

**2004 Annual Labelle Lectureship  
Centre for Health Economics and Policy Analysis  
McMaster University**

**Will changes in data health privacy legislation kill research as we know it?**

Delivered by Valerie Steeves

Department of Criminology, University of Ottawa

October 20, 2004

When Dr. Jack Tu and his co-writers (2004) published their article in the *New England Journal of Medicine* on the *Impracticability of Informed Consent in the Registry of Canadian Stroke Patients*, they raised a number of serious concerns about the ways in which data protection laws may constrain medical research. The authors argued that informed consent led both to low participation rates and to selection biases in the registry database, and they concluded minimal-risk observational research must be exempted from privacy laws if “patients are going to receive the best possible care.” A follow-up interview with Dr. Tu published in the *Medical Post* made a stronger case. The headline read: “Privacy rules may threaten research: Following PIPEDA has led to biased database for Canadian Stroke Network” (Wysong, 2004). With headlines like these, it is no surprise researchers have become increasingly wary of data protection laws.

For the purposes of this paper, I am bracketing the specific question of whether or not consent should be required for registries. Instead, I will focus on Dr. Tu’s underlying conclusion that privacy and research are involved in a zero sum game and researchers must resist data protection regulation because it will harm the research enterprise. I will suggest that the conclusion that data protection will constrain research practices is not supportable, because it is based on 6 myths:

- Myth No. 1: Data protection laws restrict access to health information for research purposes.
- Myth No. 2: Research is an unencumbered public good free of any private interest.
- Myth No. 3: Privacy is an individual right and so must give way to research as a public good.
- Myth No. 4: Observational research data collected without the patient’s knowledge and consent will lead to unbiased data.
- Myth No. 5: Privacy is a road block to better health.
- Myth No. 6: Deidentified health information does not pose a risk of harm to the patient.

I will examine each of these myths in turn and seek to establish a more nuanced understanding of the issues, in the hope that this will support ongoing discussions about the role data protection should play in the research enterprise.

*Myth No. 1: Data protection laws restrict access to health information for research purposes.*

One of the most interesting aspects of Dr. Tu’s article is the authors’ treatment of current data protection laws. They argue that public concerns about the impact of electronic health records and data mining have led many countries to pass laws to control the unauthorized use of health

information. These laws are called data protection laws and contain a set of fair information practices, typically seven or eight of the following ten principles:

1. An organization should be accountable for the personal information it has in its possession.
2. At the time of collection, it should identify the purpose for which the information will be used.
3. Collection should occur with the data subject's knowledge and consent except under specified circumstances.
4. Collection should be limited to information that is necessary to accomplish the identified purposes.
5. The information should not be used or disclosed for other purposes unless the data subject consents.
6. The information should be retained only as long as necessary to accomplish the identified purposes.
7. The organization should ensure the information is accurate, complete and up to date.
8. The information should be protected with appropriate security safeguards.
9. The organization should be open about its policies and practices and information systems should not be secret.
10. Data subjects should have the right to access their personal information and have it amended if the information is inaccurate, incomplete or obsolete (See Bennett & Grant, 1999, p. 6).

The authors then argue that "overly strict privacy laws" may constrain the viability of observational research, and point to a few examples where registries have been legally required to obtain consent from patients before their information can be added to the registry database. Although they point out that "most privacy laws" do not require consent for the collection of information for research purposes, they conclude that "conservative interpretation" on the part of data holders and research ethics boards will "virtually [mandate] that informed consent be obtained before any data are collected" (Tu et. al., 2004).

