DISCUSSION AND DEBATE

Data Protection and the Promotion of Health Research

Protection des données et promotion de la recherche sur la santé

by VALERIE STEEVES, JD, PHD
Assistant Professor
Department of Criminology
University of Ottawa

Abstract

This paper challenges the argument that data protection legislation may harm research by unduly restricting the flow of personal health information. I unpack the assumption that privacy is an individual right that must give way to research as a social good, and explore how data protection laws facilitate the flow of information for research purposes. I conclude that researchers should embrace data protection laws because they help construct trust in research practices, mitigate the commercial imperatives that flow from the fact that research is a public–private enterprise and protect the accuracy of data. Good research design should recognize that privacy is a social value and an essential element of psychological health and social relationships. And since research databases do not exist in isolation, researchers must respect the fact that the non-consensual flow of information poses risks of harm, including the secondary use of health research databases for social control, that must be managed.

Résumé

Cet article conteste l'argument voulant que les lois sur la protection des données entravent la recherche en restreignant indûment la circulation de renseignements personnels sur la santé. J'examine l'hypothèse selon laquelle la protection de la vie privée est un droit individuel qui doit céder le pas à la recherche en tant que bien social, et j'explore comment les lois sur la protection des données facilitent la circulation d'information à des fins de recherche. Je conclus que les chercheurs devraient adhérer volontiers aux lois sur la protection des données parce qu'elles aident à susciter la confiance à l'égard des pratiques de recherche, réduisent les impératifs commerciaux découlant du fait que la recherche est une entreprise publique-privée et protègent l'exactitude des données. Une bonne conception de recherche devrait reconnaître que le respect de la vie privée est une valeur sociale et un élément essentiel de la santé psychologique et des relations sociales. Et puisque les bases de données de recherche n'existent pas isolément, les chercheurs doivent respecter le fait que la divulgation non consensuelle de renseignements comporte un risque de préjudice – dont l'utilisation secondaire de bases de données de recherche sur la santé pour le contrôle social – qui doit être géré.

In 2000, the government of Canada enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to give individuals control over the collection, use and disclosure of their personal information. Even before PIPEDA became law, the health sector expressed concerns that the data protection principles it contained would unduly restrict the flow of health data to researchers (Korman 1999; Turner 1999; Poston 1999; Sholzberg-Gray 1999; Lingberg 1999; Fineberg 1999). Since the Act was proclaimed in force with respect to health information on January 1, 2002, many researchers have continued to argue that the law hampers their ability to access research data[1] (see Tu 2004; Ingelfinger and Drazen 2004; Wysong 2004).

In this paper, I argue that this position is based on six misconceptions about the relationship between privacy, research and the law. I conclude that privacy is an essential element of good research design, and that researchers should embrace data protection principles because they help build the social trust that enables research to flourish.

Misconception No. 1: Data Protection Laws Restrict Research

Data protection laws typically contain seven or eight of the following 10 principles:

1. An organization should be accountable for the personal information it holds.
2. It should identify the purpose for which information will be used.
3. It should collect information only with the data subject's knowledge and consent,

except under specified circumstances.
4. It should collect only information that is necessary to accomplish the identified purpose.
5. Information should not be used or disclosed for other purposes without consent.
6. Information should be retained only as long as necessary to accomplish the identified purpose.
7. The organization should ensure that information is accurate, complete and up to date.
8. Information should be kept secure.
9. The organization should be open about its policies and practices.
10. Data subjects should have the right to access and correct their information.

The legislative landscape dealing with the protection of personal health information in Canada is a patchwork of federal and provincial laws. PIPEDA applies to personal information (including health information) collected, used or disclosed in the course of commercial activity in both the federal and provincial sectors, unless there is substantially similar legislation in force in a province.

The provinces listed in Table 1 have health-specific data protection in place or private sector laws that have been declared to be substantially similar to PIPEDA. However, there is still the potential for cross-jurisdictional problems; for example, public sector health legislation in Manitoba and Saskatchewan applies to pharmacists, but pharmacists are also subject to PIPEDA when they collect information in the course of commercial activity. In addition, general public sector data protection legislation may apply to hospitals and/or regional health authorities (see, for example, the BC *Freedom of Information and Privacy Act*, SBC 1996, c. 165). For a more detailed discussion of the jurisdictional difficulties associated with health information legislation, see Keeshan (2004: 1–6).

