thomas /c105/h52.ih.txt. This bill was introduced in the House of Representatives January 7, 1997 by California Representative Gary Condit. Condit introduced earlier versions of this bill in 1994 and 1995 (H.R. 435), which were supported by industry representatives, privacy advocates and health policy experts; J. Goldman, "Statement of Janlori Goldman, Deputy Director, Center for Democracy and Technology, Before the House Committee on Government Reform and Oversight Subcommittee on Government Management, Information and Technology on Medical Records Technology," found at http://www.cdt.org/privacy/health/960614_testimony.html.

53 House of Representatives 3482, 104th Congress, 1st Session.

54 S. 1360, House of Representatives 52, 105th Congress, 1st Session.

55 See Ontario Ministry of Health, *A Legal Framework for Health Information* (Consultation Paper) June 1996; Manitoba Health, *Privacy Protection of Health Information* (Discussion Paper) May 1996.

56 Bill 30, Health Information Protection Act, 1st Sess., 24th Leg., Alberta, 1997 [hereinafter Bill 30].

57 Found at http://www.gov.on.ca/health/english/profess/phipa/phipa.html on 12 February 1998.

including intimate details about a person's health. The use of a number specific to the health care system would help to alleviate these concerns.[80]

The choice of an identifier is one issue to be considered with respect to health care cards. Developing technology has also added other issues, however. Various types of cards have been used for identification and insurance purposes in the health care system for many years. Typically, these cards carried basic information that was printed or embossed on the card.[81] Several types of "advanced card technologies" ("smart cards") are now available, including magnetic strip, integrated circuit and optical storage cards.[82] These cards can not only store much larger amounts of information (including images such as x-rays, for optical storage cards), but can also process information and be used to access central databases.[83] The cards could be used for identification, insurance, communication between care providers and as a portable, comprehensive patient records, which could be valuable for emergency and outreach care.[84] Pilot projects have already begun testing the use of such cards in many countries, including Canada.[85] Reactions have been ambivalent: some fear misuse of smart cards – the cards would be vulnerable to theft or fraudulent use by third parties – while others feel that use of these cards could actually enhance individuals' control and privacy.[86]

New information technologies also pose significant challenges for the definition and enforcement of duties to protect privacy. For example, since a centralized database containing health records could be accessed from a number of different points in a connected system of computers, in contrast to a paper record which is physically located in one place, it may be difficult to determine who should bear the primary responsibility for ensuring that no unauthorized access takes place. Furthermore, physical security measures,[87] while essential, will not be sufficient to protect computerized records; efforts must be made to build security into the system itself. Another enforcement problem is that with computerized data, a breach of security may be difficult or impossible to detect. "In an electronic, on-line system, the data can be viewed, studied, and downloaded from any location. The viewer of the information has not acquired any physical materials, making any theft virtually undetectable."[88]

C. Using Technology to Protect Privacy

Although the literature has chiefly emphasized the threats to privacy that are posed by new technologies, some authors recognize that technology also has the potential to protect personal information. While no system can ever offer perfect security, "[p]resent health information technology can provide appropriate safeguards and can protect health information" if it is appropriately designed, monitored and maintained.[89] In addition to all the usual measures to secure manual records, such as limiting physical access and placing controls on staff members with access to the records,[90] security features can be built into the software of computerized information systems.[91] The extent to which new technologies threaten privacy depends to a large extent on the implementation of such measures.

58 See R. F. Murphy, "Social Distance and the Veil" in Schoeman, ed., see note 9, 34 (originially published in (1964) 66 American Anthropologist 1257); A. Westin, "The Origins of Modern Claims to Privacy" in Schoeman, ed., see note 9, 56 (originally published as part of A. Westin, *Privacy and Freedom* (New York: Atheneum, 1967)). Of course, what is considered private may vary among societies.

59 F. W. Weingarten, "Communications Technology: New Challenges to Privacy" (1988) 21 John Marshall Law Review 735 at 735.

60 D. D. Bradham, S. Morgan & M. E. Dailey, "The Information Superhighway and Telemedicine: Applications, Status, and Issues" (1995) 30 Wake Forest Law Review 145. Some of the applications include electronic information exchange, image transfers (e.g. ultrasound, x-rays) and consultation by telephone or videoconferencing. See above at 152-59.

