PRIVACY ON THE INFORMATION HIGHWAY

John G. Boufford*

Privacy and information technology remind me of the story of the only lawyer in a small town who was having difficulty earning a living. So, she invited a second lawyer to set up another practice, and there was enough work for both of them.

The moral of this story, of course, is that it takes two to have a difference of opinion, and one would expect that there might be many differences of opinion on the issue of privacy between human rights advocates and information technology professionals. But that assumption may be wrong.

The Canadian Information Processing Society (or CIPS) has been active in safeguarding the public interest on privacy and other societal values for many years. Its current activities related to certification and professional practices embody the notion of privacy. As far back as 1988, the Society approved an operational guideline on *The Protection of Privacy in Information Systems* to assist members in complying with its amended Code of Ethics.[1] (These guidelines have been updated to reflect the Society's current understanding of privacy.[2]) In this way, CIPS linked a moral and ethical issue to its own self-regulating processes.

In this paper I intend to present a primer on privacy and technology issues to improve the understanding of the information systems professional and the human rights advocate. Generally, I will discuss the definition of privacy and the public's expectations thereof, threats and challenges to individual privacy on the information highway, business attitudes toward privacy, and some of the ways to mitigate the threats.

---

*John G. Boufford, I.S.P. is the Information and Privacy Coordinator for the Ontario Ministry of Natural Resources (OMNR), and the Coordinator for the Canadian Information Processing Society's (CIPS) Privacy and Information Technology Initiative. At the OMNR, he is responsible for the implementation of the *Freedom on Information and Protection of Privacy Act*. He holds an Information Systems Professional (I.S.P.) diploma from CIPS and periodically represents them on matters dealing with privacy and information technology. He is also the principle contributor to the Society's *Implementation and Operational Guidelines on Privacy and Information Technology*. The presentation upon which this paper is based was given at the Human Rights and Information Technology Conference in Fredericton, New Brunswick on April 28, 1997. The focus of this panel discussion was to discuss privacy as a human right and the competing interests of freedom of the press and law enforcement. This paper is a general overview of privacy as it relates to the information highway. The views expressed in this paper are those of the author and are not necessarily shared by his employer.

[1]Canadian Information Processing Society, *The Protection of Privacy in Information Systems: Operational Guidelines* (Toronto: Canadian Information Processing Society, 1988).

[2]Canadian Information Processing Society, *Implementation and Operational Guidelines on Privacy and Information Technology* (Toronto: Canadian Information Processing Society, 1997) This paper can be viewed on-line at http://www.cips.ca/papers/privacy/default.htm.

The subject of privacy in itself is problematic because we, as Canadians, do not share a common understanding of what constitutes privacy. Quoting from *Privacy Revealed: The Canadian Privacy Survey*, the 1992 definitive study on Canadian privacy attitudes:

> Although people clearly have a shared understanding about the general boundaries around privacy, there is considerable variety in the way different people use and understand the term and these usages often differ further from the way experts and decision-makers speak of privacy issues.[3]

Let me now discuss what privacy is. There are several commonly accepted definitions of privacy which are pertinent to this discussion. The notion of privacy was first postulated in a Harvard Law Review article by Louis D. Brandeis, later to become a Justice of the Supreme Court of the United States, and Samuel D. Warren, of the Harvard Law School, in 1890.[4] They described privacy as "the right to be let alone"[5] when they were offended by press coverage of their families, and by "recent inventions and business methods".[6] It took almost 20 years before the American courts issued judgments which adopted that principle. To some, this definition means being free of junk mail or unsolicited e-mail messages. Since these intrusions are more of a nuisance than a threat, I have generally considered the threat to informational privacy to be more pressing.

I recently gained new insights into how this definition might apply to the Internet. I read of a Moldavian website which advertised free access to sexually oriented images if customers downloaded its software. However, unbeknownst to the victim, the free program dialled a toll call, charging the customer $2 per minute. The program would not disconnect the toll call until the user shut down his or her computer.[7]

From an information technology perspective, a much better definition of privacy has been that of Alan Westin, where he described privacy as:

---

[3]F. Graves, N. Porteous & P. Beauchamp, *Privacy Revealed: The Canadian Privacy Survey* (Ottawa: Ekos Research Associates, 1993) at 40.

[4]L. D. Brandeis & S. D. Warren, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193.

[5]*Ibid.*

[6]*Ibid*, at 195.

[7]R. E. Smith, "In the Courts" (1997) 23:6 Privacy Journal 7.

