Regulation or Self-Regulation: Privacy Protection and the Information Highway

by Bruce Phillips

Everyone agrees on the need for business to respect the privacy of the individual. But there is less agreement on the extent to which privacy should be protected or on how this is to be done. In a recent appearance before the Senate Standing Committee, the Privacy Commissioner argued strongly for government regulation as opposed to the self-regulation. The following is an extract from his testimony along with comments and questions from some of the Senators present.

Three years ago I recommended that all financial institutions under federal jurisdiction be required to adhere to a code of fair information practices, with an independent oversight and dispute resolution mechanism. At the time a good deal of interest was evinced in a so-called sectoral approach. That is to say, a code of practice being developed specifically for the banks and that being embodied as regulations in the *Bank Act*.

I thought that was not a bad approach then. I still think it is not a bad approach. But my own thinking on this subject has evolved a good deal partly because of the multitude of changes that have taken place in the whole field of information management brought about by the marriage of computer technology and high speed transmission systems, and other developments as well.

Some of those include the following:

- the emergence in the province of Quebec of a new privacy regime which covers both the private and public sector and the consequent development of uneven standards across the country if other provinces follow suit;
- the imminent application of the European draft directive on privacy practice, which will empower member states of the European Union to decline to make data transfers to countries which they consider do not have adequate protection as defined by their own draft directive. At this moment we do not enjoy that standard.
- the government's own rapid move toward the implementation of new information highway techniques in the management of its own information holdings which comprehends, among other things, the marriage of private and public sector data management systems.

At the moment we have a federal *Privacy Act* which lays down conditions under which the Government of Canada may collect, use, dispose and disclose personal information. Once those arrangements are complete and we have a marriage of both government and private sector systems, what then becomes of the various forms of protection that are now offered in the *Privacy Act* unless amendments are made to cover that contingency?

Those are some of the major developments that have taken place, not to mention overall the very rapid conversion of almost all of the information management practices both in public and private sectors over to databases that are now almost completely computerized and now offer improvements in terms of the manipulation, marriage of databases and the compilation of dossiers in a degree and at a speed which was never contemplated as recently as five years ago.

This has led me to the conclusion that we need now a much more comprehensive look at the whole issue of

Bruce Phillips is the Privacy Commissioner of Canada.

privacy protection in the information highway age. When I first broached this subject generally in 1992, it was a fairly lonely position. I did not have a whole lot of company. But I feel a lot less lonely now. The government's Advisory Council on the Information Highway recently concluded its study of this particular aspect of information highway problems. Although its final report has not been published, I have seen its recommendations dealing with this issue. The advisory council will be advising the government that legislation is needed in this field and that oversight mechanisms are required.

My provincial counterparts in Quebec, Ontario, and British Columbia now all subscribe to the proposition that it is no longer possible to get by on pure voluntaryism.

> ***We have to see this issue in another dimension other than simply self-regulation. We are not self-regulating or regulating a commodity here. Privacy is not a hockey helmet***

We are talking about the legal recognition of a right and recognizing that in the specific terms in which we are dealing with it here, namely in the commercial world and in public sector information holdings. So that there are two parts of this, one of which is philosophical and the more important part if you are to understand this issue.

The other issue is whether adding a few more regulations to the statutes will impose uncomfortable or inconvenient burdens on a particular sector of business.

Everything in life is self-regulated to a certain extent. We do not have policemen sitting in the back seats of our automobiles when we drive to work in the morning. We regulate ourselves to obey traffic laws, but we know that there is a law to which we are expected to conform and that there may be a policeman waiting around the corner to see whether we do. It is that kind of inducement which helps us all understand that we have common obligations to society, but we are not left entirely to our individual discretion. That is the basis of my argument about privacy protection.

I listen with great interest to the Canadian Standards Association when they talk about voluntarism. Their code is a very interesting and exciting development. Over three years they have produced ten very important principles. If that were the law of the land, privacy advocates would be very content with it, because it expresses all the basic and important principles of privacy protection. However, if it is left entirely to the discretion of the individual corporations, and indeed in the CSA system you can subscribe to the code or not, as you wish, then it simply is not good enough.