61 The first telemedicine project, dating back to the 1950s, involved teleconferencing lectures transmitted between state hospitals. See above at 149.

62 See above at 147.

63 See above at 162.

64 See above.

65 Privacy Commissioner of Canada, *Annual Report* 1992-93 (Ottawa: Privacy Commissioner of Canada, 1993) [hereinafter Privacy Report 1992-93] at 19-20. There are statutory and criminal prohibitions on some interceptions of private communications, e.g. in Canada Criminal Code, Revised Statutes of Canada 1985, c. C-46, ss. 183-196; Radiocommunication Act, Revised Statutes of Canada 1985, c. R-2, s.9; in the United States Omnibus Crime Control and Safe Streets Act of 1968, 18 United States Code Annotated § 2510 (West 1970 & Supp. 1987) (the "Title III Wiretap Act"); Electronic Communications Privacy Act, 18 United States

For example, "[i]n the absence of protections, the holder of an identity card that allows the retrieval of [personal] information is stripped of her ability to control the flow of personal, private information."[92] However, the ability to program a "smart card" means that it "could also be used as part of an access control system to protect personal data. The memory of a smart card could be divided into several zones, each with different levels of access and security … Several technologies are available to restrict access to sensitive data, including personal identification, user verification, and cryptography."[93] Given these protections, some claim that smart cards could actually enhance privacy and individual control of personal information. This is unlikely since the information on the card would probably be duplicated in a central database,[94] but at least a properly designed card would not significantly increase the risk to privacy.

Security features to restrict access could also be built into central databases, however. Methods to identify users and restrict access include passwords and identification numbers, physical devices such as cards and keys, and physical characteristics (fingerprints, voice sample, retina scans).[95] Differentiated levels of security could, for example, allow a physician to "have access to the complete medical file, while an individual in the billing department would only have access to that data necessary for proper billing."[96] The system, having recorded all requests for access, could produce a record of all disclosures, sometimes referred to as an audit trail, which "can help determine if there has been inappropriate or fraudulent access."[97]

Other security measures could include designating terminals for particular uses and restricting their functions to those uses, for instance data input only, or reading (but not modifying) particular types of data.[98] Alarms triggered by multiple attempts to access information would help to deter unauthorized persons,[99] and requiring medical staff to be responsible for use of their passwords (which the computer would record and report) would discourage them from disclosing their passwords to unauthorized users.[100] Various methods of encryption could also be used to make access more difficult.[101] Encryption may also be an important way of reducing the risk of interception of electronic communications.

III. Responses to Technological Developments

Priscilla Regan has described different types of responses to the development of new technologies and their impact on privacy:

> Despite the fact that it was possible to invade privacy before a particular technology was used, debate about technology and privacy inevitably revisited the question about the importance of the technology. Did the technology cause the privacy invasions? Or did technology exacerbate threats to privacy that already existed? Or was the technology itself neutral, not playing a direct role but making possible either increased privacy or diminished privacy depending on those who applied the technology?[102]

Regan goes on to define three "schools of thought on the role of technology and social change."[103] The first, the "technology determinists," believe that "technology has become an end in itself … a force subject to no external controls," and that social changes follow inevitably from technological changes.[104] The opposite view, that of the

Code § 2510 (West Supp. 1987). For a discussion of the difficulty of designing legislation to deal with rapidly changing communications technology, see R. S. Burnside, "The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunications Technologies" (1987) 13 Rutgers Computer & Technology Law Journal 451.

66 Minor, see note 43 at 254.

67 Corsey, see note 40 at 586. See also Minor, above at 294: billions of dollars could be saved each year through administrative simplification, more efficient research, and fraud prevention.

68 Goldman, see note 52.

69 Petersen, see note 3 at 164.

70 L. M. Benjamin, "Privacy, Computers and Personal Information: Toward Equality and Equity in an Information Age" (1991) 13 Communications & Law 3 at 4.

71 "Health Information Privacy," see note 5 at 494.

72 Petersen, see note 3 at 168.

73 "Health Information Privacy," see note 5 at 494.

74 Simitis, see note 16 at 718-19.

75 In 1993, the Province of Alberta assigned all eligible residents a "Personal Health Number," which is a unique identifier to be kept for life by each individual. Alberta Health, *1993-1994 Annual Report* at 23.