TABLE 1. Health information protection legislation in Canada

	SUBSTANTIALLY SIMILAR PRIVATE SECTOR LEGISLATION	PUBLIC SECTOR HEALTH LEGISLATION
Alberta	*Personal Information Protection Act*, SA 2003, c. P-6.5	*Health Information Act*, RSA 2000, c. H-5
British Columbia	*Personal Information Protection Act*, SBC 2003, c. 63	
Manitoba		*Personal Health Information Act*, CCSM June 28, 1997, c. P-33.5
Ontario	*Personal Health Information Protection Act, 2004*, SO 2004, c. 3 Sched. A	*Personal Health Information Protection Act, 2004*, SO 2004, c. 3 Sched. A
Quebec	*Act Respecting the Protection of Personal Information in the Private Sector*, RSQ 1993, c. P-39.1	
Saskatchewan		*Health Information Protection Act*, SS 1999, c. 29

Some researchers have argued that these principles – especially the requirement to obtain consent – threaten the research enterprise because they make it difficult for researchers to access data that would otherwise be available to them. For example, in an influential article published in the *New England Journal of Medicine*, Jack Tu (2004) and his co-authors conclude that data protection laws are overly strict and may constrain the viability of observational research. In support of this conclusion, they point to examples where registries have been required to obtain patient consent before adding personal health information to the registry database.

This position is problematic, primarily because it "mixes apples with oranges." Data protection laws, or the apples, are the most common form of privacy regulation. As of 2004, 43 states in Europe, North America, South America, the Middle East and Asia had passed some combination of the 10 data protection principles into law. However, the principle of consent is often not included in these laws or, if included, is subject to broad exceptions. Although PIPEDA requires consent, it applies only 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 obtaining consent is impracticable. 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 rules 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 data protection principles (Council of Europe 1974). This is no accident. Data protection laws were not developed to restrict the flow of personal information to bureaucrats, state authorities and researchers but to facilitate it (Rodota 1976; Rule et al. 1980; Simitis 1987; Gandy 1993; Steeves 2002). Data protection is the friend of research because it is designed to ensure that data are accurate and available for research purposes.

When Tu and his colleagues (2004) argue that data protection laws have harmed registries in Germany and the United States, 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. 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. 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.[2]

This does not mean that personal health information is not subject to ethical standards.[3] Clearly, ethical questions remain when researchers wish to place patients under surveillance to facilitate the development of generalizable knowledge. However, many, like Tu, 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. But closer examination demonstrates that research is not an unencumbered public good.

Misconception No. 2: Health Research Is an Unencumbered Public Good Free of Any Private Interest

Clearly, we all benefit from advances in medical science. But medical research is not a purely academic exercise. Policy makers increasingly discuss medical research in economic terms (see Leader's Forum 2004: 6). Researchers are increasingly pressured to match public funding with private dollars and to pursue economically exploitable intellectual property rights. And health information itself is a now valuable commodity in the electronic marketplace (see IMS Health 2004).

This complicates the privacy/research debate because it raises serious questions about research as a public good. Marcia Angell (2004) argues that pharmaceutical research is structured by commercial imperatives that discourage innovation. In 2004, the US House of Representatives held hearings on the pharmaceutical industry because of a growing public outcry over the suppression of medical studies. Across the Atlantic, 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 then pay respected clinicians to publish the articles under their own names (Kmietowicz 2004).

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, homogeneous 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, a US biomedical company, which then entered into a licence with the Swiss pharmaceutical company Hoffman-LaRoche to use the database to study 12 specific diseases. That business arrangement has effectively barred any other researcher from using the

data for research purposes for 12 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.

Misconception No. 3: Privacy Is an Individual Right

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

Priscilla Regan (1993) argues that pitting the individual's interest in privacy against the public good to be facilitated by invading that privacy 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: 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: 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), and private communications 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 than divides the self from the non-self. Dissolving the boundary 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 healthcare and secondary interests such as research. To argue that privacy must give way to these secondary interests misses the fact that healthcare is delivered in the context of social relationships between real social actors. Practices that violate the social experience of

privacy as it is lived in our daily lives will break down the trust that is an essential part of healthcare delivery.

Surveillance, or the systematic monitoring of a person or a group for institutional purposes, is an exercise of social power; that is why people are wary of electronic health records and data matching. That does not mean that all surveillance is necessarily a bad thing. People accept surveillance for all kinds of reasons, but there is always the assumption in the background that the institution will be accountable for its actions within a framework of democratic principles. Researchers who seek to use personal health information for research purposes must be sensitive to that fact, or they will not be viewed by the public as trustworthy.

Misconception No. 4: Observational Research Data Collected without the Patient's Knowledge and Consent Will Lead to Unbiased Data

The fourth misconception is that data collected without the patient's knowledge and consent will be unbiased. But privacy is more than a social value; it is a social construction. In practical terms, this means that when privacy is not respected, trust will be lost and people will lie, withhold information or forgo services to reconstruct their sense of privacy.