There is also a lot of interest in a recent Equifax survey which purports to show that the majority of Canadians would much prefer to have this whole matter dealt with by the private sector. Of course, that survey was commissioned by Equifax Limited, which is North America's largest credit reporting institution. It was done and paid for by them, for their purposes. Furthermore the Equifax people, who include Professor Alan Westin, a noted privacy expert, noted that 74 per cent was conditional upon the assumption that business had satisfactory handled all the privacy problems.

I do not wish to get into a war on surveys, but I would offer you the Ekos survey done a year or so before. It was a much more comprehensive survey. It did not ask only one question about public attitudes toward government involvement in this, but several. It reported that approximately 90 per cent of the public was concerned and uneasy about the usage of information and that 65 per cent had concluded that it was necessary to get the government involved in a solution.

There are statistics and there are statistics, and we are entitled to take a hard look at their origin.

* * *

Senator Michael Kirby: I would like you to comment on two issues. First, what constitutes consent? Is it just someone signing their name? If they do that, should the consent only be for a limited period, such as a year or two? If you have your card for longer than that, do you have to sign for consent again? Second, what is your reaction to truly broad, unbelievably sweeping consent conditions rather than more narrow, focused and precise decisions?

Bruce Phillips: We try to describe consent as uninformed and informed consent, and to describe the difference. Informed consent is when it is written sufficiently largely and in enough detail that it is clear what is being talked about. Uninformed consent is the kind of thing you find on the backs of credit card applications — which I mentioned at the last hearing — in type so small that Superman would have trouble reading it, which says that the credit card issuing company can use the information for any purpose whatsoever. It says that right on them. I invite you to read them. That constitutes a waiver in perpetuity to any usage whatsoever which the company wishes to make of it.

All these credit card companies are very happy to subscribe to these voluntary codes and to tell you how

good their practices are. Nevertheless, for reasons I do not understand, because it seems to be contradictory to the policies to which they commit themselves and to the code, they insist on including that kind of language on the back of those applications. That is not informed consent, in my opinion.

It would be informed consent if, included in the description of the terms and conditions, there were the warning, in large print: "This application may be dangerous to the disclosure of your personal information in ways that you do not understand." That would get the customer's attention. That is more like informed consent.

I am reminded of the cellular telephone issue. People suddenly discovered that their intimate conversations were winding up on the pages of the newspapers. There was no informed consent in the sale and marketing of those products because people were not advised that that too was dangerous to their privacy. I believe that in cases like that there is an obligation on the person marketing the item to make it clear to the public what privacy implications are involved.

In respect of the particular issue here, I agree with you that this is not informed consent. There is an enormous power imbalance involved in all of these things. We know that. If people go to a bank for a mortgage and are desperate to get the house built before the rates go up next week, they will sign nearly anything to get that mortgage, including, if necessary, a waiver for subsequent third party use of the information.

The public needs to have that power imbalance redressed and to have more transparency and openness introduced into the process in the bargain.

* * *

Senator Leo Kolber: First, I must tell you that I am biased against legislation of almost any kind. You said that signing a credit card application gives your information in perpetuity. You know very well that you are giving a balance sheet which is a snapshot of what is happening on one particular day. I find that "in perpetuity" may be exaggerating the situation because a year later your financial information would no doubt be different. That point does not bother me. Could you define what you mean by privacy?

Bruce Phillips: Privacy, in the information age, is the right of the person to whom the information relates to retain some control over the disposal, collection and use of that information.

Senator Leo Kolber: That sounds like a good definition, but I am really getting at whether the cosmetics of this thing are outweighing the practicalities.

For example, a fellow makes application for a mortgage. He freely gives out his information stating his income and debts. If that information goes elsewhere; what harm has he suffered?

