GETTING LOST IN DOING GOOD: A SOCIETAL REALITY CHECK

WENDY ARMSTRONG

> Increasingly, value judgments that can profoundly affect someone's life are made by public and private bodies based on surreptitiously collected information that may or may not be accurate or even relevant. Today, sellers choose their customers and governments scrutinize their citizens. It should be the other way around in a healthy market economy and a healthy democracy.
>
> —Consumers' Association of Canada (Alberta), 1997

THE SOCIETAL LANDSCAPE

Over the past two decades, new technologies have led to dramatic growth in the collection of information in electronic databases about the circumstances and activities of individual Canadians, and equally dramatic growth in the uses of this information. Most Canadians are unaware of the extent to which this occurs.

The social and political landscape has also changed—and been changed by—these technologies and activities. Canadians have become more reliant on fewer, more distant, and larger sellers of goods and services. Former public services have been turned over in whole or in part to corporate interests through delegation, deregulation, and outsourcing. Regulations have been loosened and public protections eliminated to encourage foreign investment and trade. New public-private partnerships

Data Data Everywhere: Access and Accountability? ed. C.M. Flood. Montreal and Kingston: Queen's Policy Studies Series, McGill-Queen's University Press.

abound. Responsibilities for policing the marketplace have shifted from public to private hands. Hard won social security programs designed to help families weather the economic storms of unemployment, child-rearing, disease, disability, and old age have eroded, leaving Canadians more dependent on private markets and charity. While public debt has dropped, family debt has skyrocketed.[1] Many historical checks and balances have disappeared—including strong consumer, human rights, and public interest voices.

Despite the growth in information surveillance of individual Canadians, there has not been a commensurate increase in availability of information about the activities of governments, public agencies, and corporations. In fact, government secrecy and commercial confidentiality (not privacy protections) have become more widespread because of the nature of many of the above changes.

THE CHANGING HEALTH-CARE LANDSCAPE

There have also been changes in the nature, funding, and focus of health care, public health, and health research in Canada. During the 1990s, encouraging foreign investment to grow domestic health-care companies and expand the research industry trumped the safety and security of Canadians as the primary driver of federal and provincial health policy.[2] As a consequence, the "life sciences" industry (a term adopted by Industry Canada to get around growing public resistance to the practices of biotechnology and pharmaceutical companies) and the health research, health-care services, and public health sectors have become far more entwined.

Once discouraged partnerships between universities and industry have become a major plank in Canada's industrial policy, which focuses primarily on the commercialization of new products and services protected by intellectual property regimes. Janet Atkinson-Grosjean uses the term "merchant scientists" to describe a new breed of researchers in Canada who "move confidently" between academia and business.[3]

Public agencies, health ministries, government bureaucracies, regional health authorities and even disease advocacy groups have been drawn into the web of industry partnerships, money, and influence.[4] While these new partnerships do not necessarily buy support for industry objectives, they almost always buy silence when it comes to public criticisms or challenges of industry practices.

A shift in focus from care of individual patients and health promotion to "population health" in the early 1990s has also led to an upsurge in poorly understood and communicated epidemiological research on risk factors affecting health and illness in populations,[5] and the marketing of screening tests and pharmaceuticals to "manage risk." In the face of widespread professional and public confusion around correlation and cause, and relative versus actual risk, individual Canadians are increasingly cast

as authors of their own medical misfortunes for failing to manage these risk factors in their lives. Social stigma is now attached to an expanding number of diseases and traits.

We must keep this background in mind when we see many of the authors in this book argue that any barriers to the creation of widely accessible electronic health records and linkages of databases for research purposes are an impediment to informed decision-making in the health system and improved health for Canadians. The experiences of the Canadian public, the websites of provincial and federal privacy commissioners, and volumes of social sciences research suggest otherwise. In their enthusiasm, these authors are failing to take into account the current social and political context, the limitations of electronic databases and controls, and what Kim Vicente calls "the human factor."[6]

Therefore, the purpose of this chapter is to provide some "real world" examples of how expanding information surveillance and applications of database technologies are negatively influencing relationships in our society and important social determinants of health such as meaningful work, income, and a sense of self-worth. There are many lessons to be learned from these examples, including how the tools we use shape *what* we do and the danger of "getting lost in doing good."