> the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[8]

This definition embodies the concept of "fair information practices" which forms the basis for many of the regulatory and voluntary data protection schemes.

Throughout my involvement as a privacy advocate, I have noticed that the privacy expectations of the public are seldom consistent with either their legislated protections or with the recommendations in the voluntary codes. First, notwithstanding the explicit inclusion of groups and institutions in the Westin definition, most data protection schemes only apply to the protection of information about natural persons acting on behalf of themselves. The protection is not extended to businesses or other organizations, nor is it usually extended to an individual operating in some official capacity. To do so might circumvent the spirit and intent of freedom of information legislation.

The second inconsistent area involves the data items which are afforded protection. For example, legislation does not normally consider information about property to be personal information, while the owners and occupants of those properties certainly consider information in those same "property records" to be closely linked to their personal lifestyle. These records reveal such items as information about their property tax assessments or lifestyle choices.

In discussing the expectation of privacy, one cannot ignore the significant concern of the public about the information which businesses collect about their customers. In the above survey of Canadian privacy attitudes, this concern ranked higher than the concern about government-held information.[9] For example, businesses collectively gather fairly detailed information about their customers lifestyle including purchasing patterns, family income and other demographic information. This information is often sold, in one form or another, to market research firms. Yet individuals seem to freely provide this detailed information in return for small, or non-existent, price reductions at the check-out.

This collection and use of personal information by business is legal by current standards. North America has traditionally taken a fairly libertarian view towards regulation of business. No one would argue that individuals should not be able to decide for themselves what information they will share with others. The issue,

---

[8]A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7, as cited by A. Cavoukian, then Assistant Commissioner - Privacy, Information and Privacy Commission/Ontario, in her speech "Preserving Privacy on the Information Highway: Fact or Fiction?".(Speech to special symposium on "Free Speech and Privacy in the Information Age" at the University of Waterloo, held 26 November 1994.) Dr. Cavoukian's paper can be viewed on-line at gopher://insight.mcmaster.ca/00/org/efc/doc/sfsp/cavoukian.txt.

[9]Graves *et al.*, *supra* note 3 at 22.

therefore, is not whether these activities should be permitted, but rather the business methods and practices employed to collect and use the information.

Privacy expectations on the Internet are divided. Some individuals claim to have nothing to hide and therefore use the Internet without concern to their privacy. Others are concerned about transmitting personal, financial, or confidential information over the Internet and choose not to take the risk. But is that option practical? The velocity of the decision-making process has increased to the point where companies and individuals must communicate many decisions and other information using electronic mail.

However, having recognized the risks, very few companies and individuals have taken reasonable steps to mitigate their exposure. For example, the use of encryption software is not commonplace with the possible exception of certain Internet-based financial transactions. Generally unprotected are business communications related to job applications, grievances, and private e-mail between individuals.

Is the onus, then, on individuals to protect themselves? That position would certainly absolve the information technology professional from any real responsibility to find a solution. Individuals do have to take some responsibility for mitigating their risk. Generally, however, the public is not in a position where they can effectively protect their privacy on the information highway because the playing field is not level. In some cases there is no relationship between the data subject and the business wanting to use the personal information. As a result, the individual has little bargaining power.

The federal government was very quick to make it illegal to intercept and disclose cellular telephone calls when the conversations of prominent Quebec bureaucrats were divulged. Is not unauthorized interception of e-mail and data communications over the Internet like the interception of cellular calls over the air waves? So, on balance, we require both business standards and legislation.

What are some of the privacy threats on the information highway? Government databases seem to be finding their way online. One case, which was investigated and reported by the Privacy Commissioner of Canada, involved Revenue Canada's automated Tax Information Phone Service. Using only an individual's social insurance number to access the system, the caller could confirm that the individual receives GST refunds and when it would be mailed, the individual's RRSP deduction limit, and the amount of income tax refund owing. No additional steps were taken to verify that the caller was the data subject. It is evident to all that our social insurance numbers are not confidential. Our employers and banks have them, as do a number of other agencies.

Therefore, the Privacy Commissioner found that a social insurance number was insufficient protection for this information.[10]

This example is particularly interesting from an information systems perspective. The government believed, with some justification, that the implementation of a personal identification number would be unduly expensive. Nevertheless, the Commissioner and Revenue Canada agreed that requiring the caller to provide their "total income" from line 150 of the previous year's tax return would provide the necessary security since other callers would be unlikely to have this detail and it would be hard to guess or steal. The underlying message is that if privacy is made a requirement early in the development process, problems such as this can be avoided with moderately inexpensive techniques.