76 "Health Information Privacy," see note 5 at 458.

77 In 1991, Ontario enacted the Health Cards and Numbers Control Act, Statutes of Ontario 1991, c.1. The New Zealand Health Information Privacy Code 1994, see note 50, limits the use of unique identifiers (rule 12).

78 "Health Information Privacy," see note 5 at 459-61. Although this debate has largely taken

"technology neutralists," is that "technology has no independent force … [and] remains under human control. It is possible to anticipate all possible effects of technological change and to choose the end desired."[105] Finally, the middle view taken by "technology realists" maintains that a "dynamic relationship" exists between technology and society and that "the actual direction of change depends on both the capabilities of the technology and the uses to which it is put." Social policy is reactive and cannot have complete control: "technology determines the range of choices, and not all consequences of a choice can be predicted."[106]

The identification of these schools of thought is useful in analyzing the various responses to technological changes in health information, although it is probably more accurate to describe the range of views as a spectrum than as a set of strict categories. At one end of the spectrum are those who maintain that technology has not effected any substantial change on the processing and use of information; computers and modern communications devices are merely new vehicles for the same operations. Therefore only the most minimal of changes is necessary, for example changing definitions in legislation to include the new forms of records, either by legislative amendment or by judicial interpretation. Until quite recently, this appeared to be the approach that was in fact taken in several areas of the law: computer programs were deemed to be literary works in copyright law,[107] and fraud and theft using computers were dealt with, however unsuccessfully, under traditional criminal statutes.[108] Even recent health information bills in the U.S. have merely broadened definitions of "protected health information" to include information "recorded in any form or medium"[109] and directed the holder of information to formulate adequate security measures.[110] The definitions of "health information" and "record" in the recent Alberta bill includes information "in any form."[111] Its definition of "anonymous individual health information" contemplates the encryption of information.[112] It is interesting to note, however, the Ontario draft act does contain some provisions specifically dealing with electronic transfer of information[113] and computer linkage of records.[114]

Although legal responses have generally been limited to these minimal modifications, there appears to be a consensus among academic writers that technological developments are resulting in substantial effects on privacy protection. Even if new technologies merely facilitate rather than cause invasions of privacy, the mere fact that technology makes serious breaches easier is significant. "It is a cliché, but nevertheless true, that the inherent inefficiency of manual filing systems was quite an effective privacy protection device until recent advances in automatic data processing. … The major change has been one of scale as well as intensity."[115] There is nearly universal agreement, then, on the fact that technology is having a substantial effect on informational privacy. However, there is much less consensus on the appropriate approach to be taken in response to these changes.

place in the U.S., similar problems have arisen in Canada; see discussion of the use of the Social Insurance Number as a health care number in Prince Edward Island, *Privacy Report 1992-93,* see note 65 at 30-31.

79 "Health Information Privacy," see note 5 at 460; Minor, see note 43 at 265-68.

80 "Health Information Privacy," see above at 461; Minor, see above at 277.

81 M. Campbell, "Advanced Technology in the Health Care Sector: Selected Legal Implications" (1992) 13 Health Law Canada 164 at 164.

82 See above at 164-65.

83 See above.

84 See above at 165.

85 "Health Information Privacy," see note 5 at 462. For examples of Canadian projects, see Privacy Commissioner of Canada, *Annual Report 1995-96* (Ottawa: Privacy Commissioner of Canada, 1996) at 6-8.

86 "Health Information Privacy," see note 5 at 463.

87 A list of recommended physical security measures for computer systems is set out in Krever Commission, see note 6, vol. 2 at 182-84.

88 "Health Information Privacy," see note 5 at 494. For a discussion of similar problems in the investigation and prosecution of "computer crimes," see M. A. Jurkat, "Computer Crime Legislation: Survey and Analysis" (1986) 2 Annual Survey of American Law 511.

89 Campbell, see note 81 at 166.

90 One physical security measure specifically suggested for computers is the use of "[l]ine-of-sight barriers … to prevent unauthorized individuals from reading terminal displays while others are using them." J. D. Cohen, "HIV/AIDS Confidentiality: Are Computerized Medical Records Making Confidentiality Impossible?" (1990) 4 Software Law Journal 93 at 111.

