Ann Cavoukian, Ph.D.
Commissaire à l'information et à la protection de la vie privée/Ontario

Feuille-info

Numéro 14
Août 2007

# Technologies de communication sans fil : Protection de la vie privée et sécurité

On peut s'attendre à ce que très bientôt, tous les appareils qui servent à générer ou à sauvegarder des données comportent des fonctions intégrées de transmission sans fil ou puissent être reliés à des réseaux sans fil. Ainsi, les téléphones cellulaires et les assistants numériques sont de plus en plus perfectionnés, et sont souvent dotés de plusieurs technologies sans fil.

Ces technologies permettent de réaliser des économies, de gagner en efficacité et de faciliter l'accès à des renseignements importants. Dans le secteur de la santé, par exemple, la transmission de données sans fil permet désormais aux ambulanciers paramédicaux d'envoyer des images et des données cardiaques directement aux cardiologues, réduisant considérablement le temps d'attente pour obtenir un traitement.

De toute évidence, les avantages des communications sans fil sont nombreux. Cependant, ces technologies comportent également des risques. Faute de précautions, la transmission de données sans fil revient à placer un classeur ouvert dans une salle d'attente. Le CIPVP a d'ailleurs rendu récemment une ordonnance à la suite d'un incident où des personnes non autorisées avaient intercepté des images transmises sans fil de patients prélevant des échantillons d'urine aux toilettes.

La présente feuille-info aborde les questions relatives à la protection de la vie privée qui sont associées à l'utilisation de technologies sans fil, et complète la feuille-info n° 13, *Technologies de communication sans fil : Les systèmes de surveillance vidéo*.

## Précautions

La *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*), la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) et la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (*LAIMPVP*) énoncent des exigences en matière de protection des renseignements personnels, y compris les renseignements qui existent sous forme électronique.

En règle générale, afin de se conformer à ces *Lois*, les personnes responsables doivent prendre des mesures raisonnables pour protéger les renseignements personnels, notamment des mesures de protection matérielle, une gestion des renseignements personnels fondée sur le rôle ou des mesures technologiques comme le chiffrement.

La transmission de renseignements personnels sous forme électronique, particulièrement grâce aux technologies sans fil, crée deux nouvelles catégories de données à protéger, les « données en mouvement » et les « données statiques », ce qui complique l'observation des Lois.

Pour comprendre l'incidence des changements et progrès technologiques, il est bon de revoir régulièrement ses idées reçues et ses décisions. Il est alors possible de prendre des précautions raisonnables du genre qu'adopterait toute institution ou personne soucieuse de la protection de la vie privée. Par exemple, il fut un temps où il était raisonnable de naviguer dans Internet et de télécharger des fichiers sans coupe-feu personnel ni logiciel antivirus. Ce n'est plus le cas aujourd'hui.

Les personnes chargées de l'acquisition, de l'implantation ou de l'utilisation d'appareils électroniques qui permettent l'accès à des renseignements personnels ou qui en contiennent doivent prendre des mesures préventives pour protéger ces renseignements. Ces mesures pourraient nécessiter des connaissances techniques spécialisées; les personnes qui ne les possèdent pas devraient faire appel à des experts.

## Les technologies de communication sans fil

Les appareils sans fil partagent un certain nombre de caractéristiques, la plus importante étant qu'ils diffusent des données par ondes radio [1]. Ces ondes peuvent être encodées différemment (certaines sont analogiques, d'autres numériques), mais elles sont toutes diffusées dans toutes les directions à partir de leur point d'origine.

Cela signifie que tout récepteur qui est à la portée de l'émetteur et est réglé à la même fréquence pourra recevoir le signal. Les administrateurs de systèmes sont incapables de déterminer qui a accès au signal, de sorte que des données peuvent fort bien être divulguées par inadvertance à des personnes non autorisées.

Les signaux contenant des renseignements personnels qui sont acheminés au moyen d'une technologie sans fil doivent être strictement protégés contre l'accès non autorisé.

Parfois, la seule existence d'un signal peut divulguer des renseignements personnels. C'est le cas, par exemple, des téléphones cellulaires ou d'autres appareils mobiles, qui peuvent révéler l'emplacement et les allées et venues des personnes qui les utilisent.

