Some Reflections on Privacy and Technology

DAVID H. FLAHERTY*

I. INTRODUCTION

MY PRESENTATION IS ABOUT some reflections on the relationship between privacy and technology. I will expand, essentially, upon a series of points on privacy and technology.[1] If this were an interactive session, I would ask, "What do you think that I am going to say about that topic?" Many would probably think I was going to respond like some Luddite and beat the heck out of technology, let's destroy our computers and smash our CD-ROMS, because they have only five years of shelf life. That is not what I am going to do at all. In fact, one of the sub-themes of my presentation is that technology can be used very effectively to protect our privacy rights in everyday life, whatever other challenges it poses to the preservation of private life in the twenty-first century.

I am not going to address definitions of privacy at the outset, because the topic is such a quagmire. One of the most basic and now quaint articulations, "the right to be left alone," was by Justice Louis Brandeis, as he was later known, in the *Harvard Law Review* in 1890—one of the most famous law review articles of all time, called the "Right to Privacy." The article responded to perceived problems with photographers and the yellow press allegedly interfering with the wedding of one of these upper-class people (presenting, in fact, a nineteenth century example of the impact of a new technology, the flash camera, on privacy).[2]

In retrospect, it is really quite charming, to think about privacy as the right to be left alone, because, in modern industrial societies, we have so little physical or mental space to be truly left alone, and the digital world leaves us even less such space. You can be alone when you are reading e-mail or visiting

---

* David H. Flaherty served as the Privacy Commissioner of British Columbia, 1993–1999.

1 This paper is a revised version of a presentation in the Isaac Pitblado Lecture Series, Law Society of Manitoba, Winnipeg, 6 November 1998.

2 Louis Brandeis and Charles Warren, "The Right to Privacy," *Harvard Law Review*, 5 (1890), 193–220.

web sites or chat groups, but people are at you, in a sense, all the time. We are suffering in many ways from information overload and excessive accessibility to others. Many of us are also aware of the digital footprints that we leave behind many times each day, and the profiling of our lives that this makes possible. In urban places, with large populations, individuals do not have much solitude of the sort that was traditionally available and, no doubt, still is in rural areas.

I also take it for granted that people value personal privacy, since I have rarely met anyone who can satisfy me that they do not. People sometimes say to me, "I really don't worry about my privacy, because what do I have to hide?" But one has only to start asking questions about "How much money do you have in your bank account?", "Have you ever had psychiatric care?", or "Have you ever had an abortion?", and people quickly discover, "Well, I do have some sense of privacy in the form of a fair amount of information about myself that I prefer to keep under my control." That is a basic definition of concern for informational privacy, which is the subset of the general privacy topic that I am concerned with in this essay.

I want to emphasise that privacy as a value and a human right is technologically neutral. To be in favour of protecting one's own privacy interests, is not to take a position, positive or negative, on the application of technology. For example, the legislation in British Columbia on privacy in the public sector, like the federal *Privacy Act*,[3] covers both manual and automated records on individuals.[4] My concern, as the Privacy Commissioner for British Columbia, is for what you would properly call informational privacy, or data protection, as a constitutional, legal, and non-legal right or claim by individuals. As noted, informational privacy is only part of the big privacy picture. It has nothing to do, for example, in terms of my own jurisdiction, with controlling wiretapping, or dealing with Peeping Toms, or eavesdroppers on airplanes. There are even some limits on my jurisdiction with respect to such invasive practices as strip searches or body cavity searches (records have to be created). There are all kinds of states of privacy worthy of protection, and one of the things I want to suggest is that the Privacy Commissioner of Canada, Bruce Phillips, and his provincial and territorial counterparts, should be given a much broader jurisdiction, over a wider set of privacy issues, than simply informational privacy.[5]

---

3 R.S.C. 1985, C. P–21

4 *Freedom of Information and Privacy Act*, R.S.B.C. 1996, c. 165 at Schedule 1, s. 42(g).

5 I have developed this theme, at least a little, in D.H. Flaherty, "Visions of Privacy for the 21st Century," in C. Bennett & R. Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age*, (Toronto: University of Toronto Press, 1999) at 19–38.