A. Enhancing Privacy Protection in the Information Age

A considerable amount of effort has been expended in trying to develop a legal and technological framework for protecting privacy in the context of the new methods of recording, storing and transmitting data. Institutions are being encouraged to devise and implement policies that take into account the additional challenges of technological developments.[116] As we saw above, a variety of security measures have been identified to help ensure privacy of personal data. An implicit "technology neutral" perspective assumes that although technology poses threats to privacy, the law and technology itself can be effective in countering these threats, and some even claim that "[a]utomation of health data is … an opportunity to *improve* informational privacy."[117]

Although the potential for technological and legal protections of privacy do seem promising, several factors indicate that our optimism should be cautious and qualified. To put it in Regan's terms, the more appropriate response would be a realist one which recognizes that we cannot have complete control in the face of rapidly developing technologies. Technological safeguards may be effective in making access to records difficult – perhaps even more difficult than in traditional manual record systems. However, all admit that no security system is perfect, and we must acknowledge the possibility of unauthorized access in even the best designed system. If access is obtained, the new technology makes any breach of security more serious by allowing easier access to larger amounts of data and facilitating the processing of data for use in ways not anticipated, let alone consented to, by the data subjects. The only way to avoid this problem would be to severely limit the *collection* of data so that it is simply not there to be accessed. However, this cannot be an acceptable solution, at least in the health care context, where many "powerful reasons exist for the broad collection and use of health data."[118]

Matters are further complicated if we recall the distinction between threats to privacy from authorized versus unauthorized users. The development of security measures focusses on preventing unauthorized access to information systems and their records. However, new technologies also expand the range of authorized users and uses of information, and restricting the range of authorized uses and disclosures involves much more difficult policy choices that balance individual interests in privacy with potential benefits in terms of quality of care, efficiency and public health protection.[119]

B. Is Privacy Obsolete?

In the face of these difficulties, some have taken the more radical stance that technology has made privacy impossible and that we should treat the whole notion of protecting privacy as obsolete. This deterministic attitude sees technology as driving society and social values, not the other way around.[120] Rather than keep up the futile exercise of trying to protect privacy, we should dispense with that concept altogether and turn to other, more appropriate paradigms for the management of information.

A compromise approach might retain a fairly high standard of security and privacy only for certain kinds of extremely sensitive data. For example, the American Medical

91 For a description of various physical and access and information control measures, see Corsey, note 40 at 602-604.

92 Minor, see note 43 at 256.

93 "Health Information Privacy," see note 5 at 462-63.

94 See above at 463.

95 Cohen, see note 90 at 111, n. 145.

96 See above at 111-12.

97 "Health Information Privacy," see note 5 at 492.

98 Krever Commission, see note 6, vol. 2 at 184.

99 See above at 185.

100 Cohen, see note 90 at 112.

101 Krever Commission, see note 6, vol. 2 at 185.

102 P. M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill, NC: University of North Carolina Press, 1995) at 11.

103 See above.

104 See above.

105 See above at 12.

106 See above at 13.

107 Copyright Act, Revised Statutes of Canada 1985, c. C-42, section 2: "'literary work' includes ... computer programs ... ."

108 Jurkat, see note 88 at 513ff.

109 See e.g. Medical Records Confidentiality Act of 1995, see note 54, section 3(14); Fair Health Information Practices Act 1997, see note 52, section 3(3).

110 Medical Records Confidentiality Act of 1995, see above, section 111; Fair Health Information Practices Act 1997, see above, section 105.

111 Bill 30, see note 56, sections 1(1)(g), (n).

112 See above, section 1(1)(b): "'anonymous individual health information' means health information in which identifying facts have been removed or encrypted."

113 See note 57, section 4(5).

114 See above, Part IV.

Record Association guidelines recommended that at least in some facilities, data on HIV and AIDS should not be included in computer databases at all, but should be restricted to manual files.[121] If we doubt that any safeguards can be adequate, it may be preferable to remove particularly sensitive records from new record keeping systems altogether. Alternatively, a high level of physical and technical security, too costly and impractical for use in the whole system, could be put in place to protect highly sensitive information. American health policy has already showed a tendency to provide different levels of privacy for categories of information considered to be more sensitive: for example, there are special laws protecting the records of drug and alcohol rehabilitation centres,[122] and most states have specific legislation targeting HIV/AIDS information.[123]