This outline of the law is problematic, primarily because it mixes apples with oranges. Data protection laws are the most common form of privacy regulation. As of 2004, 43 states in Europe, North America, South America, the Middle East and Asia have passed some combination of fair information practices into law. However, the principle of consent is often not included in these Acts or, if included, is subject to broad exceptions. Bennett & Raab (2003, p. 73) argue that the Council of Europe's Convention for the Protection of Individuals with

Regard to the Automatic Processing of Personal Data continues to serve as a model for countries passing legislation, and it does not require informed consent be obtained by data collectors. The Canadian Protection of Personal Information and Electronic Documents Act (PIPEDA) does include a consent provision. However, PIPEDA only applies to information collected in the course of commercial activity and, like virtually every other data protection law, it expressly provides that researchers do not have to obtain consent or even inform individuals that their information is being collected where the information is used for statistical, or scholarly study or research and it is impracticable to obtain consent. Similarly, under Ontario's new Health Information Protection Act, health information custodians may disclose personal health information to researchers without consent where the research plan has been approved by a research ethics board. The Act specifically mandates that the ethics board should consider whether or not obtaining consent would be impracticable in the circumstances.

Special provisions for research are not a new phenomenon. Since 1974, data protection laws have exempted information used for statistical, scientific or historical purposes from the application of fair information practices (COE, 1974). This is no accident. Data protection principles were developed not to restrict but to *facilitate* the flow of personal information to bureaucrats, state authorities, industry and researchers (Rodota, 1976; Rule et al, 1980; Simitis, 1987; Gandy 1993; Steeves 2002). The first national data protection Act was passed by Sweden in 1973. At the time, Sweden was the most computerized country (Burkert, 2000, p. 48) and the country with the most routine surveillance in Europe (Flaherty, 1989, p. 98). Since 1947, each Swedish citizen has had a unique numeric identifier and large amounts of personal data have flowed freely between government, the Church of Sweden and industry. Legal historian David Flaherty calls Sweden "the model surveillance society in the Western world, because of its high degree of automation, the pervasiveness of Personal Identification Numbers (PINs) to facilitate record linkages, and the extent of data transfers between the public and private sectors" (p. 4). Jan Freese, former director-general of the Swedish Data Inspection Board, calls Sweden a "paradise" for data banks (Freese, 1987, p. 108). Indeed, a companion piece to Dr. Tu's article in the *New England Journal of Medicine* points out that the Nordic countries have ideal databases for research purposes because they are universal in scope, literally following every citizen from cradle to grave (Ingelfinger & Drazen, 2004).

Sweden did not adopt data protection to protect privacy or to restrict the flow of information; it passed its Data Protection Act because it wanted to protect its national sovereignty in case its databases fell into foreign hands (Riley 2004; Burkert, 2000, p. 48). Other jurisdictions, including the Council of Europe, the United States, the European Union, Great Britain and Canada, turned to data protection to promote political and economic integration, efficiency and the legitimization of existing information collection practices (Steeves, 2004). Data protection is not the foe of research because it is designed to ensure that data are accurate and available to managerial elites, including researchers. One of its primary purposes is pedagogical; it seeks to restructure citizen concerns about privacy into the fair information framework to promote trust and legitimize collections (Canada, 1998, pp. 2-3, 7).

When Dr. Tu and his colleagues argue that these kind of "overly restrictive privacy laws" have harmed registries in Germany and part of the United States, for example, they have jumped out of the apple cart into the oranges. Germany is the only country in the world with a constitutional

right to informational self-determination. As a constitutional guarantee, that right trumps data protection laws. In fact, the right to informational self-determination was articulated by the German Supreme Court during the 1983 crisis over the national census in spite of the fact that the census proposal complied with the legal requirements of data protection laws and had the support of all the major data protection commissioners in the country (Flaherty, 1989, p. 81). The United States is also a special case because it is the only Western country that has not enacted comprehensive data protection laws; it relies instead on piecemeal legislation and litigation. The US is also unique among the common law countries because its courts have recognized a general tortious right to privacy which enables people to sue for damages that flow as a result of invasion. Countries like Canada, on the other hand, that rely on data protection legislation to protect personal information typically do not legally restrict the flow of data to researchers.