There could be embarrassment that his financial situation is not what he would like people to think it is; or it is much better than people think it is and they will come asking him for money or he will be solicited. I appreciate that is not a good thing. However, is it worth creating a new body of legislation? Lawyers will make a lot of money, the legislation will go to the Supreme Court at some point and there will be a whole new body of cases and law and implementation problems. In other words, are we making a mountain out of a mole hill?

Bruce Phillips: It is very difficult to obtain precise information about what occurs behind corporate veils. If there is no right of entry, it is difficult to find out what is happening.

I can give you specific instances of real harm being inflicted as a consequence of what I consider to be unfair or inadequate information practices. Books have been written on the subject. The largest body of journalism in history reposes in the United States where there is a privacy press that has been active for some time. They report literally hundreds of cases of people suffering real harm.

For example, there is a hard-working man who applies for a mortgage loan. The mortgage company took some preliminary details and stated that it all looked okay. Assuming it all checked out, he would receive the loan. He was told to go ahead and make the deal with the builder.

On the strength of that assurance he began making deals with his builder and signing contracts. In the meantime, the lending company did a more thorough check. They called him some time later and said, "Sorry, the deal is off, you are a dead beat. We just got a check on you from the credit company." It plunged that man into an enormous amount of difficulty with the builders. His employer heard about it. His job was in jeopardy. He had to pay legal expenses to sort it all out.

That was based on a credit report that did not even apply to him. It involved somebody else all together. That is what can happen when there is an absence of transparency in the process.

Senator Leo Kolber: That is a bad example, and it is unfair. Thirty years ago, I went to Brooks Brothers and ordered some shirts. I wanted to pay cash, however the clerk wanted me to sign something and become a credit customer because I would receive points. I did it. I got a letter from Brooks Brothers a week later saying I was a dead beat and I would not receive credit from their company.

I called Brooks Brothers back and they insisted my credit was no good. The clerk asked if my wife's name

was something and I said no. He said, "Did you live at this address?" I said no. There was another Leo Kolber some place who was a dead beat. I do not find the example you gave me very illuminating.

Bruce Phillips: I found it fairly persuasive. If the people concerned with those dossiers were made aware at regular intervals of what was in them, that kind of problem could be avoided.

There was a case of a town in New England where the entire tax roll of 1500 people were being carried as tax delinquents by a credit reporting company without their knowledge because there is no obligation by anybody involved in that process to let people know what is on their files. That is one aspect of privacy; it is not all of it, of course.

* * *

Senator John Sylvain: I was one of the biggest users of Equifax Canada Inc. Before it became Equifax, it was called the Retail Credit Company. The Retail Credit Company had to change its name to Equifax to get rid of the baggage it had acquired over all those years.

Forty five years ago I used a lot of their services. It is interesting how the information was gathered. It shows how far we have come in the collation of this information and the limitations that have been put on the type of information gathered.

In those days, they used to hire a bunch of young people — they were as low paid as you could get them — and they went around to Bruce Phillips' neighbour, Mrs. Smith, and said, "What kind of a guy is Bruce Phillips? Does he take a drink? Does he beat his wife?" This is what occurred.

One chap applied for automobile insurance to a company and was turned down because it was said that he was in the entertainment business. It turned out it was Peter Jennings who was here in Ottawa reading the news. He was not really an entertainer — as he is now — he has done well for himself. He had been turned down for insurance because of what some neighbour said about him being on CTV or CBC.

The system we had before was much worse than it is now. There were a lot of changes made and a lot of the information that used to be gathered is now prohibited. People cannot be described by their religion or morals et cetera which used to be written in large letters across the application forms.

There is still a need for the individual who is to lend the money to know something about the recipient. Senator Kolber, if you were a total stranger, he would want to know a little bit more and get some information from a third party perhaps. The question is how far that can go.

I have no objection to the underwriter receiving as much information as possible. I was an underwriter for many years, and I needed all the information I could get. I still made a lot of mistakes.

Once the information is given, privacy enters in. It could be given voluntarily if that is what the individual wants. Most people do not read anything on the back of an application form. They sign simply because they need the money.