## Les technologies Wi-Fi

Les technologies Wi-Fi (*Wireless Fidelity*) permettent le réseautage sans fil (voir le tableau 1 ci-dessous).

Permettant de relier des ordinateurs sans fil, elles sont peu coûteuses, de sorte que nombre de personnes, qui sont dans bien des cas des profanes en réseautage, se servent désormais de matériel Wi-Fi. Par exemple, les routeurs sans fil sont de plus en plus courants dans les réseaux domestiques ou les petits réseaux d'entreprise.

Cependant, si les données ne sont pas chiffrées, ou si une forme de chiffrement dépassée et inadéquate est utilisée (p. ex., le système WEP), les renseignements personnels transmis par l'entremise de ces réseaux sans fil peuvent être interceptés. On soupçonne que des voleurs ont accédé à un réseau sans fil chiffré au moyen du système WEP pour s'emparer de données sur les cartes de crédit et de débit de plus de 45 millions de clients du détaillant T.J. Maxx.

Il y a lieu d'utiliser des techniques de chiffrement récentes pour réduire le risque d'interception. Les grandes organisations peuvent recourir à des réseaux privés virtuels (RPV) pour leurs travailleurs à distance, alors que le système d'accès protégé Wi-Fi (WPA ou WPA2)[2] conviendrait aux particuliers et aux petites organisations.

Il ne faut pas oublier que tout appareil sans fil relié à un réseau peut servir de point d'accès non autorisé à l'ensemble du réseau à moins d'être correctement réglé. Les atteintes à la sécurité des systèmes informatiques peuvent entraîner la divulgation de bases de données complètes contenant des renseignements personnels. Pour éviter les fuites de données aux points d'accès sans fil, il est essentiel de sécuriser tout le réseau, et non seulement certains appareils qui y sont reliés.

---

[1] À proprement parler, les appareils à infrarouges sont également sans fil, mais comme ils sont utilisés de moins en moins, nous ne les abordons pas dans le présent document.

[2] Les systèmes WPA and WPA2 étaient généralement considérés comme sécuritaires au moment de la rédaction de la présente feuille-info. Cependant, comme les normes changent continuellement, il est bon de le confirmer auprès de son fournisseur de services.

## Bluetooth

La technologie Bluetooth permet à des appareils électroniques de communiquer entre eux au moyen de signaux sans fil de courte portée. Elle s'utilise pour relier, par exemple, un téléphone cellulaire à un écouteur, un clavier à une souris ou un ordinateur portable à une imprimante par un processus de « jumelage ».

Il existe des fonctions de sécurité mais certains systèmes Bluetooth ne sont pas totalement sécurisés. On a relevé des cas précis d'accès non autorisé : vol de données, intrusions et détournement[3], le plus grave étant le vol de données contenues dans un appareil Bluetooth vulnérable.

Cette vulnérabilité varie selon l'appareil en question, et les fabricants tentent actuellement de résoudre ces problèmes de sécurité. Entre-temps, assurez-vous que tous vos appareils Bluetooth sont sécurisés et que tous les renseignements personnels transmis sont anonymisés.

N'activez pas les fonctions Bluetooth sur les appareils qui contiennent des renseignements personnels ou qui y ont accès avant de confirmer que la liaison est sécurisée et protégée.

## Puces émettrices

La technologie sans fil peut être intégrée dans une puce électronique ou y être greffée. C'est le cas des étiquettes d'identification par radiofréquence[4].

Ces étiquettes ont de nombreuses applications. Dans le secteur de la santé, par exemple, des systèmes les utilisent pour jumeler les patients et les ordonnances qui leur sont fournies, ce qui permet d'éviter les erreurs de médicaments ou de dose.

Parmi les autres technologies semblables, mentionnons les cartes à puce intelligente sans contact, qui servent notamment de cartes de crédit et de débit, et les appareils de communication en champ proche, comme des téléphones cellulaires qui permettent de faire des micro-paiements à des distributeurs automatiques. Le recours de plus en plus fréquent à des appareils qui émettent des renseignements financiers peut, si l'on ne se soucie pas suffisamment de la sécurité, exposer les utilisateurs au vol d'identité et à d'autres formes d'atteinte à la vie privée.