That does not mean that personal health information is not subject to ethical standards. Clearly, ethical questions remain when researchers wish to place patients under surveillance to facilitate the development of generalizable knowledge. Dr. Tu argues that observational research poses little risk to individual privacy; on the other hand “Clinical registries play a vital role in disease surveillance, quality improvement, and patient safety and must continue to do so if patients are going to receive the best possible care.” This leads us to Myths Nos. 2 and 3: Privacy is an individual right that must give way to health research as an unencumbered public good.

*Myth No 2: Health research is an unencumbered public good free of any private interest.*

The current debate over health information privacy in Canada is typified by calls for balance. Researchers, hospital administrators and pharmaceutical companies argue that individual privacy rights must not be allowed to constrain medical research because research is a social good that competes with, and trumps, the individual interest in privacy. Clearly, we all benefit from advances in medical science. But research is no longer a purely academic exercise. Medical researchers are now under pressure to match public funding with private dollars and to pursue economically exploitable intellectual property rights. The shift away from pure science complicates the privacy/research debate because it raises serious questions about research as a public good.

There is no doubt that health information is a valuable commodity in the electronic marketplace, and that fact changes the research landscape. In 2000, the American Medical Association generated \$20 million (US) by selling doctors’ biographies to pharmaceutical companies who then cross-matched the information with prescription information to micro-market specific physicians. In that same year, drug companies spent an additional \$12 billion (US) on expensive dinners and conferences to encourage doctors to sell more of their drugs (Gay Stolberg & Gerth, 2000). The world’s largest seller of health information, IMS, reported revenues of \$1.3 billion in 2003, and claims “just about every major pharmaceutical and biotech company in the world” as a client (IMS, 2004).

Research is increasingly discussed in economic terms by policy makers. For example, the Leader’s Forum on Health Research in Canada met in Ottawa in September, 2004 to discuss future directions for the research enterprise. The Forum is a partnership of government research

agencies, teaching hospitals, health research institutes, charities, scientific societies and industry (Leader's Forum, 2004, p. 6). They concluded:

The advent of the new economic order is calling for a new and challenging public policy paradigm where social priorities such as health, education and skills development become drivers of information-era growth and competitiveness especially in terms in research and innovation (p. 6).

[and]

It will be equally important to frame health research not only as an integral part of health and health care, but also as a driver of information-era growth and competitiveness. In a knowledge-based economy where businesses and jobs cluster around talent, human capital will increasingly be at the cutting edge of economic competitiveness. A dedicated approach to investing in the research that will enhance the health, education and skills of Canadians will be a principle avenue to foster growth and innovation (p. 11).

However, market models do not always lead to good health care. Dr. Marcia Angell, former editor of the *New England Journal of Medicine*, argues that pharmaceutical research is structured by commercial imperatives which discourage innovation. For example, drug companies focus on developing variations of popular drugs, because these “me-too” drugs have a successful track record of grabbing a share of an established lucrative market. Dr. Angell quotes Dr. Sharon Levine, the associate executive director of the Kaiser Permanente Medical Group:

If I'm a manufacturer and I can change one molecule and get another twenty years of patent rights, and convince physicians to prescribe and consumers to demand the next form of Prilosec, or weekly Prozac instead of daily Prozac, just as my patent expires, then why would I be spending money on a lot less certain endeavor, which is looking for brand-new drugs? (Angell, 2004).

The general public is increasingly concerned about the commercialization of medical research (Goldstein, 2004). Sweden is investigating the suicides of a number of teens who were prescribed anti-depressants. The California legislature held hearings in August on the same issue. California Senator Tom Torlakson said, “Our offices were deluged with requests to testify from family members of suicide victims” (*ibid*). In September, the US House of Representatives held hearings on the pharmaceutical industry because of what the *Washington Post* called “the growing outcry over suppressed medical studies” (*ibid*). At the end of the month, Vioxx was withdrawn from the market because it has been linked to a higher incidence of stroke and heart attack. In October, Professor David Healy testified before a British House of Commons Committee that many of the articles published in the *British Medical Journal* and the *Lancet* are ghost written by pharmaceutical companies that pay respected clinicians to publish the articles under their own names. Another doctor testified that he was offered two years' salary to suppress negative test results regarding a drug (*ibid*).