Market Research by Stealth and Stealth Marketing

> Corporations have moved swiftly and definitively to exploit the advantages of new information technologies and consolidated their power as never before.
>
> —Bricker and Greenspan, *Searching for Certainty*, 2005

One of the most significant developments over the past two decades has been the widespread commercial adoption of *stealth marketing* based on new market research techniques that use "unobtrusive" information surveillance and data mining. This has been facilitated by the decreasing cost of data storage, the increasing use of "virtual" money (credit and debit cards, preauthorized payment, and online banking), and the commercialization of the Internet in 1993.

According to a former marketing executive, the word *stealth* is used to describe these strategies because "consumers are usually unaware that their personal information is being collected, used, or sold for market research and marketing purposes," and because "there is a great deal of fakery and trickery in the industry."[7]

Companies gather personal information from myriad sources, including the digital footprint we leave every time we make a purchase with credit or debit or Air Miles cards or visit a website. Collected information reveals (and infers) much about our activities, our beliefs, our health, and our vulnerabilities. This information is then used and/or sold to interested

and willing purchasers, including companies in market research, data management, and public relations, which are now often one and the same.

"Fat" databases can include credit and rental history; family make-up; assets; employment history; education; history of home, auto, and health insurance claims; visited websites; magazine subscriptions; and driving record. Below are examples of lists for sale that are tied to an individual's name and address:[8]

- types of books purchased
- subscriptions to particular magazines
- registrations on and visits to websites
- responders to direct mail/TV/radio/Internet solicitations
- holders of particular credit/reward cards, purchases using those cards
- ailments and medications
- diets and nutritional concerns
- causes (associations) to which we donate

With remarkable ease, new generation software can take even anonymized data, match it with other lists, and effectively re-identify many individuals.[9] Psychologists working for market research companies then manipulate and analyze the collected information to develop sophisticated campaigns—including the use of news outlets and "thought leaders"[10]—for clients to sell products, services, and ideas. With today's strategies, few people are even aware they have been marketed to.[11]

No industry has been as effective in using these strategies as the pharmaceutical industry in its efforts to influence government regulators, medical knowledge structures, and the public. For example, in the space of little more than a year Paxil's manufacturer GSK took a little-known and once-considered rare psychiatric condition and helped transform it into a major epidemic called "social anxiety disorder"—claimed at one point to affect one out of eight.[12]

Everyone likes to think they are not influenced by these strategies, but the evidence says otherwise. Governments also hire these market research companies to create the spin necessary to convince citizens of the merits of specific policies and actions. Regardless of actual research findings or intent, money and messaging drown out the facts.

Electronic Databases and Market Segmentation

> Technology switches the opportunities for subversion from individuals to organizations.
>
> —Mark Lisac, *Edmonton Journal*, 1995

Electronic databases have also allowed corporations—particularly dominant telecommunication, banking, and energy companies—to segment their

large customer base into high value customers and low value customers. High value customers obtain high quality service, special pricing benefits, and regular contact. Low value customers are shifted to voice messaging systems and call centre staff who have no authority to act.

Michael Janigan, general counsel and executive director of the Public Interest Advocacy Centre in Ottawa, describes how, now that governments have retreated from the traditional role of protecting small consumers in these inherently non-competitive sectors, a consumer "caste" system is emerging in Canada:

> We've segmented the market to the extent that you now have different castes of consumers. There are the upper castes of consumers in industries such as telecommunication and energy where big business and high volume purchasers are able to construct whatever deal they can with suppliers of goods and services. These discounts are largely paid for by the rung of customers in the lower or middle caste who effectively don't get any discounts and have little means of affecting any kind of change. Finally, there is a lower caste of "untouchables" and their business is not really welcomed by any suppliers, as evidenced by what has happened in banking over the past decade.[13]

In the early 1990s, as the financial services sector was being deregulated, banks reduced their hours and closed hundreds of branches. They shifted to electronic banking and also got out of the small loans business. High end customers were shifted to high interest credit cards. Low end customers were shifted to new (and even higher cost) cheque cashing and "payday" loan companies, which rushed in to fill the gap. According to a 2007 Manitoba study, when converted to annual percentage rates, the combined interest and fees for payday loans averages 778 percent.[14] Comparatively, someone obtaining a line of credit at a bank could expect to pay between 8 and 14 percent. Traditional banking services are commonly required to rent an apartment, hook up utilities, or obtain employment. Barriers to access to these services in this era of automatic deposits and preauthorized withdrawals are an important social determinant of health.