II. PRIVACY AND THE COURTS

I HAVE SAID TO YOU that I regard privacy as a non-legal right in many ways. The kinds of interactions we have with our families, our relatives, our friends, our neighbours in a small town, or with people we have just met, all reflect various states of privacy, like exercising the concept of reserve when we are dealing with strangers. There is the important idea of preserving and protecting an intimate friendship or relationship, or just simply intimacy with another person, perhaps a partner, which presupposes a voluntary exchange of "intimacies." All of those are states of privacy that, really, we have to assert and claim for ourselves and are not simply the product of legal rights as such.[6]

So, ironically, although I am speaking to a group of people who are largely lawyers, I am interested in ways in which personal privacy can be protected under legal systems and under the rule of law, but largely without recourse to the courts, because it is too expensive and tedious to do so in ordinary instances and cases. In fact, one of the issues I want to raise for consideration is, "Is privacy best protected in the courts?" I will return to that theme, acknowledging, of course, that the Supreme Court of Canada is regularly determining how much privacy we are entitled to in our relations with the state on the basis of the *Charter of Rights and Freedoms*.[7]

I am not concerned in this paper with the complex issue of how privacy is treated in the courts, such as in the acceptance or rejection of evidence in criminal cases. I am aware of the U.S. and Canadian privacy litigation, especially under the *Charter*. The book by Ellen Alderman and Caroline Kennedy called *The Right to Privacy* is literally, chapter after chapter, about American privacy cases.[8] I am not aware of such a book in Canada, but it would now be possible to prepare one. We do not have a strongly developed tradition of privacy litigation, except with the Supreme Court of Canada's interpretation of sections 7 and 8 of the *Charter* in criminal cases, often involving drug charges.[9] As an idealist, I would like to see the *Charter* explicitly amended to include the right to privacy, so that those wishing to assert their privacy "rights" could go to court.[10] I have not abandoned litigation as a way of protecting what

---

6 I treat solitude, intimacy, anonymity, and reserve as the four states of privacy. See A.F. Westin, *Privacy and Freedom*, (New York: Atheneum, 1967) at 31–32.

7 See *R* v. *M.R.M.*, [1998] 3 S.C.R. 393 and *R. v. Godoy*, [1999] 1 S.C.R. 311.

8 E. Alderman and C. Kennedy, *The Right to Privacy*, (New York: Knopf, 1995)

9 See D. H. Flaherty, "On the Utility of Constitutional Rights to Privacy and Data Protection" in *Case Western Reserve Law Review*, Vol. 41, No. 3, 1991 at 831–856.

10 Testified, with the Privacy Commissioner of Canada, before the Special Joint Committee on a Renewed Canada, Ottawa, 9 December 1991, with respect to entrenching a constitutional right to privacy for Canadians.

an individual claims to be a right to his or her personal privacy. In fact, as Information and Privacy Commissioner, I write decisions that seek to strike a balance between openness and disclosure for personal information in records held by a very broad range of public bodies, and my decisions are reviewable in the courts.[11]

The issue remains: are courts the best way to protect privacy? In Quebec's Civil Code there is a right to respect for private life, in French "un droit a la vie privée."[12] It was used recently in a prominent case, where a Quebec woman's picture was taken in public without her permission. The photo was subsequently published in a newspaper, and she successfully sued for invasion of her privacy.[13] So that is an example of how the Quebec Civil Code has been used on occasion to protect privacy (for better or worse). The Canadian Charter is not used quite so easily, not least because of the costs of litigation in the common law tradition.

There are privacy tort acts in most of the western provinces. They are simply called Privacy Acts and they mostly originated in the 1960s.[14] They are rarely used, they have not been very successful, and they really do not address, successfully, the four privacy torts that Dean William Prosser identified in the *California Law Review* in 1960, as including intrusion on solitude, public disclosure of private facts, putting people in a false light in an offensive fashion, and unauthorized commercial use of one's identity.[15]

I think we have a real problem in Canadian law, of how do you help someone who is alleged to have suffered a tortious invasion of his or her privacy, who is alleged suffering or harm, and which falls into one of Prosser's categories? Certainly, suits are filed very infrequently in such areas, and my impression is that they are not very successful.

III. PRIVACY COMMISSIONERS

IN CANADA, WE HAVE invented and created the idea of both privacy commissioners and freedom of information commissioners. The privacy commissioner model is flourishing all over the world. All of the European Union countries have the equivalent of privacy commissioners, who are often called data protection commissioners. In Canada, our innovation is to put together the

---

[11] See online: <http://www.oipcbc.org> for my decisions.