Commercial imperatives pose serious risks to research, not only because the public is distrustful of these kinds of corporate practices. Once health information is alienated from the individual

and reconstituted as property in the corporation's hands, access to that information will be limited. This is precisely what happened with the Icelandic Health Sector Database. The Database was created by statute in 1998 and contains the genealogical history, genetic information and personal health records for every Icelander. Since the population of Iceland is relatively small, homogenous and isolated, it is an ideal sample for genetic research. The Icelandic government sold the exclusive rights to use the data for research purposes to deCode Genetics, an American biomedical company, which then entered into a licence with the Swiss pharmaceutical company Hoffman-LaRoche to use the database to study twelve specific diseases. That business arrangement has effectively barred any other researcher from using the data for research purposes for twelve years, the duration of deCode's contract with the Icelandic government (Hloden, 2000).

Privacy protects research from these kinds of restrictions because it mitigates against commodification. And this reflects the fact that privacy is not only an individual human right; it is a social good in and of itself.

*Myth No. 3: Privacy is an individual right and so must give way to research as a public good.*

This leads us to the third myth about privacy and research, that privacy is an individual right and must give way to research as a social good. As Dr. Tu notes, others go further and suggest that patients in a publicly funded health care system have a "social obligation" to let researchers use their medical data to improve the health care system for the benefit of all (Upshur 2001; Al Shahi, 2000).

Priscilla Regan argues that privacy policies have been ineffective because too often policy makers pit the individual's interest in privacy against the public good to be facilitated by invading that privacy. This creates a zero sum game where privacy must be "balanced" against the social interest in efficiency and security. However, as Regan concludes, this dichotomy is a false one:

Most privacy scholars emphasize that the individual is better off if privacy exists. I am arguing that society is better off when privacy exists. I argue that society is better off because privacy serves common, public and collective purposes. If you could subtract the importance of privacy to one individual in one particular context, privacy would still be important because it serves other important functions beyond those to the particular individual (Regan, 1993, p. 16).

Indeed, privacy is rich in sociality. Alan Westin's seminal work on privacy, *Privacy and Freedom*, suggests that privacy is an essential element of intimacy and the ability to enter into "close, relaxed and frank relationships" (Westin, 1967, p. 31). The respect shown by others for anonymity and reserve creates a "psychological barrier against unwanted intrusion" that is dependent upon the interaction between the individual seeking privacy and the others with whom he or she interacts (p. 32). Private communications protect social life from the destructive ramifications of completely candid communications, and enable us to enter into relationships of trust (p. 39). Psychologist Irwin Altman (1975) builds on Westin's insights, and argues that privacy is a boundary control mechanism that divides the self from the non-self. Dissolving the

boundary through surveillance weakens both our sense of self and our ability to enter into relationships with others.

One of the most difficult aspects of the emerging health research infrastructure is that it collapses the boundary between the patient's primary interest in health care and secondary interests such as research. To argue that privacy must give way to these secondary interests misses the fact that health care is delivered in the context of social relationships between real social actors. Surveillance that violates the sociological experience of privacy as it is lived in our daily lives will break down the trust that is an essential part of health care delivery.

Surveillance is an exercise of social power, and that is why people are wary of electronic health records and data matching. That does not mean that all surveillance is necessarily bad. People accept surveillance for a number of purposes, but there is always the assumption in the background that the institution conducting the surveillance will be held accountable for its actions within the framework of democratic principles. Researchers who seek to recruit patients for observational research must be sensitive to that fact, or they will not be viewed by the public as trustworthy. And that leads us to the fourth myth, that data collected without the patient's knowledge and consent will be unbiased.