Janigan goes on to illustrate the appropriateness of the metaphor of the caste system as it relates to the lack of contact between castes, resulting in the development of completely different perceptions of the price and quality of service within the population because of this market segmentation. This is in sharp contrast to situations where a product or service is marketed in a similar fashion to all customers, such as when "everyone pulls up to the pump for gasoline." In these circumstances, it is far more likely that there will be an outcry over price or quality because everyone is affected.

And what about claims of greater efficiency? Although the major argument put forward by the big banks for mergers is to take advantage of efficiency gains arising from shared databases, studies on bank mergers

have shown that, over a certain size, economies of scale are absent or unimportant.[15] There is no evidence that any efficiency gains from shared electronic databases are routinely passed on or fairly distributed to customers. And technology is expensive to service.

Function Creep and New Employment Screening Companies

> Computer matching turns the traditional presumption of innocence into a presumption of guilt: in matching, even when there is no indication of wrong-doing, individuals are subject to high technology search and seizure.
>
> —Bruce Phillips, Privacy Commissioner, 1995

Information housed in multiple public and private databases is now beginning to influence many other relationships in our lives, a phenomenon called "function creep." It is now commonplace for potential and current employers or agencies to obtain or require access to detailed personal information as a condition of establishing a relationship.

Verification Inc. is a US-based company that offers Canadian employers both background checks and ongoing monitoring of employees. The purpose of these services, according to promotional materials, is to enable employers to "manage risk."

In 2007, an Edmonton woman in her forties was contacted by a former employer, a large North American investment firm with thousands of Canadian employees, and encouraged to apply for a new position. She applied and was hired on the spot. She was then asked to sign a form authorizing Verification Inc. and all its agents to conduct a background check—now a required practice for all the firm's employees. This check could include *but was not limited to*

> information from personnel files, educational institutions, government agencies, companies, corporations, credit reporting agencies, law enforcement agencies ... academic, residential, achievement, job performance, attendance, litigation, personal history, credit reports, driving records, and criminal history records for which an absolute discharge or full pardon has not been granted.[16]

She also had to undergo a criminal check and be fingerprinted. Uncomfortable, the woman contacted Verification Inc.: "I wanted to know just who were the contracted agents, why there was no time frame for destruction of the record, and what did the phrase 'not limited to' really mean, particularly about my health information," she told a consumer advocacy organization in 2007.[17] She also went searching to find out what she could about the company, its owners, and track record.

The company advised her that an example of a company agent would be the RCMP and that, yes, there was no specified period for record

retention. The company would also continue to monitor her personal records while she remained with her current employer. She could find no information on the company's owners or track record. She did, however, find out that Verification Inc. also offered tenant screening, drug testing, and occupational medical screening. No one could give her a clear answer about her medical records.

She told her new boss she did not want to sign. He urged her to sign, saying, "After all, there is so much information floating around out there already and you can't do anything. Why not sign it?" *When she refused, she was summarily fired.*

The woman said her biggest concern was the potential for identity theft and resulting financial losses with so much information stored in one database and the information being transferred across international borders (the example the company gave her was India; personal interview by author, 16 April 2007). Other observers have raised additional concerns about the growth of such screening:

- How might it influence the job opportunities of someone with a past cannabis charge, a different sexual orientation, or membership in the wrong political party or religious group?
- What about someone treated in the past for medical conditions such as breast cancer or depression that can increase the premiums for a company's benefit plan?
- Will the cult of efficiency ensure many do not make the first cut—*or even apply*?
- Will this create a new caste of "unemployables"?

Having to expose such detailed personal information (and explain any discrepancies) to strangers and individuals with whom we hope to establish relationships plays into human fears of being labelled in ways that can lead to embarrassment, strained relations, lost opportunities, and social exclusion. Although such fears are often dismissed, they have a legitimate basis. The files of human rights and civil liberties organizations, privacy commissioners, and public interest groups are filled with cases.