For example, researchers in South Australia found that just under 10% 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 the fact that their information had been released without consent (Mulligan 2001). A study in Massachusetts found that over one-quarter of teens would not go to the doctor if they had concerns about confidentiality (Cheng et al. 1993). In California, one in 10 people have changed their behaviour to protect their medical privacy by going to another doctor; paying for services directly; forgoing medical care; providing an inaccurate or incomplete medical history; or asking the practitioner not to write down details of the health problem. 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 (1975: 22) privacy is "an interpersonal event." This means that failing to respect patient privacy will lead to biased data because patients will change their behaviour to account for the invasion.

Misconception No. 5: Privacy Is a Roadblock to Better Health

The fifth misconception is that privacy is a roadblock 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 versus 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 meant that the patient was never "off-stage," never free to drop his or her 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. Altman's work on personal space and territorial behaviours led him to conclude that these kinds 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: 40). Leontine Young (1966) argues that "without privacy there is no individuality," and Westin (1967: 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.

… the patient's lack of privacy meant that the patient was never "off-stage," never free to drop his or her social mask and relax free of others' expectations.

Simple equations that mandate a "minimal loss" of privacy to advance research as a "public good" simply do not fit with the complex social-psychological meaning of privacy as it is experienced by real social actors. Privacy defines the boundary between self and others. It cannot be traded in exchange for some other benefit, such as efficiency or convenience. 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 misconception.

Misconception No. 6: De-identified Health Information Does Not Pose a Risk of Harm to the Patient

Researchers are interested in trends and patterns, not what individuals do with their lives. However, the value of electronic databases lies in the fact that files in different databases can be linked by matching personal identifiers. In its 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. However, extending research into such a wide range of personal activities connects the health record to non-traditional 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. The mere creation of a pool of data poses risks because the powerful are able to use those data for social control. David Flaherty (1989: 84) 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." Westwood (1999: 231) talks about the "almost biological imperative" of governments and corporations to operate more efficiently in the promotion of collective interests. Westin (1967) concludes:

> 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: 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 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 it 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. In 2004, British Columbia struggled with the implications of contracting out its health records management to US companies that are subject to the *USA 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 that 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 a subjective exercise. As Andrew Feenberg (1995: 97) wrote, "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." The research subject is therefore more than "the bearer of a mechanical body"; he or she is 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.

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.

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 misconceptions. Data protection laws are useful tools for researchers because they help to construct trust in research practic-

es, mitigate the commercial imperatives flowing from the fact that research is a public–private enterprise and protect the accuracy of data. Good research design recognizes that privacy is a social value and an essential element of psychological health and social relationships. And since research databases do not exist in isolation, researchers must respect the fact that the non-consensual flow of information poses risks of harm.

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.

Correspondence may be directed to Valerie Steeves, PhD, Department of Criminology, University of Ottawa, 25 University Street, Ottawa, ON K1N 6N5; tel.: 613-562-5800 Ext. 1793; fax: 613-562-5304; e-mail: vsteeves@uottawa.ca.

NOTES

1. Although there is health-specific data protection legislation in place in six provinces (see Table 1), these laws are all modelled on the data protection principles set out in the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data* (1980) and the Canadian Standard Association's *Model Code for the Protection of Personal Information* (1996). The CSA code was incorporated into law in PIPEDA and, as such, PIPEDA continues to serve as a template for data protection legislation in the health sector, especially given the public–private character of the health industry. Private sector use of health information must comply with PIPEDA unless there is substantially similar legislation in place in the province. Moreover, much of the debate around health information was initiated when PIPEDA was being debated in the Senate prior to its passage into law. Accordingly, PIPEDA remains a key focal point of analysis.
2. More specifically, data protection laws do not unduly restrict the flow of information for research purposes. Protocols are subject to certain requirements, such as the prior approval of a research ethics board.
3. Provincial health sector laws (set out in Table 1) give a significant data protection role to research ethics boards (REBs); however, vague statutory requirements in this regard and the lack of a coherent regulatory regime do raise questions about the ability of many REBs to play this role effectively.

REFERENCES

Al Shahi, R. and C. Warlow. 2000. "Using Patient Identifiable Data for Observational Research and Audit." *British Medical Journal* 321: 1031–32.

Altman, I. 1975. *The Environment and Social Behaviour.* Monterey, CA: Brooks/Cole.

Angell, M. 2004. *The Truth about Drug Companies: How They Deceive Us and What to Do about It.* New York: Random House.

California Healthcare Foundation. 1999. *Medical Privacy and Confidentiality Survey*. Princeton, NJ: Princeton Survey Research Associates.

Canada. 2000. *Personal Information Protection and Electronic Documents Act*, 2000 SCC c. 5

Caplan, P. and L. Cosgrove, eds. 2004. *Bias in Psychiatric Diagnosis*. Lanham, MD: Rowman & Littlefield.

Cheng, T., J. Savageau, J. Sattler, A. DeWitt and G. Thomas. 1993. "Confidentiality in Healthcare: A Survey of Knowledge, Perceptions, and Attitudes among High School Students." *Journal of the American Medical Association* 269(11): 1404–8.