[12] *Code civil du Quebec*, R.S.Q. 1991 c.64, arts. 3, 35

[13] *Aubry* v. *Editions Vice-Versa inc*, [1998] 1 S.C.R. 591.

[14] P. H. Osborne "The Privacy Acts of British Columbia, Manitoba and Saskatchewan" in *Aspects of Privacy Law: Essays in Honour of John M. Sharp*, ed. Dale Gibson, (1980 Butterworths: Toronto) at 73.

[15] W.L. Prosser, "Privacy," (1968) 48 *California Law Review* at 383–423.

information commissioner and the privacy commissioner, as has been done recently in Manitoba, by giving jurisdiction over the *Freedom of Information Act* and *Privacy Act* to the Ombudsman. So, what we have done is to create in almost all the provinces of Canada (except Prince Edward Island, Newfoundland, and Nova Scotia), privacy commissioners who are intended to be a source of *systemic* solutions for informational privacy issues. But we do not have jurisdiction over such matters as the privacy aspects of credit reporting, although I think we should. We do not have obvious jurisdiction over genetic testing, or drug testing, or strip searches by the police, although if records are created in such fields, I do have jurisdiction over them in British Columbia. But the generic privacy commissioner is an attempt to set up an administrative tribunal with a pro-active role—what I call the privacy watchdog mandate—to protect the privacy interests of individuals in the face of what is perceived to be invasive technology or invasive practices.

What we try to do is to transparently balance competing values in both decision-making on access to records and in advice-giving.[16] For example, I was recently involved in reviewing the use of data for a mammography screening program in British Columbia. I read in the press about the fact that the B.C. Cancer Agency and our Ministry of Health were going to write letters to every woman over fifty who is not in the database of the Cancer Agency, and tell them that they should get mammography screening. I wondered where they were going to get the data.

It is an example of the application of technology to conduct data matching, because one can take the list of names under the Medical Services Plan, which contains everybody who has health insurance—and all the people in the database of the B.C. Cancer Agency—and match them together for a specific purpose. Ages are included in the Medical Services Plan database, so you can see who has not been treated by the B.C. Cancer Agency. So I stimulated a debate within the Ministry of Health whether this was an appropriate use of the Medical Services Plan database. I consulted with a variety of people, including the women who work with me. And at the end of the day, I agreed with the Minister of Health that it was an appropriate use of data to send the letters to these people. And there were some complaints subsequently made to me as Privacy Commissioner that this practice was not an appropriate balance of competing interests but, in my view, it was ultimately acceptable.

The problem with the balancing issue is that my job requires me and my colleagues to give advice a lot of the time. And I can sometimes give advice until I am blue in the face. Attorney General, Colin Gabelmann, of the NDP, decided to institute criminal record checks for everybody who works with

---

[16] D. H. Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?" in *Technology and Privacy: The New Landscape*, eds., Marc Rotenberg and P. E. Agre (MIT Press, 1997) at 167.

children in the province. Now, at first blush, that might sound quite reasonable in an age where we have serious problems with sex offenders and paedophiles preying on young people. But I asked the Attorney General's ministry, "Where was the social scientific evidence that this practice would be beneficial and would actually protect children?" At the end of the day, they could offer no persuasive evidence whatsoever from any other civilized society on the face of the earth. But, that did not stop the NDP government, and the legislature, from unanimously going ahead and spending perhaps $15 million a year running criminal record checks on one-sixth of the adult population of British Columbia, who have any contact with children.

The Ministry of Health ran such names against the records in the Canadian Police Information Centre (CPIC), which I regard as giving parents a false sense of security. Almost nobody in the first 100 000 or so checked were found to be unqualified to work with children.

Why? Because paedophiles are much too devious to be caught by such a system. And, at the end of the day, in my jaundiced view, a very expensive system has had little direct benefit.[17] But, at the end of the day, the legislature can do what it wants in a democratic society and, from the point of view of a privacy commissioner, our job is to articulate the privacy interests that are at stake in a particular situation and, simply defer to the legislature for the final decision.