*Myth No. 4: Observational research data collected without the patient's knowledge and consent will lead to unbiased data.*

Privacy is more than a social value; it is a social construction. Privacy is embedded into the act of language, because it is the boundary between the self and the non-self. At a theoretical level, the self emerges because it can become conscious of itself as a social object through discourse with others (Mead, 1934). If discourse becomes distorted through surveillance, then people act in ways that reconstruct their sense of privacy (Steeves, 2004; see also Altman, 1975).

In practical terms, this means that when privacy is not respected, trust will be lost and people will lie, withhold information or forego services to reconstruct their sense of privacy. For example, researchers in South Australia found that just under ten percent of survey participants felt that doctors would not use their personal health information responsibly, and that for some, this lack of trust was based on actual experiences of the non-consensual release of health information (Mulligan, 2001). Adolescents are particularly sensitive to privacy concerns; a study in Massachusetts found that over one-quarter of teens would not seek out health care if they had concerns about confidentiality (Cheng, et. al., 1993). A study conducted on behalf of the California Healthcare Foundation in 1999 found that one in ten people have changed their behaviour to protect their medical privacy by: going to another doctor; paying for services directly even when insured; choosing not to seek medical care; providing an inaccurate or incomplete medical history; or requesting that the practitioner not write down the health problem, or record a less serious or embarrassing condition. And people who know their medical privacy has been breached in the past are four times more likely to participate in these behaviours (California Healthcare Foundation, 1999).

As Altman noted, privacy is "an interpersonal event" (Altman, 1975, p. 22). This means that failing to respect patient privacy will lead to biased data because patients will change their behaviour to account for (in anticipation of?) the invasion.

*Myth No. 5: Privacy is a road block to better health.*

This leads to the fifth myth, that privacy is a road block to better health because it creates an obstacle to medical research. Ingelfinger and Drazen (2004) put it this way: “Public health is threatened by incomplete data more than individual privacy is threatened by disease registries.” In the logic of the zero sum game of privacy vs. health research, increasing one means decreasing the other.

But social psychological research indicates that privacy may be a determinant of psychological health in its own right. In his seminal study of mental institutions, Erving Goffman (1966) found that the patient’s lack of privacy – with the attendant lack of control over personal space or belongings, and the public regulation of bodily functions – meant that the patient was never “off-stage,” never free to drop his social mask and relax free of others' expectations. Patients were also unable to maintain the boundaries between the various social roles they played. Since they were always under observation, they were accountable to the watchers for all facets of their behaviour. Goffman called this form of boundary violation “looping.” Altman’s work on personal space and territorial behaviours led him to conclude that these kind of privacy violations are “a deterrent to rehabilitation, because they expose the self, eliminate a number of normal self-boundary control processes, and make the person extremely vulnerable to others” (Altman, 1975, p. 40). Leontine Young (1966) argues that “without privacy there is no individuality” and Westin (1967, p. 34) links the loss of privacy to emotional breakdown and suicide. Woogara (2001) argues that health professionals’ respect for the patient’s privacy is vital for the patient’s emotional, psychological and physical well-being.

Simple equations which mandate a “minimal loss” of privacy to advance research as a “public good” simply do not fit with the complex sociological and psychological meaning of privacy as it is experienced by real social actors. Once privacy is understood as the boundary between self and others, it sits at the core of inter-subjectivity and self-reflexivity. As such, it cannot be traded off for some other benefit, like efficiency or convenience, and carving out an autonomous space for medical research to the detriment of privacy will have social consequences that flow beyond the original goal of facilitating research. And that leads to our final myth.