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.

Feenberg, A. 1995. *Alternative Modernity: The Technical Turn in Philosophy and Social Theory*. Berkeley: University of California Press.

Fineberg, A. 1999. Senate Standing Committee on Social Affairs, Science and Technology. 36th Parliament, 2nd session. Evidence. Issue No. 5, December 2.

Flaherty, D. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: University of North Carolina Press.

Gandy, O. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.

Goffman, E. 1961. *Asylums*. New York: Doubleday.

Health Canada. 1999. *Canada Health InfoWay: Paths to Better Health*. Advisory Council on Health Infrastructure. Ottawa: Author.

Hloden, O. 2000. "For Sale: Iceland's Genetic History." *Action Bioscience*. Retrieved August 21, 2006. <http://www.actionbioscience.org/genomic/hlodan.html#Primer>.

Hunter v. Southam, [1984] 11 DLR (4th) 641

Iceland. 1998. *Icelandic Health Sector Database Act*, No. 139/1998.

IMS Health. 2004. *IMS Investor Briefing 2004*. Retrieved August 21, 2006. <http://media.corporate-ir.net/media_files/irol/67/67124/presentations/briefing2004.pdf>.

Ingelfinger, J. and J. Drazen. 2004. "Registry Research and Medical Privacy." Editorial. *New England Journal of Medicine* 350(14): 1452–53.

Keeshan, D. 2004. "'P-Day' Arrives in Canada." *Health Privacy in Canada: Law, Practice and Compliance* 2(3): 1–6.

Kmietowicz, Z. 2004 (October 23). "Consumer Organisations Criticise Influence of Drug Companies." *British Medical Journal* 329: 937. Retrieved August 21, 2006. <http://bmj.bmjjournals.com/cgi/content/full/329/7472/937>.

Korman, R. 1999. Senate Standing Committee on Social Affairs, Science and Technology. 36th Parliament, 2nd session. Evidence. Issue No. 3, November 30.

Kyllo v. US, 2001 121 S. Ct. 2038

Leader's Forum for Health Research in Canada. 2004 (September). *Strengthening the Foundation of Canada's Health Research Enterprise: A Backgrounder*. Ottawa: Author

Lindberg, M.C. 1999. Senate Standing Committee on Social Affairs, Science and Technology. 36th Parliament, 2nd session. Evidence. Issue No. 5, December 2.

Mulligan, C. 2001. "Confidentiality of Health Records: Evidence of Current Performance from a Population Survey in Australia." *Medical Journal of Australia* 174: 637–40.

O'Connor, A.M. 2004 (May 30). "Who Wants to Know?: Privacy vs. Security Debated." *Los Angeles Times*.

Ontario. 2004. *Health Information Protection Act*, Bill 31 2004.

Organization for Economic Co-operation and Development. 1980 (October 1). *Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data*. OECD Doc. C(80)58.

Poston, J. 1999. Senate Standing Committee on Social Affairs, Science and Technology. 36th Parliament, 2nd session. Evidence. Issue No. 3, November 30.

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, Kingston, Ontario.

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 and D. Uglow. 1980. *The Politics of Privacy: Planning for Personal Data Systems As Powerful Technologies*. New York: Elsevier.

Sholzberg-Gray, S. 1999. Senate Standing Committee on Social Affairs, Science and Technology. 36th Parliament, 2nd session. Evidence. Issue No. 3, November 30.

Simitis, S. 1987. "Reviewing Privacy in an Information Age." *University of Pennsylvania Law Review* 135: 707–46.

Standards Council of Canada. 1996. *Model Code for the Protection of Personal Information*. CAN/CSA Q-830. Ottawa: Author.

Steeves, V. 2002. "Privacy and New Media." In P. Attallah and L.R. Shade, eds., *Mediascapes*. Toronto: Thomson.

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." *New England Journal of Medicine* 350(14): 1414–22.

Turner, V. 1999. Senate Standing Committee on Social Affairs, Science and Technology. 36th Parliament, 2nd session. Evidence. Issue No. 3, November 30.

United States. *Partial Birth Abortion Ban Act*. US Public Law No. 108-105, 11-5-03.

Upshur, R., B. Morin and V. Goel. 2001. "The Privacy Paradox: Laying Orwell's Ghost to Rest." *Canadian Medical Association Journal* 165: 307–9. [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." In C. Bennett and R. Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press.

Woogara, J. 2001. "Human Rights and Patient's Privacy in US Hospitals." *Nursing Ethics* 8(3): 234–46.

Wysong, P. 2004 (April 20). "Privacy Rules May Threaten Research." *The Medical Post* 40(16).

Young, Leontine. 1966 (March). "A Child's Right to Privacy." *McCalls*: 57.