There is no question that human beings have valued personal privacy in the face of assaults by technology over time. Many of the great innovations of the so-called Industrial Revolution, the telegraph, the telephone, the camera, were initially seen as highly invasive of personal privacy, perhaps leading to the end of private life.[18] In every instance, ways have been found to protect our privacy interests. I remember, with some embarrassment, that the continued use of party lines for "private" subscribers in Lachine, Quebec, in the late 1940s, facilitated eavesdropping on one's neighbours. This is a reminder that privacy-enhancing technologies, in this case the private line, are not new. Later I will illustrate some examples of invasive technologies as we start the 21st century.

A. Technologies Searching for Applications

My concern is with technologies that are in search of an application. This is a fancy description for the following example: There was a drug testing system developed for prisoners in the United States, in the 1980s, called the EMIT system. It was very cheap to do a test. But, the promoters had to sell more machines, very simple machines, in order to make more money. Essentially,

---

[17] D. H. Flaherty, *Controlling Surveillance, supra* note 16.

[18] D. J. Seipp, *The Right to Privacy in American History*, Harvard University Program on Information Resources Policy, (Cambridge: Harvard University, 1978)

employers started using them on people in the work place. The problem with the EMIT system was that the standard error deviation was higher than the normal incidence of drug users in our society, leading to an excessive number of false positives. EMIT was a technology in search of an application, with too many errors inherent in it, with at least short-term negative consequences for particular people. Privacy commissioners are constantly looking for such examples.

I wrote a book, published in 1989, called *Protecting Privacy in Surveillance Societies*.[19] The theme of preventing surveillance societies is an important one. Because, at the end of the day, what we are trying to do as privacy commissioners is to prevent, as much as possible, unnecessary surveillance of one another as human beings by governments, by corporations, or by our fellow human beings. That is a constant theme of our work: How much surveillance is too much surveillance? You will note that the mammography example that I used is a form of surveillance of the population. There may be people with religious or ethnic reasons who do not want (or are not allowed) to go and receive a mammography, but they are still going to get a letter from the government saying that it would be a good idea for them to do so.

Some of the threats to privacy posed by technology come from the blurring of public/private boundaries. An example of that is Smart Health in Manitoba, owned by EDS and the Royal Bank, which has been in the start-up phase of building a health information network for the province of Manitoba. Several years ago, when they started this process, I was one of those privacy advocates who said, "How can you possibly do this in Manitoba without health privacy legislation?" How can you have the Royal Bank, which then owned the entire company, building a health information network for the province of Manitoba? The government, in its wisdom, took such suggestions seriously, and brought in, not only a *Privacy Act*,[20] but health information privacy legislation, the first of its kind in the country.[21] Most of us in the privacy business regard the latter as a model in that regard. Private companies like ISM-BC, IBM, and Smart Health are getting directly involved in the operation of data systems as part of the outsourcing of government services that is becoming so common these days. What are you going to do under those sorts of circumstances? Are there any solutions? I think that Smart Health is finding appropriate solutions.

Technology, therefore, poses both risks and benefits for personal privacy. Let me just list some of the practices that are posing problems. I heard a private detective speak in Vancouver, last Friday, as part of the annual privacy

---

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

[20] C.C.S.M. P125.

[21] *Personal Health Information Act*, S.M. 1997, c. 51

conference that my office runs. He told us that if you could spend $500 to $1 000 a day, he could find out almost anything you wish. He tried to claim that he would not breach legal or ethical boundaries, but I am very sceptical on that point. He is talking, of course, about following people, engaging in eavesdropping, tape recording, photography, and tapping of telephones. Recent U.S. events have too well illustrated the risks of such practices.

B. Digital Footprints

On to other kinds of things, which are much more trendy in late 20th century than the old fashioned private detective following someone around. We generate digital footprints as we use the internet (the World-Wide Web, as we send out email, or as we use our credit cards).[22] Detailed profiles of individuals are due to the growth in the capacity of intelligent software. There are now quite extraordinary data mining algorithms, developed largely by banks, that will allow them to surf through all of the personal data held by the Royal Bank, or the Bank of Montreal, or Citibank, and will profile your financial and commercial transactions almost completely. That sounds very appealing if you really want to have a relationship, as it is called, with the Bank of Nova Scotia, for example. If all you want to do is buy a Guaranteed Investment Certificate, you do not really want to enter into a life-time relationship with a financial institution. Often these kinds of "data mining" operations are not transparent to us, and we have not consented to them. If you want to agree to a full-scale "relationship" with the Royal Bank of Canada, an adult is free to do so. Take the Air Miles program, or the Safeway customer loyalty program, for example.