There are a number of problems with such an approach, however. First of all, a clear discrepancy in the treatment of specific types of information may actually defeat the purpose of protecting privacy, since it can lead, for example, to the result that "the very fact that a certain individual's health record is confidential discloses the fact that the individual has HIV."[124] Second, the kind of information that is highly sensitive may vary considerably from individual to individual, and many different kinds of information – an almost infinite variety – must be considered potentially sensitive.[125] Access to apparently innocuous information may also have serious consequences if it can be linked to other information.[126] A strict categorical approach also is unresponsive to legitimate needs for disclosure and use of information classified as sensitive.[127]

Furthermore, one school of thought holds that privacy actually has negative effects on individuals and society. "One argument for [protecting privacy] was that intimate facts about oneself … are often embarrassing if disclosed to others than those to whom we choose to disclose them." Far from enhancing our dignity or autonomy, however, "[w]e have made ourselves vulnerable – or at least far more vulnerable than we need be – by accepting that there are thoughts and actions concerning which we ought to feel ashamed or embarrassed."[128] Applying this view to the specific problem of protecting sensitive information, we must take seriously the possibility that by creating special categories of information – HIV status, a history of substance abuse or psychiatric care – to be protected with the utmost secrecy, we are in fact further stigmatizing individuals to whom those categories apply. The implication is that some kinds of medical conditions are acceptable for public knowledge, but others must be kept hidden. Although an individual is, in theory, free to waive the privilege of privacy, there is a strong suggestion that she should not do so.

Some might argue that these concerns should lead us away from the notion of privacy altogether, and toward accepting that we should not seek to conceal information about our past or present health for fear of perpetuating the idea that we should be ashamed of it. Unfortunately, given the great personal cost that we know often does result from disclosure of, for example, a person's HIV status, to adopt such an approach as a matter of public policy would be unfair and irresponsible. It seems that a better

115 Michael, see note 34 at 8. See also L. A. Albinger, "Personal Information in Government Agency Records: Toward an Informational Right to Privacy" (1986) 2 Annual Survey of American Law 625 at 627: "In the past, the very difficulty of record-keeping provided some privacy protection. Records often were handwritten, unwieldy, seldom reproduced, easily lost or destroyed, or too widely dispersed to be conveniently collected."

116 See e.g. note 110 and accompanying text; Cohen, see note 90 at 111ff; Krever Commission, see note 6 at 182ff. See J. R. Reidenberg, "Setting Standards for Fair Information Practice in the U.S. Private Sector" (1995) 80 Iowa Law Review 497 for a skeptical view on the effectiveness of relying on voluntary adoption of fair information practices in the private sector.

117 "Health Information Privacy," see note 5 at 492 (emphasis in original). See also Krever Commission, see note 6, vol. 2 at 161.

118 "Health Information Privacy," see note 5 at 453.

119 See "Health Information Privacy," note 5 at 471ff for a discussion of these and other anticipated benefits of a health information infrastructure.

120 See above at 4; Regan, see note 102 at 11.

121 Cohen, see note 90 at 108.

122 "Health Information Privacy," see note 5 at 503.

123 Cohen, see note 90 at 104.

124 Minor, see note 43 at 282, quoting submissions to Subcommittee hearings on the Fair Health Information Practices Act 1994.

125 "Health Information Privacy," see note 5 at 503-504.

126 Krever Commission, see note 6 at 170-71. One of the unique properties of information is its potential for synergies in combination with other information. See e.g. R. C. Dreyfuss & D. W. Leebron, "Foreword:

alternative would be to define a minimum, uniform required level of privacy for all health information, and allow individuals to designate specific items or categories of information which they do not wish to be disclosed.[129]

Another approach might be to dispense with protecting privacy itself and instead direct our attention to preventing the harms that may result from disclosure and improper use of personal information. Anti-discrimination laws can be amended or interpreted to ensure that discrimination on the basis of information gained by access to an individual's health record is subject to legal sanction. Human rights legislation typically includes "physical disability" as a prohibited ground of discrimination;[130] this language has been interpreted to include AIDS and HIV and other physical conditions.[131] The influence of this approach can be discerned from the fact that despite some attempts to draft a bill to protect the privacy of genetic information,[132] current legislative activity in the United States is focussed on bills designed to deal with the effects of access to genetic information, in particular discrimination on the basis of genetic characteristics in insurance.[133]

There is no doubt that anti-discrimination laws can help to prevent harm to individuals from the disclosure and use of their health information. The range of harms targeted by such laws is limited, however. Even assuming that the laws are effective in preventing discrimination in employment, housing, public services and the like, they cannot prevent more subtle but equally serious harms, for example to an individual's interpersonal relationships. Exclusive reliance on legal prohibitions of certain types of harms that may flow from improper use and disclosure is only an acceptable approach if we deny that there are unique, independent interests protected by the right to privacy, such as the injury to one's dignity and intimate relationships.