*Myth No. 6: Deidentified health information does not pose a risk of harm to the patient.*

Researchers often argue that they are interested in trends and patterns, not what individuals do with their lives. However, the value of electronic databases lies in the fact that the databases can be linked. For example, researchers need to know that Person A’s test results belong to Person A’s medical discharge record or death certificate, so they can track the outcome of the intervention. Obviously, that means that personal identifiers must be maintained so information from different records can be matched. In the Health InfoWay report, Health Canada (1999) argued that one of the benefits of an electronic health network is that it will enable researchers to explore the non-medical determinants of health, and develop “empirically based information” on lifestyle choices, nutritional habits, family support, housing, working conditions and financial status. Once again, to track that information requires unique personal identifiers; however, extending research into such a wide range of personal activities connects the health record to non-traditional health sources of data. And creating networks of personally identifiable data creates risks to privacy that must be managed.

To argue that researchers are trustworthy and can therefore operate outside of established legal rules regarding the privacy of personal information is to miss the point. Law is not a best-case scenario exercise; legal rules are written to protect us from the consequences of the worst case scenario. As I stated above, surveillance is an exercise in social power. The mere creation of a pool of data poses risks because the powerful are able to use that data for social control. David Flaherty puts it this way: in a surveillance society, “record linkages are so easy to accomplish that the power holders cannot resist using them to try to solve real and alleged social problems” (Flaherty, 1989, p. 94). Westwood talks about the “almost biological imperative” of governments and corporations to operate more efficiently in the promotion of collective interests (Westwood, 1999, p. 231). Westin concludes that, “Although organizations often seek to use surveillance to ... solve problems of genuine social importance... if all that has to be done to win legal and social approval for surveillance is to point to a social problem and show that surveillance would help to cope with it, then there is no balancing at all, but only a qualifying procedure for a licence to invade privacy” (Westin, 1967, p. 370).

Once medical databases are created, they become useful to employers, insurers and the state. And the way that researchers access information affects the ability of these others to do so as well. The law is an exercise in line drawing; with respect to privacy, the line of protection is drawn when the individual has a “reasonable expectation” of privacy (*Hunter v. Southam*). Non-consensual access by others creates a *de facto* loss of expectation, and this has ramifications for the legal remedies available. For example, the *Kyllo* case held that police cannot use thermal radiation scanners to “see” into a private dwelling house unless the technology is in “common public use.” Accordingly, common use may negate any expectation that activities that occur within four walls are “private.” Similarly, non-consensual access to medical records may negate the patient’s expectation that the information will be kept confidential.

This is precisely the argument that was used by the United States Justice Department when they wanted access to hospital records to identify patients who were given late term abortions, for the purposes of enforcing the Partial Birth Abortion Act. The Justice Department argued that common access by researchers, insurers and others meant that patients no longer have an expectation of privacy with respect to their medical records (O’Connor, 2004). Although the argument was ultimately unsuccessful, it demonstrates the permeability of “reasonable expectations” in a social environment structured by invasive practices. And the issue is far from over. British Columbia is currently struggling with the implications of contracting out its health records management to American companies which are subject to the US Patriot Act. Under s. 215 of the Act, these companies may be ordered to secretly hand over “any tangible thing” to the FBI – including records containing personal health information. Again, the implementation of new technological infrastructures which are exempt from privacy rules facilitates other uses of health records, and researchers must be cognizant of the fact that their access to health data does not occur in isolation of these broader social and legal dynamics.

The non-consensual flow of health data poses significant risks of harm to the patient, because this opens up the data to secondary uses. Caplan and Cosgrove (2004) argue that the mere fact a psychiatric diagnosis is recorded can lead to loss of custody, health insurance, employment and the legal right to make decisions on financial and other matters. This is even more problematic

when one factors in research that indicates that the patient's gender, race, socio-economic status, physical disability, and sexual orientation can bias the diagnosis process.

Privacy is a flashpoint precisely because medical research is both an objective and subjective exercise. As Andrew Feenberg writes, "The body is the site of medical knowledge and action. It enters medicine as both object and subject insofar as it is both the thing on which medical technique operates and the bearer of the person who commands medical services" (Feenberg, 1995, p. 97). The research subject is therefore more than "the bearer of a mechanical body" but one of the social actors involved in an ongoing relationship that encompasses researcher, patient, physician, and scientist. Research infrastructures that fail to take account of the sociality inherent in the relationship between researcher and subject will be resisted.