I recently discovered while shopping at Safeway that it was going to cost me ten dollars for detergent rather than eight, because I did not belong to the Safeway Customer Club. I obtained an application form and took it home like a good, academic privacy commissioner to read the small print. I did not like it. The next day, I called Safeway Customer Service in Victoria, I was referred to the Vancouver office, Calgary, then California, and back again to the Calgary office. After a while, I got a recorded message and left a message. A representative of the vice president of public affairs called me back and tried to tell me what Safeway does with its customer data. The first thing that she said was that such information is stored in the head-office computer Salt Lake City.

Now, that is not terribly comforting to a Canadian provincial privacy commissioner, or any Canadian consumer. The practice is not transparent to consumers, and any consumer challenge would face major legal barriers because of lack of jurisdiction. I learned eventually that Safeway does not need a real name, a real address, or a real phone number. You can check off that you never

---

[22] D. H. Flaherty "Privacy on the Internet" online: <http: //www.oipcbc.org /publications /presentations/internet_privacy.html>.

want to hear from them again in the form of sales promotions. Not surprisingly, I have a Safeway Customer card with a totally fake name, address, and phone number; and I saved a whole two percent on my first grocery bill. But, you should not have to go that far to protect your privacy. By sheer accident, a newspaper reporter called up that same week to ask if I had anything to say about Air Miles and the Safeway Customer Club. I have received more play in the media with that particular interview than with many other things I have done.

Privacy is invaded by all kinds of practices. I discovered, by doing a site visit, for example, that everybody going in and out of the new Vancouver Public Library was subject to video surveillance. And tapes were being kept for a period of time. I asked the individual responsible a former U.S. marine, "Do you realize that you are creating a record under the provincial legislation?" And he responded, "Says who?" Fortunately, with some assistance from the director of my office, we were able to agree that, yes, the tape was a record under the provincial *Freedom of Information and Protection of Privacy Act*.[23]

Here is another example of something I have done successfully in British Columbia to restrict surveillance. I was concerned, at the start of my term, about the fact of automated databases being used for unintended purposes, such as to locate people. The BC Assessment database, located on BC Online, contains all real estate assessments for a province of 4 million people, with probably more than 1 to 1.5 million property owners listed. These real estate ownership records are accessible, for a modest fee, from a public library, or from a law firm that has an account. I did not like the fact that this province-wide database was searchable by name. I worried about the privacy of battered spouses, sheriffs, police officers, social workers, and doctors who perform abortions. We reached an agreement with the BC Assessment Authority whereby you can no longer locate an individual by name from this source, since we have taken the names of people out of the automated version of the real estate assessment authority records.[24] You can still get the names and addresses by going locally to a municipal hall but, otherwise, you have to just search for a piece of property for a person by address. I regard that as considerable progress in terms of protecting certain aspects of individual privacy in British Columbia.

---

[23] D. H. Flaherty, J. M. Young and R. K. Friesen, "Investigation Report, P98–012: Video surveillance by public bodies: a discussion, Office of the Information and Privacy Commissioner for British Columbia, March 1998, online: <http: //www.oipcbc.org/investigations/reports/invrpt12.html>.

[24] D. H. Flaherty and M. E. Carlson, "Investigation Report, P98–011: An investigation concerning the disclosure of personal information through public property registries, Office of the Information and Privacy Commissioner for British Columbia, March 1998, online: http://www.oipcbc.org/investigations/reports/invrpt11.html.

The Minister of Municipal Affairs subsequently put our recommendations into law.