Other privacy threats on the information highway are theft of identity and credit card fraud. These are significant problems which can cause major disruption in the lives of the victims. It appears that these problems are exacerbated by ineffective systems design which allows the perpetrator to easily change the victim's address, permitting the fraud to go unnoticed, or by techniques which allow the credit grantor to update the victim's credit history in a manner which causes a corrected credit history to be over-written by inaccurate information.

From these examples, we can determine that it really does not matter whether the personal information on the information highway is in the custody of a government agency or a private company. In either case, the threats are real and the data subject's privacy should be protected. And governments seem to be recognizing that fact. Quebec has enacted privacy legislation which applies to the private sector[11], and British Columbia's act[12] applies to certain self-regulating professions. Finally, Justice Minister Rock[13] announced his government's intention to introduce privacy legislation which will apply to the private sector. Clearly, privacy is on the agenda and the pendulum is swinging in favour of increased protection of personal information.

It also appears that, contrary to popular belief, the attitude of Canadian business toward privacy codes may not be negative. An employee of a Canadian industry association stated that privacy is the most important issue facing that industry sector over the next 12 months. That industry would prefer a consistent privacy regime which

---

[10]Privacy Commissioner of Canada, *Securing the Tax Phone Line, Annual Report Privacy Commissioner* (Ottawa: Canada Communications Group, 1994-95) at 46.

[11]*An act respecting the protection of personal information in the private sector*, S.Q. 1993, c. 17.

[12]*Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165.

[13]The Hon. A. Rock, Minister of Justice and Attorney General of Canada, Address (Eighteenth International Conference on Privacy and Data Protection, Ottawa, 18 September 1996) [unpublished]. This address may be viewed on-line at http://infoweb.magi.com/~privcan/conf96/se_rock.html.

is internationally accepted and enforceable. Its view is that this is preferable to dealing with a hodgepodge of privacy legislation in different countries, states, and provinces.

Echoing that sentiment, a business person from a technology company argued that a national certification or conformance assessment (CA) process for products which meet privacy standards is impractical. Clearly, companies operating on a global marketplace need to be certified in one nation, and to have that certification recognized in other countries which have adopted a similar standard. It is impractical to have a product tested and certified in each country because it is unduly expensive and it increases the time for a product to reach the marketplace. It also appears that in some countries, the CA process is abused as a method of delaying product introduction while their domestic industries develop a competing product.

Discussions are now occurring between privacy advocates and industry representatives about the effectiveness of a "self-declaration of conformance". If effective, this form of conformance assessment is particularly suited to the information technology sector because of the continual nature of product development.

The question may be what does an efficient conformance assessment regime have to do with the legitimate privacy concerns of the consumer? The response, of course, is that the Canadian marketplace is too small for a company to develop products for the information highway, unless those products can be exported to other countries. As a result, we may see fewer domestic products which conform to privacy standards that Canadians believe to be important.

To the privacy advocate, a data protection scheme must be considered only a first step in privacy protection on the information highway. To create an environment where privacy-friendly information technology products become the norm, we must facilitate the development of bi-lateral and multi-national agreements where a tested and certified product from one country will be recognized in another country without recertification.

What can human rights advocates and information systems professionals do to alleviate these issues? First, and foremost, more discussion is required on the issue. This need not be formal. Form a professional relationship with a privacy advocate if you are a systems professional, and visa versa. The more these issues are discussed, the easier it will be to develop creative and inexpensive solutions to some of the privacy intrusions.

Second, do not believe everything you read about how technology violates individual privacy. Generally, technology is inherently neutral with respect to privacy. However, those without an understanding of privacy have implemented information technology in a manner which threatens privacy. There also appears to be a good deal of sincere, but misguided information in circulation. Check the validity of information with someone who understands the technology.

Third, systems designers and developers should prepare a privacy impact assessment for any system which maintains personal information about staff, customers or stakeholders. These analyses will reveal problems while they are still able to be fixed at a reasonable cost. In some complex cases, it may be advisable to hire a privacy consultant to prepare the privacy impact analysis.

Finally, become familiar with privacy-enhancing technologies. Examples of these include data and biometric encryption products, and anonymous payment schemes. However, exercise caution in this area. Misuse of a privacy enhancing technology (such as electronic fingerprinting) can be intrusive.

Privacy is a human right. There is no shortage of examples where the application of technology has resulted in an erosion of privacy. But a partnership between human rights and information technology professionals can begin to address some of the challenges posed by the application of information technology.