Social exclusion is now a well-recognized social determinant of health and well-being. Chronic social stress can lead to continuous output of cortisol in the body, which in turn negatively influences disease processes.[18] Social exclusion also exerts a powerful influence on someone's sense of self-worth and response to others.[19]

Medical labelling is particularly problematic—and often wrong. A 2004 compilation of essays edited by psychologists Paula J. Caplan and Lisa Cosgrove, *Bias in Psychiatric Diagnosis,* provides many examples of how a simple visit to a therapist for counselling, or documentation of a highly subjective diagnostic label in a medical chart, can have consequences ranging from loss of child custody, to denial of health insurance

and employment, to removal of one's right to make decisions regarding legal affairs.[20]

In addition, a 1993 survey by the Canadian Medical Association found 7 percent of Canadians had not sought out diagnosis or treatment because of worries about how it might affect other aspects of their lives such as insurability or employment.[21] By 2007, 11 percent reported holding back information from a health provider because they were concerned about who it would be shared with or what purposes it would be used for.[22] Will this number rise as Canadians become aware of how many more people with no established relationship now have access to their health information? What are the implications of people choosing not to disclose relevant information? How will it affect the accuracy of diagnosis, the safety of treatment, the spread of contagious diseases, and the reliability of research data?

Gary Marx, a sociology professor at the Massachusetts Institute of Technology, has shown that public resistance to information surveillance occurs in many invisible ways, including individuals obscuring their identities and providing false or incomplete information.[23] Nevertheless, the function creep of electronic databases is difficult to control or monitor.

The Segmentation of Citizens and Loss of Data

> A culture of inequality may be more significant than material inequality.
>
> —Richard Eckersley, "Is Modern Western Culture a Health Hazard?" *International Journal of Epidemiology*, 2005

Over the past two decades, provincial and federal governments in Canada have adopted many of the practices of corporate interests, including the use of electronic databases to more efficiently monitor and segment citizens. This has led to decreased social cohesiveness, increased individualism, and a less egalitarian society.

The increasingly restrictive nature of social benefits has led to greater intrusion into the financial and family life of many Canadians.[24] On top of an applicant's financial or health worries is added the pain of having his or her family life judged (both morally and financially) by strangers. In order to avoid this discomfort, some people eligible for benefits do not apply.[25] Avoiding moral and financial scrutiny is also often cited in private by supporters of private health-care options and online commercial medical record repositories such as Google Health.

Gaps in basic data arising from the loss of universality of public programs and the shift to private spending have already created problematic bias in research results and public discourse. There are even greater barriers to obtaining reliable information in the commercial realm.

The Catch 22

> The Catch 22 of having [the right to control access] over one's own medical records or information is that other parties can request authorization for access as a condition for being considered for a service or product or employment. Denying access is interpreted as having something to hide.
>
> —Office of the Information and Privacy Commissioner of Ontario, *Interim Order PO-1881-I*

In many of the previous examples, broad authorizations for vaguely described sharing and uses of personal information are buried in application forms or conditions of service that few people give a second thought to signing.[26] Below is an excerpt from a typical medical authorization form in the Canadian health and life insurance industry that applicants are required to sign.

> I/We authorize any health care professional, as well as any health or social service establishment, any insurance company, the Medical Information Bureau, financial institution, personal information agents or security agencies, my/our employer or any former employer and any public body holding personal information concerning me/us, particularly medical information, to supply this information to [the life insurance company] and its reinsurers for the risk assessment or the investigation necessary for the study of any claim…

Lack of awareness of *which* particular establishments might be contacted and *what* information is contained in each establishment's file can create problems.