I have already said to you that my perceived role as Privacy Commissioner is to identify the privacy interests that are at stake in each situation that I encounter, in each application of technology, in each new product that comes along. Right at the moment, we are working with the provincial Ministry of Health on plans for a Health Client Registry, which will be a considerable enhancement to the simple "tombstone" data available in our Medical Services Plan. What we as privacy watchdogs require is what we call a "privacy impact assessment." Other privacy commissioners in Canada are developing the same notion. We now have a template for what a privacy impact assessment should look like, developed in conjunction with the Chief Information Officer for the province.[25] We are making sure that residents of British Columbia, the citizens of British Columbia, do not have to do this work for themselves. We are sitting down with the Ministry of Health and saying, "How exactly is this client registry going to work? Why are you doing it? What are the consequences for privacy?" At the end of the day, the average citizen will have some advanced assurances about what is happening, based on our detailed research and investigations. I am quite confident, based on my experience to date, that they can be addressed in a practical, common sense, cost-effective way since, I believe, these traits have been the hallmarks of the work of my office during the past six years.

What are the goals of privacy protection and legislation? Partly it is self-regulation. Those companies that are in privacy-intensive businesses, that is, companies which collect a lot of personal information, should self-regulate by adopting the privacy code recently promulgated by the Canadian Standards Association as a product of public and private sector cooperation.[26] Self-regulation is the beginning of wisdom.

C. Protective Legislation

What is new in protective legislation for privacy? This issue arises because, from my point of view, common law remedies do not appear to be useful. The recent Manitoba legislation, that I have already mentioned, is quite progressive, both from the freedom of information and privacy side and with respect to the coverage of all health information. The major newcomer is Bill C–54, the federal privacy bill, which was introduced in late September 1998. The federal

---

[25] "Privacy Impact Assessment Model," Office of the Information and Privacy Commissioner for British Columbia, 1998 online: http://www.oipcbc.org/publications/advice/pia.html, and "Privacy Impact Assessment Form," Information, Science and Technology Agency, Ministry of Advanced Education, Training and Technology, Government of British Columbia, 1998.

[26] Canadian Standards Association, *Model Code for the Protection of Personal Information* (Rexdale: CSA, 1996). online:: www.csa.ca.

privacy bill, from a provincial privacy commissioner's point of view, is an answer to our prayers. It is a miraculous intervention by the federal government, which I think will be a catalyst to action in the provinces for data protection in the private sector. At the end of the day, I do not care whether the federal privacy bill covers the private sector in British Columbia directly, or whether we come up with a "Made-In-British Columbia" solution by extending our existing provincial *Freedom of Information and Protection of Privacy Act* from the public sector to the private sector (to the extent that there is any difference between the public and private sector these days). IBM is increasingly running most of the data operations for our government, either directly or through its subsidiaries, such as ISM-BC. IBM is also doing major development work for the privacy-intensive ministries, such as the Ministry for Children and Families.

The federal privacy bill essentially says that for personal data processed as part of a commercial activity, the bill will have immediate jurisdiction. I expect that Canadian Blood Services can send membership information from one part of the country to another and would not be caught by this particular piece of legislation. But *Beautiful BC Magazine* has customers and subscribers across the country and around the world: such activities would be covered by this particular piece of legislation. So would Roger's Chocolates, a popular Victoria-based chocolatier with a mail-order business. Now, neither of those businesses have heart-rending privacy problems compared with health information or police information. Nevertheless, these are areas in which customers, clients, and employees should expect fair information practices to be followed. If the provinces do not act themselves to occupy this commercial territory, the federal bill will prevail.[27]

I also want to mention the European Union directive on privacy protection, which went into effect on 25 October 1998. It was, perhaps, typical that it was a front-page story the following day in the *New York Times*, but I did not see an explicit mention of it in the Canadian media.[28] In North America, only Quebec, which has regulated its private sector since 1994, meets the standards of the European Directive.[29] The E.U. Directive essentially says that European countries can move personal data in identifiable form between and among each other for commercial purposes, without any kind of scrutiny for privacy

---

[27] Bill C–54, *An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act*, 1st Sess., 36th Parl., 1998, (2nd Reading 3 November 1998), at s. 4, 27, 30.

[28] E. L. Andreurs, "European Law Aims to Protect Privacy of Data: Some Trade with U.S. Could Be Disrupted" *The New York Times* (26 October 1998) A1.

[29] Loi sur la protection des renseignements personnels dans le scteur prive (Quebec), L.R.Q., c. P39.1.

protection, because each country, each of the almost twenty members, have equivalent, comparable protection for privacy in place. None of us in North America, except Quebec, could meet the same standard.

