[*Texte*]

There are things that can be done fairly quickly, like the audible beep that DOC and the industry are looking at, the introduction of a beep signal so that if you're not on a cellular phone but you're talking to someone on a cellular phone the beep lets you know, hey, I'm talking to this person on a cellular phone; I'd better watch it.

I guess it's hard for officials to know. There's a panoply of privacy principles that are in play here. Today we're looking primarily at legislation, but we could also give you a thorough briefing on the whole privacy principles, if that would be of help to you.

Mr. Horner: Is the technology available to make it totally private?

Mr. Breau: It depends, of course, at what cost. For example, the military—

Mr. Horner: What do you mean, cost?

Mr. Breau: Well, I was going to say that the military, for example, are very concerned about interception—

Mr. Horner: Of course.

Mr. Breau: —and they use very sophisticated means of making it so-called private. It depends on the level of technical sophistication, which usually is associated with the higher cost one wishes to go to in order to protect the communication. If it's national security, governments take great measures to encrypt signals so that they're not intercepted by foreign governments, etc. For consumers there's another level of encryption that will go a long way to protecting a signal. There are many technical ways of doing it. Usually the more sophisticated they are, the more they cost.

It's much like a house. You could put a single lock on your front door, or you can put six locks on it. You can do various things. You can get alarm systems. There are many technical options, but they come at a cost.

The Chairman: Has anybody costed out the figures on total encryption, total security? I have a concern here. I have to assume that every phone call that is made, the person who calls and the person who receives the call assume that is private. There's a basic fundamental assumption here on the part of the public that it's a private communication, unless otherwise so designated. Yet I don't see that assumption in this bill. I don't see anything technical or legal here that assumes that is a basic assumption and right of the individual. We are just finding out here that we have options.

Mr. Breau: Just to return to the privacy principles again, privacy is a right. The other principle which is important states, "When services are introduced which erode personal privacy, privacy should be restored at no charge". That would argue that, as we introduce a new service, the privacy has to be there at no additional cost.

The Chairman: But did you not just say that for total encryption, for total security, you're going to have to pay a heck of a lot for it.

[*Traduction*]

Il y a certaines choses que l'on peut faire assez rapidement, par exemple l'introduction d'un signal sonore qui vous avertirait que vous parlez à quelqu'un qui utilise un téléphone cellulaire, en utilisant vous-même un téléphone ordinaire. Ce signal sonore constituerait pour vous un avertissement.

Il est difficile pour le moment de savoir tout ce qui serait nécessaire, car il y a beaucoup de principes en jeu concernant la protection de la vie privée. Pour le moment, nous discutons essentiellement de mesures législatives mais, si vous le désirez, nous pourrions organiser une séance d'information sur tous les principes relatifs à la protection de la vie privée.

M. Horner: Existe-t-il déjà une technologie permettant de rendre ces conversations totalement privées?

M. Breau: Cela dépend du prix que l'on est disposé à payer. Dans l'armée, par exemple. . .

M. Horner: Que voulez-vous dire?

M. Breau: J'allais vous dire que l'armée, qui tient beaucoup à ce que ses communications ne soient pas interceptées. . .

M. Horner: Bien sûr!

M. Breau: . . .on utilise des méthodes très sophistiquées pour se protéger contre ce risque; mais cela coûte très cher. Au fond, plus on veut protéger le secret des communications, plus cela coûte cher. Quand il s'agit de questions de sécurité nationale, les gouvernements sont prêts à aller aussi loin qu'il le faudra pour garantir que leurs signaux ne puissent pas être interceptés, par exemple par un gouvernement étranger. Pour ce qui est des particuliers, on peut protéger les signaux en ayant recours à des systèmes de cryptage qui ne sont pas nécessairement aussi sophistiqués. Il y a beaucoup de solutions techniques à ce problème et le coût dépend du degré de protection que l'on veut obtenir.

C'est un peu comme vouloir protéger sa maison. Vous pouvez installer une seule serrure sur votre porte d'entrée, ou vous pouvez en installer six. Si vous le voulez, vous pouvez aussi installer un système d'alarme. Il y a donc bon nombre d'options techniques, à des prix très variables.

Le président: A-t-on calculé le coût d'un système de sécurité totale? À mon avis, quand deux personnes ont une conversation téléphonique, les deux supposent que leur conversation est privée. Cela me semble assez fondamental. Or, je ne retrouve pas cette hypothèse dans le projet de loi. Je ne vois ici aucune disposition technique ou juridique correspondant à cette hypothèse fondamentale, qui représente un droit des particuliers. En fait, nous découvrons qu'il y a des options.

M. Breau: Pour en revenir aux principes de protection de la vie privée, il est vrai que cette vie privée constitue un droit. Autre principe important, je l'ai exprimé tout-à-l'heure, «quand on introduit des services qui portent atteinte à la vie privée, celle-ci doit être rétablie sans frais pour l'usager». Autrement dit, si nous introduisons un nouveau service, nous devons garantir que la vie privée des usagers sera protégée sans que cela leur coûte plus cher.

Le président: Mais vous venez de dire que la sécurité totale coûterait très cher.