There was a clause in an insurance policy in Quebec which had to be written in red because it was a co-insurance clause. It was still not read by anyone. If they did they would not have understood it.

How far should a financial institution go to explain that the information given for the purpose or transaction stays there? Do you see a difference between purpose and transaction? How far must the underwriter go and be given information in order to make a decision? Consequently, what happens to the information after that?

Bruce Phillips: A sufficient explanation ought to be given so that reasonable people would understand why the information is being sought. That is to say, in simple, big, easy-to-read type and in language that is clear and unambiguous and easy to understand.

The federal *Privacy Act* says you cannot collect information from people unless it is authorized by a program activity of the department concerned and without explaining why you want the information. However, it is pretty fuzzy as well. If I were to rewrite it, I would try to use language such as that.

If you are buying a cellular telephone, put a big warning label on the package. I am not kidding. I am serious. The label would say "Warning: This device is subject to interception by anyone in the general public. Be aware".

That philosophical approach to the explanation for the purpose for collecting information ought to be applied. It is simple, clear and easy to read.

Senator Marjorie LeBreton: I was particularly interested in your reference to one-stop shopping for banking, insurance, and so on down the line. My concern has to do with the rights of the individual and the privacy of the individual. When a person arranges a loan to buy a car or a mortgage to buy a house, they are nervous about it. They are so relieved when it has been approved that they will sign anything. They take up an offer to perhaps buy mortgage insurance or car insurance. Five years down the road, at a time to renew the mortgage, their situation vis-à-vis their health changes. This information is all there, and the lender learns that the person is ill. The institution is reluctant to lend them the

money or renew the mortgage. It also affects their ability to insure the mortgage.

Do you see that as a real risk or a fear in the future, and should the act be amended to take that type of scenario into consideration?

Bruce Phillips: You are really discussing an issue of credit worthiness. We have said over and over again that there is nothing in the Office of the Privacy Commissioner that resists the notion of the right of business to collect sufficient information to do its business. In every business transaction, there is at least an implied understanding between the two parties to the transaction that enough information must be exchanged so that both sides know what they are doing.

In the particular example you cite, the circumstances of the person who wishes to obtain credit have changed materially over the course of the relationship with the credit-granting institution. I would say the credit granter is entitled to that information.

I would go on to say, though, that I do not see that the rest of the world would be entitled to that information. That is our problem with all of this information collection business. What happens to it subsequently? How much does the client really understand what is going on? What recourse is there for the customer if there is dissatisfaction? What confidence is there in a system in which they do not have the right to get an independent investigator.

Those are the issues that I see. The right of the credit granter to ask for the information in the first instance seems to me to be a reasonable one.

Senator Marjorie LeBreton: You talked about the standards of European countries. You said that we in Canada do not meet those standards at the present time. Does the United States meet those standards? Does this in any way impede our ability to compete in the future?

Bruce Phillips: The answer to the second question is possibly, probably, unless we do something. The answer to the first one is no, the United States does not have, in my opinion, or in the opinion of any experts, what the European Community would consider to be adequate privacy safeguards.

The essence of the European approach is that both public sector and private sector information gathering and information retention and disclosure is governed by law and is subject to examination by a policeman, a data protection commissioner in all these jurisdictions. To them, adequate protection, which is the standard now contained in Europe for transborder data flows, does not cover voluntary codes of the kind that we have in this country.

I am baffled by the reluctance of the private sector to accept as a legal requirement what they are only too prepared to swear up and down they will vigorously enforce if they are only left to do it themselves. What is the difference? I say is that one is a traffic law where I say, "Just don't bother me, and I will not run any stop lights." The other one is, "Well, if you do run a stop light, somebody might catch you, and it will cost you $10." I do not understand, unless there is something involved in their practices which they simply do not want to talk about.