So we are in a situation where a Manitoba insurance company, moving customer information, or client information, or employee information back and forth from Winnipeg to the United Kingdom or France, runs the risk now of the national data authority in a European Union country saying that you cannot transfer that information to Manitoba, because there is no adequate protection for European personal data that is coming to this province. The Americans are trying to fight this directive as a potential trade war and remain persuaded of the merits of self-regulation. I hope they fail. I think that the federal bill is a very good step in the proper direction of following the model of Quebec and will put Canada and its remaining provinces in compliance with the European Union's Directive.

The federal privacy bill is being sold by Industry Canada and the Department of Justice protection for electronic commerce. That is perfectly fine with me. I am persuaded by Industry Canada that, as a nation, Canada is ideally suited to take advantage of electronic commerce in an entrepreneurial sense. And if one way to further protect privacy as the human right is to protect electronic commerce, that is very acceptable. It is a form of progress.

In terms of the theme of this paper, there are a series of privacy-enhancing technologies (PETs) that can also be used. Privacy enhancing technologies include biometrics, smart cards, active badges, the use of passwords, audit trails, and so forth. Some of them are well beyond being fads at this point in time.

I was invited to do a site visit at the BC Cancer Agency and I asked them, "You've got a provincial network with almost every woman over forty in the province in it.[30] It is accessible at eighty different places at your hospitals and treatment agencies. Do you use passwords?" "Yes." "Do you ever change the passwords?" "No." Not a good answer. "Do you have an audit trail in the system so we can find who looked at someone's record, if you're in that system?" The Cancer Agency had an audit trail system, but they had never turned it on. Now, I can assure you, those practices have changed since my site visit.[31] Those are examples of the kinds of practices that we try to encourage to allow technology to protect the privacy interests of citizens and computers.

I have to admit that I am somewhat pessimistic about the ability of Privacy Commissioners in this kind of setting. Absent, particularly, is support from the legislature and from interested or aroused citizens. Technology is moving very quickly. B.C. is developing not only an enhanced version of CPIC (the

---

30 D. H. Flaherty, "The British Columbia Cancer Agency: The Results of a Privacy Check-Up," Office of the Information and Privacy Commissioner for British Columbia, April 1998 online: http://www.oipcbc.org/investigations/site_visits/Cancer.html.

31 *Ibid.*

Canadian Police Information Centre), but also a regional police information system called JUSTIN. Since they are using 1970s technology in CPIC, it should be upgraded. But JUSTIN and CPIC itself, will sweep up even more data on us. With the software that is available today, it will become even simpler to amass information that may or may not be correct or appropriate on individuals. Once such rich data bases exist, it is almost impossible, in practice, to control access to them.

And I need not discuss the latest person, in this case in Newfoundland, who was falsely accused and arrested and then released on the basis of DNA evidence, as an example of the threat of technology, although, in this case, DNA actually helped protect an innocent person. But you can just imagine, in a small Saskatchewan town, or as has already happened in England, if there is local a sex offence of some sort, all males can be urged to come forward to give a "voluntary" DNA sample, and the kinds of pressures that puts on individuals if they wish not to conform with what would probably be a normal reaction: yes one should do that. That poses a set of very, very interesting questions, and I am not so arrogant as to think I know for certain what the answers are in that particular kind of case. There is not only the presumption of innocence, but also the issue of whether such a voluntary DNA sample should be kept permanently or destroyed after the intended use is accomplished. Some law enforcers would like to have a permanent DNA record for each of us.

IV. Other Forces Affecting Privacy and Technology

I WANT TO ADDRESS, briefly, the relevance of economic and market forces to the issue of privacy and technology. As I obtained more privileged information about plans for information systems during my work as Privacy Commissioner, I become more conversant with the realities of market forces and economics in this process. Many of the privacy anxieties of official and other privacy advocates are somewhat paranoid in terms of what the market, in the form of a business case, will actually allow to happen. Thus, one fear associated with the Interim Report in September 1998 of Health Canada's Advisory Council on Health Infostructure was that its proponents intended a vast national data bank of the personal health information of each and every one of us. Admittedly, it took interactions on the part of my fellow privacy commissioners to obtain assurances that that was indeed not the intention. Health Canada and provincial ministries of health will be fortunate to obtain the resources to permit medical records to be transported across the country electronically, with consent, or to allow relevant health records for individuals in any given health region to be so interconnected as to become useable. The simple fact is that it is not economically feasible to integrate large masses of personal health data. However, I expect my successors to have to deal with that issue.