When a young woman starting her own business in Ontario applied for a disability insurance policy, she was surprised to be turned down because the company said her medical records showed that she had a history of repeat physician visits for "psychological counselling." It turned out her physician—someone her family had gone to for years because the physician never rushed them and always encouraged them to talk about other things in their lives when they went in for routine problems—had been billing all the appointments as psychological counselling. When confronted by the woman, the physician said, "Well, how else am I going to get paid for the real amount of time I spend to provide you with good care?" Ironically, even this visit was billed as "psychological counselling." No disability insurer will touch this young woman because all such information is shared with other health and life insurers through an industry-run North American database. Nor does she feel she can destroy her parents' relationship with the doctor by filing a complaint.[27]

Lack of Redress and Remedies for Harm Done

Sloppy data entry, coding errors, confusion with common names, software problems, bias or prejudice, internal and external breaches, unauthorized

uses, and fraud all contribute to remarkably inaccurate information in databases.

Fraud and identity theft. The existence of electronic databases and the ease of access to so much personal information in these databases have been major drivers in the success of an international fraud industry dominated by organized crime. Identity theft, an emotionally and financially debilitating experience, is the fastest-growing crime in Canada. Once false information has been spread far and wide, it is impossible to track down and correct.

Inappropriate responses. The response of merchants and public agencies to date has been to collect and store *even more* personal information in electronic databases in order to authenticate someone's identity. Ironically, this creates an even greater risk if data breaches occur, which they do with remarkable regularity, including many involving sensitive medical records. Worse yet, many of the same companies whose information practices are contributing to fraud are now marketing "identity theft insurance" and "protection services" to the public.

Multiple uses of databases. Problems with data integrity, interpretation, and user-friendliness arise when databases are used for more than one purpose. This last issue came into focus in 2001 when an Ontario farmer spent over $40,000 attempting to correct his acknowledged incorrect OHIP records due to fraudulent billing by his physician. The province initially refused because the record was also used for accounting purposes.[28] In Alberta, a proposal to merge detailed electronic *medical* records in physicians' offices with provincial electronic *health* records has many physicians worried that the interface will be less useful for clinical care and will compromise their code of ethics and obligations to patients.

Three important conclusions follow:

- While good decisions can, in theory, be made with good information, bad decisions (that result in harm) can be made with bad information.
- Most of the financial, social, and emotional harm from inaccurate or biased information in electronic files is borne by individuals and their families.
- The more users and uses (authorized and unauthorized) and the greater the amount of data collected, the greater the likelihood that data will be corrupted. Designing a database for many purposes often limits the usefulness of the database for some of the purposes.

The Holy Grail of Automation

> Professionals need to think more about the interaction between technology and moral values, particularly in today's world where there are so many pressures to put economic concerns ahead of everything else.
>
> —Kim Vicente, *The Human Factor*, 2004

Opportunities to influence physician behaviours through built-in prompts, performance measures, and "evidence-based" treatment algorithms are frequently cited benefits of electronic patient records and databases. But are there downsides?

A 2008 article by Sarah Bowen and Sara Kreindler looking at Manitoba's experience with indicators suggests a need for caution.[29] So do anecdotal reports from patients. As the wife of a man with diabetes wrote in an email to a family support group,

> We definitely are trusting less and less. Our physicians (a husband/wife team) try to follow all the best practice guidelines. She still wants Lloyd [a Type 1 diabetic] to be on the altace, which lowers blood pressure even though his pressure is normal for a 20-year-old and he turns 60 this year!! He discontinued after one dose when he had a hypotensive episode while operating a power saw nearly two years ago and had to have his finger reattached. Also he had an appointment after his fasting blood work. The lab had switched over to a new computer system and he was in a lineup for 2 1/2 hours waiting. His blood pressure at the appointment was 78/50 and she still wanted him to take the altace!! Just following the guidelines makes no common sense.

While automation and standardization have benefits, there are also pitfalls, particularly when users become too reliant or trusting of the applications. And when something goes wrong, it affects far more people. How quickly can embedded algorithms in electronic records be changed given the "here today, gone tomorrow" nature of medical wisdom? Who designs these algorithms? Who is responsible for harm done? Given all we know about the variations in human biological and emotional responses, just how standardized and automated can we afford to be?

Broken Promises

The province of Alberta now has the most comprehensive electronic health record system in the country and a trail of broken promises regarding citizen safeguards. The Alberta *Health Information Act* (*HIA*), passed in 1999, required prior one-time patient consent for uploading patient information in the custody of health-care providers (e.g., hospitals, doctors, pharmacists) to a central provincial government-controlled electronic

health record system. The legislation restricted its scope to wholly or partly publicly funded services and providers, with some notable exceptions such as pharmacies and pharmacists.