As we saw above, there are some writers who insist that privacy as such is superfluous as a legal concept because all of the relevant interests can be protected in other ways.[134] Especially now that technological developments have increased the difficulty and cost of protecting privacy, it would be foolish, if this is true, to continue to focus our attention on privacy rather than on those other aspects which are more easily dealt with in the information age. For instance, several experts[135] in the area have forcefully maintained that we must do away with the idea of privacy as "informational seclusion" and instead work to foster the individual's ability to control the use of information – a right to "informational self-determination."[136] This approach begins with the recognition that "in many instances the processing of personal information will take place" and then looks at how to "create a structure within which personal data may be utilized while an individual's capacity for decisionmaking is respected and encouraged."[137] Perhaps privacy was valued for its role in enhancing personal autonomy, but by controlling the use of information, and ensuring that information processing is procedurally fair and transparent, the same goal may be achieved in a way that is more appropriate to the contemporary context.

Privacy and Information Technology" (1986) 2 Annual Survey of American Law 495 at 497: "Two separate pieces of information may be worth little, while the combination is worth a fortune."

127 "Health Information Privacy," see note 5 at 503.

128 R. A. Wasserstrom, "Privacy: Some Arguments and Assumptions" in Schoeman, ed., see note 9, 317 at 330.

129 For example, Alberta's Bill 30, see note 56, provides in section 16(1) that an individual or her representative may request at any time that a record or any portion of a record containing personal health information not be disclosed in the context of the provision of health services without consent. The Ontario Draft Personal Health Information Protection Act (see note 57) has a similar provision in section 14(1)(1.), which says that the subject of personal health information may instruct the custodian of the information in writing that certain information is not to be disclosed for the purposes of providing or facilitating health care to the subject.

130 E.g. Human Rights, Citizenship and Multiculturalism Act, Revised Statutes of Alberta 1980, c. H-11.7; Charter, see note 22; Americans with Disabilities Act, 42 United States Code § 12101 (Supp. 1992).

131 A. S. Leonard, "Discrimination" in S. Burris et al., eds., *AIDS Law Today: A New Guide for the Public* (New Haven: Yale University Press, 1993) 297 at 299-301.

132 See the draft Genetic Privacy Act, found at http://www-busph.bu.edu/Depts/LW/GPA/GPA.htm; and articles in "The genome imperative: symposium" (1995) 23 Journal of Law, Medicine & Ethics 309-81.

133 See Electronic Privacy Information Center, "EPIC Online Guide to 105th Congress Privacy and Cyber-Liberties Bills" found at http://www.epic.org/privacy/bill_track.html. Many

This analysis is primarily concerned with the use of information by governments and other organizations to control the behaviour of individuals,[138] and as a response to this concern it seems reasonable and appropriate. In the context of health information, for example, medical records may be used to monitor and control use of health services,[139] and it is no doubt important to ensure that this control is not excessive and is not abused. However, there are also a number of other concerns that arise in the context of health information, and among them is the individual's dignity and the injury it may suffer from having very sensitive private information disclosed against her will. The patient's autonomy, which has been vigorously protected by health law, is not just impaired by attempts by an insurer to control use of services; the decision how and when to share personal information is itself also an important aspect of autonomy.