In conclusion, privacy is not a barrier to research. It is an essential part of the social relationships that facilitate the development of new knowledge. Arguments that privacy must "give way" to research are both counter-productive and overly simplistic. Good policy should be based on realities, not myths.

Reality No. 1: Data protection laws are a useful tool for researchers because they help to construct trust in research practices.

Reality No. 2: Rules and regulations regarding the flow of medical information are needed to mitigate the commercial imperatives which flow from the fact that research is a public-private enterprise.

Reality No. 3: Privacy is a social value which must be built into good research design.

Reality No. 4: Good privacy practices promote research because they protect the accuracy of data.

Reality No. 5: Privacy is an essential element of psychological health and social relationships.

Reality No. 6: Research databases do not exist in isolation, and researchers must respect the fact that the non-consensual flow of information poses risks of harm in a democratic society.

There may be times when individual consent for research uses is indeed impracticable, but the answer does not lie in exempting research from legal and ethical oversight. What is needed is ongoing dialogue that moves us out of the zero-sum game so we can create infrastructures that account for the role that respect for privacy must play in the advancement of knowledge.

### **Works Cited:**

Al Shahi R, Warlow C. Using patient identifiable data for observational research and audit. *BMJ* 2000;321:1031-2.

- Altman, I. (1975). *The environment and social behaviour*. Monterey, California: Brooks/Cole.
- Angell, M. (2004). *The truth about drug companies: How they deceive us and what to do about it*. New York: Random House.
- Bennett, C.J. & Grant, R. (1999). *Visions of privacy: Policy choices for the digital age*. Toronto: University of Toronto Press.
- Burkert, H. (2000). Privacy - Data Protection: A German/European perspective. Governance of Global Networks in the Light of Differing Local Values. C. Engel & K. H. Keller. (Eds.). Baden-Baden: Nomos.
- California Healthcare Foundation. (1999). *Medical privacy and confidentiality survey*. Princeton Survey Research Associates.
- Canada. (2000). *Personal Information Protection and Electronic Documents Act*. S.C. 2000, C. 5.
- \_\_\_\_\_. Health Canada. Advisory Council on Health Infrastructure. (1999). *Canada Health InfoWay: Paths to better health*. Ottawa: Public Works and Government Services Canada.
- \_\_\_\_\_. Industry Canada and the Department of Justice. Task Force on Electronic Commerce. (1998). *Building Canada's Information Economy and Society: The Protection of Personal Information*. Ottawa: Public Works and Government Services Canada.
- Caplan, P. & L. Cosgrove (Eds.). (2004). *Bias in Psychiatric Diagnosis*. Lanham, Maryland: Rowman & Littlefield Publishers.
- Cheng, T., J. Savageau, J. Sattler, A. DeWitt, and G. Thomas. (1993). Confidentiality in health care: A survey of knowledge, perceptions, and attitudes among high school students. *Journal of the American Medical Association* 269(11): 1404-1408.
- Council of Europe. (1974). *Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. Resolution (74) 29.
- Council of Europe. (1981). *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*. CETS NO. 108, Strasbourg, 28.I.1981.
- Feenberg, A. (1995). *Alternative modernity: The technical turn in philosophy and social theory*. Berkeley: University of California Press.
- Flaherty, D. (1989). Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill: University of North Carolina Press.