There are, I might add, many things not being talked about these days in the field of information management, not the least of them being security of information. This is a subject that is only a component of the privacy question generally. There was one survey that showed something like a quarter of all businesses surveyed have suffered losses because of computer crime. I was at a conference in Toronto a few months ago, and I talked to several people from private corporations who are responsible for computer security. They had all suffered losses. Companies are not talking about it. They are afraid to talk about it because it might rattle public confidence in the security and integrity of their information holding systems. Those costs are being passed on to the public, and the public does not know anything about it.

There was a computer security conference in Montreal a couple of months ago, and the chief of computer security of the United States Department of Defence was there. He told the following story. He became concerned about computer insecurity. He hired tiger teams or attack teams and told them, "Do your best to see if you can penetrate my systems." I think there were several hundred or a thousand attempts, and they were successful in cracking his systems over 90 per cent of the time and were detected doing it only 5 per cent of the time. These were some of the most sensitive computerized databases in the entire United States, which shows you how vulnerable they are. I was informed the FBI ran similar tests with similar results.

That is a whole other aspect of the privacy question, because that covers all kinds of information, including personal information. If the Department of Defence of the United States can do no better than that, what kind of security does your file in some bank have? It is something that this committee may want to consider. It is a big issue, and it is getting bigger.

* * *

Senator David Angus: I do not see that there will be a huge new growth industry for lawyers. Nor do I see a great new body of jurisprudence building up. I also do not see a huge mushrooming bureaucracy that you ascribe to his comments.

Today, people only make complaints when they know about it, or if they feel they have enough moral suasion that something might be done about it. Basically, they know it is all voluntary and there is no law behind it.

Are not the 1,500 complaints which you see on the government side, and whatever other number there is on the private side, like needles in a haystack in terms of what ultimately there would be?

Bruce Phillips: I do not have a crystal ball. You have certainly raised a very good point, senator. I will address it this way. When it comes to enforcement, oversight and sanctions, a lot depends on the way you go about it. You can put in place a hard-nosed kind of system with a police mentality driving it; or you can put in place an ombuds approach committed to education, committed to understanding the culture of business and committed to bringing business along in a greater appreciation of what is involved.

It is my own view that you do not have to fine banks or transportation companies vast sums of money, or anything of that nature. I think the power of embarrassment is the most effective power there is when dealing with things such as civil and human rights. If a bank were found by an independent ombudsperson to be systematically or repeatedly offending good privacy practice, and that was drawn to the attention of the public, then I do not think you would have to go a whole lot farther than that before the bank would understand that the retention of its clientele would require a different approach on their part.

There is always an ongoing debate in matters of this kind about whether my kind of office, which is that kind of office, or the order-powering agency is better.

* * *

Senator John Stewart: I am interested in the way you focus on financial institutions. You say changes in banking legislation over the past several years have created increasingly powerful financial interests. Immediately upon reading that I said to myself: Mr. Phillips is really against that legislation, not on financial grounds but because of its implications for privacy. It seems to me that, in a sense, you throw up your hands and say, "Well, each segment of this financial department store has a right to specific information, but of course there should be a water-tight wall between each segment of the department store." You seem to think that that would be sufficient. I suspect that regardless of what the law says with regard to rights, that these walls are quite pervious and that information will leak through in gallons.

If privacy is as important as you say it is — ought we not to think of the validity of the merging of these various financial operations that were permitted by the previous legislation so that the next time around, with a view to privacy, we separate some of these activities, such as insurance, banking and the like? Perhaps you do not want to go that far.

Bruce Phillips: I state this as a self-evident fact. Chartered banks are now authorized to participate in a great many other financial activities from which they were previously foreclosed. As a consequence, in my opinion for what it is worth, they are bigger, stronger and more powerful institutions. Individual clients are not as strong.

To come to the specific point you raise about one-stop shopping, that addresses what we call in our racket the "transparency issue" or the "informed-clientele issue". If you are collecting and using information about people, it should be clearly understood by everybody what is your information practice. Thus, if you are running an operation in which you are offering a variety of services, and if you collect information from a customer and you may use it for all those purposes, they should know about it in advance. That is what I am saying.