IV. Conclusion

Therefore, I would argue that there is an independent and important interest served in limiting the dissemination of information, independent from procedural fairness in the collection, use and disclosure of data. The range of all possible harms cannot be addressed by other types of legislation, and a selective approach to privacy protection suffers from many weaknesses. It goes without saying that privacy cannot be absolute, at least if the individual wants to receive health care,[140] and in some cases, where a compelling public interest exists, even regardless of the individual's wishes. This does not mean, however, that information systems should not be legally and technically designed to minimize disclosure of personal information whenever possible and to the greatest possible extent. The concept of minimal intrusion, that when disclosure is necessary it should involve the smallest possible amount of information and the minimum number of recipients, is, in fact, an accepted part of policies on health information and personal information generally.[141] It is also commonplace to respect the subject's autonomy by requiring consent for disclosure in most cases.[142]

These rules limiting disclosure are currently accepted as part of information policies; the other aspects of fair information practices add different and perhaps equally important types of protection. My concern, however, is that positions which deny or minimize the significance of protecting privacy as an independent value may eventually lead to limits on disclosure being relaxed, overwhelmed by exceptions or discarded altogether. The remaining fair information practices rules and other forms of legislation such as anti-discrimination statutes will provide individuals with a reasonable degree of protection with respect to some interests, but cannot compensate for a loss of privacy.

The development of new data processing technologies has made these concerns more urgent in two related ways. First, the technology itself, without adequate protective measures, increases the scope and intensity of threats to privacy. Second, technological advances have acted as a catalyst to provoke a re-examination of the value of privacy. Since the

states also have legislation prohibiting genetic discrimination in health insurance. See K. H. Rothenberg, "Genetic Information and Health Insurance: State Legislative Approaches" (1995) 23 J. L. Med. & Ethics 312.

134 See note 18 and accompanying text. One of these other aspects is the individual's interest in private property. One of the effects of technological development in information processing is the increasing commodification of information. See e.g. A. W. Branscomb, *Who Owns Information?: From Privacy to Public Access* (New York: Basic Books, 1994). One possibility, then, might be to shift the emphasis from protecting privacy to creating and enforcing property rights in personal information. This has been suggested by some commentators, e.g. M. S. Faigus, "*Moore* v. *Regents of the University of California* – A Breach of Confidentiality Within the Physician-Patient Relationship: Should Unique Genetic Information be Considered a Trade Secret?" (1993) 24 University of West Los Angeles Law Review 299. There are, however, numerous difficulties with treating information, especially personal information, as property. Unfortunately an adequate discussion of these issues is beyond the scope of this paper.

135 Simitis, see note 16; Schwartz, see note 15.

136 This phrase is borrowed from a German judicial decision; see Simitis, above at 734.

137 Schwartz, see note 15 at 555.

138 Simitis, see note 16 at 710-24. Simitis describes the use of information by health insurers, school authorities, various branches of government and employers to enforce conformity in individual behaviour.

139 See above at 710-12.

protection of privacy in the information age, if it is possible at all, will require an additional investment, interested parties have renewed debates about the question of whether privacy is worth protecting. The answer may well be different depending on the kind of information and the context in which it is collected and used. In the renewed analysis provoked by the new technologies, it is important to be aware of these differences and of the whole range of concerns. A single approach to information policy may not be appropriate for all contexts just as we have learned it is not appropriate for all times. Unless we are willing to accept a deterministic view that we cannot control what the effects of technology will be, we must make choices carefully, considering all of the possible values and interests.

140 It bears mentioning here that the common law recognizes the right of an individual to refuse medical care, even when such care would apparently be in the individual's best interests. See e.g. *Malette* v. *Shulman* (1990), 72 Ontario Reports (2d) 417 (Ontario High Court).

141 See e.g. Bill 30, note 56, sections 37 (disclosure restricted to non-identifiable health information where this is sufficient for the purposes of disclosure) and 38 (disclosure permitted only to the extent necessary for the purposes of disclosure); Health Information Practices Code 1994, see note 50, Rule 11(3): "Disclosure under subrule (2) is permitted only to the extent necessary for the particular purpose"; Fair Health Information Practices Act of 1997, see note 52, section 111(c)(1): "A use or disclosure of protected health information by a health information trustee shall be limited, when practicable, to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed."

142 See e.g. OECD Guidelines, note 34, article 10: "Personal data should not be disclosed, made available or otherwise used for purposes other than [the purposes specified when data was collected] except: (a) with the consent of the data subject; or (b) by the authority of law"; Bill 30, see note 56, sections 29 (disclosure permitted with the consent of the subject) and 30 (circumstances in which disclosure without consent is permitted); Fair Health Information Practices Act of 1997, see note 52, section 112.