- Freese, J. (1987) Seminar on openness and protection of privacy in the information society: Proceedings. Voorburg, Netherlands: Embassy of Sweden and Netherlands Central Bureau of Statistics.
- Gandy, O. (1993). *The panoptic sort: A political economy of personal information*. Boulder: Westview Press.
- Gay Stolberg, Sheryl and Jeff Gerth. (2000, November 16). Medicine Merchants: Tracking the Doctors. *New York Times*.
- Goffman, E. (1961). *Asylums*. New York: Doubleday.
- Goldstein, Ritt. (2004, October 4). Drug industry scandal a “crisis”. *Inter Press Service News Agency*.
- Hloden, O. (2000.) For Sale: Iceland’s genetic history. *Action Bioscience*.  
<http://www.actionbioscience.org/genomic/hlodan.html#Primer>
- Hunter v. Southam*, [1984] 11 D.L.R. (4th) 641.
- Iceland. (1998). *Icelandic Health Sector Database Act*. Act No. 139/1998.
- IMS. (2004). *IMS Investor Briefing 2004*. [http://media.corporate-ir.net/media\\_files/irol/67/67124/presentations/briefing2004.pdf](http://media.corporate-ir.net/media_files/irol/67/67124/presentations/briefing2004.pdf)
- Ingelfinger J. & J. Drazen. (2004). Editorial: Registry research and medical privacy. *The New England Journal of Medicine* 350(14): 1452-1453.
- Kyllo v. US* (2001), 121 S. Ct. 2038.
- Leader’s Forum for Health Research in Canada. (2004). *Strengthening the Foundation of Canada’s Health Research Enterprise*. Ottawa.
- Mead, G.H. (1934). *Mind, self and society*. Chicago: University of Chicago Press.
- Mulligan, C. (2001). Confidentiality of health records: Evidence of current performance from a population survey in Australia. *Medical Journal of Australia* 174: 637-640.
- O’Connor, A.M. (2004). Who wants to know?: Privacy vs. security debated. *Los Angeles Times*. May 30.
- Ontario. (2004). *Health Information Protection Act*. Bill 31 2004.
- Regan, P. (1993). Surveillance and new technologies: Changing nature of workplace surveillance. Paper presented to the Strategic Research Workshop on New Technology, Surveillance and Social Control, at Queen’s University.

- Riley, T. (2004). Personal interview. 22 April.
- Rodota, S. (1976). Privacy and data surveillance: Growing public concern. Policy issues in data protection and privacy. OECD Information Studies no. 10. Paris: OECD.
- Rule, J., D. MacAdam, L. Stearns & D. Uglow. (1980). *The politics of privacy: Planning for personal data systems as powerful technologies*. New York: Elsevier.
- Simitis, S. (1987). Reviewing privacy in an information age. *University of Pennsylvania Law Review* 135: 707-746.
- Steeves, V. (2002.) Privacy and new media. *Mediascapes*. P. Attallah and L.Regan Shade, Eds. Toronto: Thomson.
- \_\_\_\_\_. (2004). *Data Protection Regimes: A Historical Exposition and Comparative Legal Analysis*. Unpublished paper.
- Sweden. (1973). *Data Protection Act*.
- Tu, J., D. Willison, F. Silver, J. Fang, et al. (2004). Impracticability of Informed Consent in the Registry of the Canadian Stroke Network. *The New England Journal of Medicine*. 350 (14): 1414 - 1422.
- United States. *Partial Birth Abortion Ban Act*. US Public Law No. 108-105, 11-5-03.
- Upshur, R., B. Morin & V. Goel. (2001). The privacy paradox: laying Orwell's ghost to rest. *Canadian Medical Association Journal* 165: 307-309. [Erratum, CMAJ (2001) 165: 888.]
- Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.
- Westwood, J. (1999). Life in the privacy trenches: Experiences of the British Columbia Civil Liberties Association. *Visions of privacy: Policy choices for the digital age*. C. Bennett & R. Grant, Eds. Toronto: University of Toronto Press.
- Wyson, Pippa.. (2004, April 20). Privacy rules may threaten research: Following PIPEDA has led to biased database for Canadian Stroke Network. *Medical Post* 40(16).
- Young, Leontine. (1966). A child's right to privacy. *McCalls*. March: 57.