A 2003 survey by the Privacy Commissioner of Alberta found that although many Albertans expressed support for (undefined) electronic health records, "*exercise of individual consent over who can obtain access to an Electronic Record was considered extremely important to 89% of Albertans*" (emphasis added).[30] In 2003, the Alberta government quietly eliminated Section 59—the requirement for patient consent prior to uploading records in Wellnet (now Netcare)—and gave patients the right to request that their health service provider withhold certain information from Netcare, although providers were not obligated to comply. The reason given for these changes was that providing information to patients about how their information might be used prior to obtaining authorization was administratively burdensome. In short, it cost time and money. The government news release read, "*Health Information Amendment Act* Protects Patient Confidentiality While Providing Needed Access."[31]

Later revisions to the Act in 2006 allowed disclosure of certain health information by health services providers to *police* and other authorities as well as *third party payers* (insurers) without a patient's prior knowledge or consent.[32]

In 2007, there were 24,000 registered users eligible to access Alberta Netcare based on an honour system and the "need to know," including retail pharmacists, managers, administrators, evaluators, and educators. The same year, a health-care worker was caught and charged for improperly surfing a patient's record and fined $10,000. She was checking up on her boyfriend's ex-wife.[33]

In 2008, the Privacy Commissioner of Alberta released a report.[34] It revealed that a 2003 amendment to *HIA* that allowed masking of specific fields of health information by patients had not been communicated to the public, and that there were no administrative tools to support it. It also provided the first real insight into just what information was being housed in Netcare. Also in 2008, the Alberta Auditor General reported that information technology (IT) security within the government of Alberta was woefully inadequate.[35]

In 2009, proposed amendments (Bill 52) to *HIA* included expanding the Act to cover privately funded services and removing the requirement of health service providers to at least consider a patient's wishes with regard to uploading information to Netcare. Amendments would also allow for the creation of undefined "health information repositories" for research purposes with no identified governance model. Other amendments would effectively limit auditing of the trail of sites accessing someone's records as well as oversight of new applications of health information by the Privacy Commissioner. The icing on cake was a provision making it an offense (with massive fines) for doctors and other service providers to refuse to

upload their in-house medical records to Netcare upon the Minister's request, including such things as notes about private conversations.

For the first time in the history of the legislation, the Alberta Medical Association and the Alberta Privacy Commissioner raised a public alarm. Albertans began to stir. The Standing Policy Committee on Health heard from more organizations and individual Albertans than they had in the history of the legislation.[36] While some significant accommodations were made, others were not, and the regulations that will reveal the nuances in these amendments are not yet complete.

The problem with all these broken promises is that history has shown repeatedly that if people are not dealt with in good faith, they in turn will not deal in good faith. This creates a definite lose-lose proposition for just about everyone in society.

CONCLUSION

> Sometimes the measurable drives out the important.
>
> —Howard Brody, Director, Institute for the Medical Humanities

In the Canadian health research community, there is a widely held pro-electronic health record and database linkage agenda that makes four key assumptions.

1. The creation and linkage of broadly defined health and administrative databases will provide more accurate and meaningful information.
2. Any harm done to the public or society by the creation and uses of electronic records for health research will be more than offset by the benefits.
3. Research results will be unbiased and available to all.
4. This information will be used only in ways that will improve the health system and the health of Canadians.

These four assumptions are optimistic and naive. They are not borne out by the experiences of Canadians. Nor do they take into account the social and political landscape, the nature of the technology itself, and human nature.

In his best seller, *The Human Factor*, engineer Kim Vicente points out how technological innovation is progressing so quickly that we have fallen behind in our ability to manage it, and it now poses significant threats to our quality of life.

Therefore, extreme caution is urged in continuing to promote the creation of ever more databases and linkages—including the many different faces of electronic health records—without more protections for individuals. Because there is such a high risk of unintended harm in this area, health researchers must be vigilant to avoid "getting lost in doing

good." What if the failure of health researchers to respect and protect the interests of individuals in this information age turns out to be the cause of many of our current health and social problems—and not the cure?