What we are ultimately trying to do with respect to the use of personal information is to create trusted relationships among individuals, between individuals and their governments, and among consumers and customers and employees of corporations. We want to have trusted relationships and a culture of trust, with consent as crucial to the protection of what we call informational self-determination. The German Constitutional Court, in 1983, released a famous census decision, which identified the concept of informational self-determination.[32] The principle is that we should be able to control the disclosure and circulation of our own personal information. Now, think about it: you make a phone call with a credit card, you make a purchase with a credit card, you check into a hotel, you buy airline tickets, or you visit a web site or participate in a chat group. We are losing control of our own information all of the time, which is why we have to have these systemic protections in place, through the use of privacy commissioners, to whom you can complain, and who try to give advice and assistance about the protection of privacy interests. But at the end of the day, you must, try to protect your own privacy, because you are best positioned to do it yourself.

I would also like to briefly address the relevance of politics and ideology to the issues of privacy and technology. There is a serious risk that privacy commissioners will function only as legitimators of new technology, a theme that I developed in a recent article.[33] Similarly, I will only remind you of the ideology of capitalism which drives politicians in particular to seek any methods of cost cutting, avoidance of waste, and reduction of fraud that will save the money of taxpayers. While I am well aware of the meritorious aspects of such concerns, my experience is that they also usually lead to less privacy than desirable for one segment or another of our fellow citizens. In the heat of the moment, politicians in any Western country are difficult to persuade to put privacy ahead of some other goal.

V. CONCLUSION

NOW, AT THE END of the day, comes this question: What can or what should lawyers do for their customers, for their clients, in these kinds of situations of real or alleged invasions of privacy? Surely you need to be aware of the relevant legislation. The *Personal Health Information Privacy Act* in Manitoba, for example, to the best of my knowledge, covers health information everywhere: doctors' offices, private labs, all kinds of private locations that we do not now cover in British Columbia, because we have not been wise enough to pass a

---

[32] *Tenth Report of the Data Protection Registrar* (London: HMSO, 1995) at 16.

[33] D. H. Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?" *supra* note 16 at 46.

similar piece of legislation.[34] So, any clients who have health information are now facing a set of standards, and probably liabilities, for failing to comply with that Manitoba Legislation.

I have already said that self-regulation for the private sector needs to be promoted. Interested parties should look at the contracts that are used among service providers to companies that are in privacy-intensive industries, where they collect a lot of personal information. Oaths of confidentiality are an important matter, especially if the signer knows what an oath of confidentiality means. I am often told by psychiatric hospitals that everyone here has signed an oath of confidentiality. I know that on their first day at work, they signed other things, including their application for a Social Insurance Number. Do staff have any reasonable idea what an oath means? There is a component of staff training here that is very important on an ongoing basis, not just when a piece of legislation comes into effect.

I also want to emphasize the importance of meaningful consent for data collection and use. When we go to get our cars fixed, we avert our eyes when a service person puts a form in front of us, saying sign here. And, literally, if my garage took my car for a drive on the great pier in Victoria and drove it off the end, on the basis of what I signed, it would likely be my fault. So when is consent meaningful? Do people have any idea what is going to be done with their personal data when they go into hospital, or when they go into a doctor's office? We have done serious work on that issue in B.C. I must say, that after five years of work, from my point of view, the most sensitive privacy issues at the provincial level are in the health field, which is largely a matter for provincial jurisdiction. I think that all of us, ultimately, have to be very, very sensitive to the health issue. You may think that I have been giving a self-advertisement for privacy commissioners and that I am trying to justify my job. One of the virtues of my position is that it ends in August 1999 and is not renewable, because information commissioners are so threatening to political interests in British Columbia that we have to be replaced!

You have to be your own privacy commissioner. And you have to decide, in your own life, to the extent that you can do it, where you want to draw the line between openness and candour; or, to what extent you want to control your personal privacy. You reflect on it: all of us protect our personal privacy day in and day out by various strategies that we have developed. That is exactly the way it should be. Privacy commissioners—and technology—come into play when you can no longer protect your own privacy by yourself, which is the challenge that most of us face as individuals in our daily lives.

---

[34] D. H. Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?" *supra* note 16 at 46 at 188.