ACCESS TO INFORMATION AND CONFIDENTIALITY OF PERSONAL INFORMATION ON INTERNET

Internet is a worldwide computer network made up of a collection of national, regional and private sub-networks linked by a common communication protocol.

Navigation on Internet is generally carried out in the privacy of home or from the workplace, creating an illusion of anonymity.

NAVIGATION ON INTERNET LEAVES TRAILS

Web sites generally recognize the addresses of network providers and the type of software enabling a user to surf the network. They can also determine whether they were previously visited by a user and when this visit was paid. They can even retrieve some of the information provided during the preceding visit. In theory, this is not sufficient to identify the visitor. However, if identifying information is transmitted to a site (subscription, purchase, transaction, participation in a draw), the trails left can be paired. Likewise, the transmission of an e-mail address made up of a genuine family name and first name makes it possible to identify an individual, even among homonyms.

We should always be aware that visiting a Web site leaves a trail and that some data remain stored in memory. Even when the transmission is secure, an ill-intentioned individual can obtain confidential information if the site is insufficiently protected. As a result, it is recommended not to disclose any personal information on Internet. Those who ignore this advice would do well to deal only with well-established organizations that enforce security measures. These organizations should clearly inform citizens of their rights and their responsibilities in case of a breach of confidentiality.

THE LAW

Internet knows no borders. In Québec, rights of access to information and privacy are entrenched in the *Charter of human rights and freedoms*. These rights are governed mainly by the *Québec Civil Code* and two laws: the *Act respecting Access to documents held by public bodies and the Protection of personal information* and the *Act respecting the protection of personal information in the private sector*. The basic principles laid in these laws are broad enough to adapt to technological change. However, when dealing with organizations outside our territory, which as a rule are not subject to our laws, enforcement problems arise.

ACCESS TO INFORMATION.

The Act respecting access provides that every person is entitled to access documents held by public bodies. Internet may represent, for public institutions, a way of communicating with citizens. In the matter of access to government information, the Commission observes the following broad principles:

- **Internet can be used as a means to convey information of public interest. It is essential for public institutions using electronic networks to guarantee access to all information and services deemed of public interest.**
- **In the interest of citizens who choose not to use electronic services, conventional means of access to information and services must be maintained.**
- **Subscription to services offered on Internet must be free and voluntary.** For example, persons subscribing to an Internet service should not have their names entered on a mailing list without their consent. They have to be provided an opportunity to give their consent.

THE PROTECTION OF PERSONAL INFORMATION

A huge mass of personal information can circulate between users and network providers. The law states that information identifying individuals is confidential. Public and private organizations must therefore protect such information. To this end, the Commission believes the following principles must apply:

- **Public and private institutions planning to offer services on Internet must first assess the possible repercussions of this new technology on the protection of the citizens' personal information.**
- **The collection, storage, use, release and destruction of personal information must abide by the law.**

For example, a private enterprise building up a file on a customer should only collect such personal information as is necessary for the purpose of the transaction. In addition to informing customers of their right to access their files and correct the information they contain, the company must advise them of the purpose and use of their files, the status of persons authorized to consult them, and where they are held. Before collecting information from a third party on its customers, the company must seek their consent. Clicking "OK" on a computer does not constitute necessarily a valid assent. The company is also responsible for the security of the information from the time it is collected through its storage.

Likewise, a private company holding, using or communicating personal information must ensure its **confidentialit**y. It must check its accuracy and update it before using it. It must also secure the customer's consent before releasing the information or using it for purposes other than those envisaged at the time it was.collected.

Rights of access and correction must be respected, as the law stipulates. Administrators of networks and service providers, whether in the public or private sector, must give citizens free access to their personal information. They may require payment, however, for the transcription, reproduction or transmission of the information requested.

When requested in writing by the person concerned, public and private organizations must rectify any inaccurate, incomplete or ambiguous information and, if need be,

transmit these corrections to those who have received the erroneous information. A denial of access or correction must be accompanied by a written notice informing petitioners' of their right to appeal to the Commission. Out-of-date information must be destroyed, in accordance with the Commission's requirement on the destruction of documents containing personal information.

- **Adequate security measures must be taken to ensure the protection of personal information.**

All Internet users are bound by the legal obligation to protect personal information. Web site administrators must devise their own security measures. They should adopt a "code of conduct" specifying their duties and obligations. Public and private sector employees should use a code and a password to access databases containing personal information, limit their access to administrative needs, sign a confidentiality protocol, and record in a daily journal every instance of access.