NOTES

1. Vanier Institute of the Family, The Current State of Canadian Family Finances Series (Annual Reports, 1999–2007), www.vifamily.ca (accessed 26 November 2009).
2. C. Fuller, *Caring for Profit: How Corporations Are Taking Over Canada's Health Care System* (Vancouver: CCPA and New Star Books, 1998). In the mid-1980s, areas of health care with the potential to attract foreign investment included home care, long-term care, and health information systems.
3. A. Silversides, "Merchant Scientists: How Commercialization Is Changing Research in Canada," *The Walrus*, May 2008, http://www.walrusmagazine.com/articles/2008.05-science-and-commercialization-ann-silversides/ (accessed 21 October 2009).
4. S. Batt, *Marching to Different Drummers: Health Advocacy Groups in Canada and Funding from the Pharmaceutical Industry* (Toronto: Women and Health Protection, 2005), http://www.whp-apsf.ca/pdf/corpFunding.pdf (accessed 21 October 2009).
5. N. Krieger, "Questioning Epidemiology: Objectivity, Advocacy and Socially Responsible Science," Editorial, *American Journal of Public Health* 89, no. 8 (1999): 1151-53.
6. K. Vicente, *The Human Factor: Revolutionizing the Way We Live with Technology* (Toronto: Vintage Canada, 2004).
7. T. Young (President of Drug Safety Canada), interview with author, 4 June 2005.
8. P. Lawson, Canadian Internet Privacy and Public Interest Centre, "Consumer Health Information as a Commodity" (presentation to Electronic Health Information and Privacy Conference, Ottawa, 13 November 2006), http://www.idtrail.org/files/lawson_ehealth-nov2006.pdf (accessed 21 October 2009).
9. K. El Emam, E. Jonker, S. Sams, E. Neri, A. Neisa, T. Gao, and S. Chowdhury, *Pan-Canadian De-identification Guidelines for Personal Health Information* (report prepared for the Office of the Privacy Commissioner of Canada, 2007), http://www.ehealthinformation.ca/documents/OPCReportv12.pdf (accessed 21 October 2009).
10. A. Ries and L. Ries, *The Fall of Advertising and the Rise of Public Relations* (Toronto: HarperCollins Publishers Inc., 2002).
11. A. Cassels and R. Moynihan, *Selling Sickness: How the World's Biggest Pharmaceutical Companies Are Turning Us All into Patients* (New York: Nation Books, 2005).
12. Ibid.
13. M. Janigan, interview by author for an unpublished paper, "The Changing Face of Consumer Protection in Alberta; What's Below the Waterline?" March 2005.
14. J. Buckland, T. Carter, W. Simpson, A. Friesen, and J. Osborne, "Serving or Exploiting People Facing a Short-Term Credit Crunch? A Study of Consumer

Aspects of Payday Lending in Manitoba" (Manitoba Public Interest Law Centre, 15 September 2007), http://publicinterestlawcentre.ca/files/payday_lending_report.pdf (accessed 21 October 2009).
15. R. Kerton, "Consumers Assess Mergers among Big Banks" (presentation by the Consumers' Association of Canada to the Honourable Ralph Goodale, 31 December 2003), http://www.consumer.ca/pdfs/bank_mergers.pdf (accessed 21 October 2009).
16. "Verification Inc. Pre-Employment Form" (2006), in the Consumers' Association of Canada (Alberta) "Submission to the Standing Policy Committee on Health, Alberta Legislature, Re: Bill 52, Amendments to the Alberta Health Information Act," Appendix 4 (4 February 2009), http://www.assembly.ab.ca/committees/health/submissions/HE-B52-008B.pdf (accessed 3 March 2010).
17. Caller to Consumers' Association of Canada (Alberta) in Edmonton; and interview by author, 16 April 2007.
18. CBC Ideas, "Sick People or Sick Society," Part 1, produced by Jill Eisen (Podcast, 3 March 2008), http://podcast.cbc.ca/mp3/ideas_20080303_4892.mp3 (accessed 21 October 2009).
19. Jane Elliott's famous Blue Eyes–Brown Eyes Exercise demonstrates this response.
20. P.J. Caplan and L. Cosgrove, *Bias in Psychiatric Diagnosis* (Lanham, MD: Jason Aronson, 2004).
21. Survey of Canadians by Canadian Medical Association (1993, personal files).
22. R. Ouelett, President of the Canadian Medical Association, "Physician-Patient Relationship: Trust" (presentation to the CIHR Health Information Summit, Toronto, 20–21 October 2008), http://www.f2fe.com/cihrsummit/Robert%20Ouellet.pdf (accessed 3 March 2010).
23. To explore the research and writing of Prof. Gary Marx, see his home page at http://web.mit.edu/gtmarx/www/garyhome.html#Online (accessed 21 October 2009).
24. For example, while over 300,000 manufacturing jobs have been lost in Canada, less than 40 percent of these unemployed workers qualify for Employment Insurance benefits.
25. W. Armstrong and R. Deber, "Missing Pieces of the Shift to Home and Community Care: A Case Study of the Conversion of an Alberta Nursing Home to Designated Assisted Living" (M-THAC working paper, 2006), http://www.teamgrant.ca/M-THAC%20Greatest%20Hits/M-THAC%20Projects/All%20info/Hinton/Publications/p401090.pdf (accessed 3 March 2010).
26. Canadian Internet Policy and Public Interest Clinic, "On the Data Trail: How Detailed Information about You Gets into the Hands of Organizations with Whom You Have No Relationship" (Ottawa, 2006), http://www.cippic.ca/documents/May1-06/DatabrokerReport.pdf (accessed 21 October 2009).
27. Personal interview by author, by phone, 2003.
28. Information and Privacy Commissioner of Ontario, *Interim Order PO-1881-I*, http://www.ipc.on.ca/.
29. S. Bowen and S.A. Kreindler, "Indicator Madness: A Cautionary Reflection on the Use of Indicators in Healthcare," *Healthcare Policy* 3, no. 4 (2008): 41-48.

30. Office of the Information and Privacy Commissioner of Alberta, "OIPC Stakeholder Survey" (GPC Research, March 2003). Of those Albertans polled, 89 percent also felt their consent should be required before disclosure of identifiable health information to someone doing health research, and about one-third would not agree to having their de-identified health information disclosed to researchers without consent.
31. Government of Alberta, "*Health Information Amendment Act* Protects Patient Confidentiality While Providing Needed Access" (News release, 25 February 2003). Although Albertans' support for the concept of electronic health records has increased over the years, complaints to advocacy groups suggest that most Albertans incorrectly assume information cannot be accessed without an individual's expressed consent.
32. See Part 5: Disclosure of Health Information, *Health Information Act* (Alberta), for a full list of allowed disclosures (not including 2009 amendments), http://www.qp.alberta.ca/574.cfm?page=H05.cfm&leg_type=Acts&isbncln=9780779746682 (accessed 21 October 2009).
33. R. Lombardi, "Alberta Health Care Cases Highlight Future Privacy Issues," *IT World Canada* (6 June 2008), http://www.itworldcanada.com/news/alberta-health-care-cases-highlight-future-privacy-issues/00036 (accessed 3 March 2010).
34. Office of the Information and Privacy Commissioner of Alberta, "Investigation Report Concerning the Disclosure of Health Information Using Alberta Netcare," Report H2008-IR-001 (15 May 2008), http://www.oipc.ab.ca/ims/client/upload/H2008-IR-001%20FINAL%20FOR%20RELEASE_20080515_.pdf (accessed 1 October 2009). See details of Netcare in the appendix of the report.
35. Government of Alberta, *Report of the Auditor General of Alberta* (Edmonton, April 2008), http://www.oag.ab.ca/files/oag/April_2008_Annual_Report.pdf (accessed 3 March 2010). Also see more details in the October 2008 *Report of the Auditor General of Alberta* at http://www.oag.ab.ca/files/oag/Oct_2008_Report.pdf (accessed 3 March 2010).
36. Bill 52 and presentations by groups to the Standing Committee on Health, Alberta Legislature (2009), http://www.assembly.ab.ca/committees/health/ (accessed 11 October 2009).