Lorsque vous vous servez d'appareils à circuits intégrés pour recueillir ou utiliser des renseignements personnels, assurez-vous de chiffrer ces renseignements ou d'utiliser des mesures de sécurité d'une efficacité équivalente. Les systèmes d'information auxquels ces appareils sont reliés devraient assurer une protection de bout en bout des renseignements personnels.

## Les téléphones cellulaires et les assistants numériques

Les téléphones cellulaires et les assistants numériques sont en convergence rapide, et peuvent être considérés comme des appareils semblables. Ils sont utilisés non seulement pour les communications vocales mais aussi comme modems sans fil ou navigateurs Web. Lorsqu'ils servent à transmettre ou à stocker des courriels ou des messages instantanés, ils peuvent comporter des risques.

Réglez vos téléphones cellulaires et assistants numériques afin qu'ils fonctionnent de manière sécurisée. Parmi les caractéristiques de sécurité dont ils peuvent être dotés, mentionnons le chiffrement des transmissions, les mots de passe et la suppression automatique des données.

---

[3] Voir notamment Carettoni et coll., * Studying Bluetooth Malware Propagation: The BlueBag Project +, IEEE Security & Privacy, mars-avril 2007, vol. 5, no 2, p. 17-25.

[4] Voir Lignes directrices régissant la protection de la vie privée pour les systèmes d=identification par radiofréquence à http://www.ipc.on.ca/images/Resources/up-rfid_guide_f_web.pdf.

Il importe aussi de ne pas se servir de ces appareils pour discuter de questions personnelles ou commerciales délicates dans des endroits publics.

Lorsque vous vous servez des fonctions de transmission ou de stockage de données des téléphones cellulaires, assistants numériques et appareils semblables, ne vous laissez pas influencer par leur petite taille et traitez les données avec autant de soin que celles qui se trouvent dans votre ordinateur de bureau ou votre ordinateur portable.

## Conclusion

Les technologies de communication sans fil sont désormais bien établies. Les appareils sans fil deviendront de plus en plus variés et leur nombre se multipliera. Leur utilisation comporte des économies et des gains d'efficacité indéniables; cependant, il ne sera possible de profiter de ces avantages qu'en créant une culture de la vie privée. À mesure que ces technologies sans fil seront intégrées dans les systèmes d'information et les procédés des entreprises, une quantité considérable de renseignements personnels sera nécessairement acheminée par ondes radio. Celles-ci pouvant être reçues par toute personne qui se trouve à leur portée, il est impossible d'empêcher des personnes non autorisées d'y avoir accès. Par conséquent, les responsables des renseignements personnels doivent veiller à ce que les « données en mouvement » fassent l'objet d'un chiffrement fort en tout temps.

## Tableau 1 - Catégories de réseaux sans fil[5]

| | Réseau personnel | Réseau local | Réseau métropolitain | Réseau étendu |
|---|---|---|---|---|
| Technologie | Bluetooth<br>Ultralarge bande | 802.1b<br>802.1a<br>802.1g<br>(Wi-Fi) | 802.16<br>802.16a<br>802.16e<br>(WiMAX) | GSM<br>GPRS<br>CDMA<br>2.5G<br>3.5G |
| Débit | Moyen<br>1 à 2 Mbits/s | Élevé<br>11 à 54 Mbits/s | Très élevé<br>Qualité de service jusqu'à 268 Mbits/s | Faible à moyen<br>10 kbits/s à 2,4 Mbits/s |
| Portée | Très courte<br>3 m (~10 pi) | Courte<br>100 m (~300 pi) | Moyenne<br>50 km (~31 milles) | Longue<br>(mondiale) |
| Connectabilité | Entre ordinateurs portables, ordinateurs de bureau et périphériques; entre appareils et systèmes | Entre ordinateurs; entre ordinateurs et Internet | Entre réseaux locaux ou ordinateurs et Internet à haute vitesse câblé | Entre téléphones intelligents ou assistants numériques et réseaux étendus ou Internet |

[5] Adapté de Dekleva, Sasha et coll., * Evolution and Emerging Issues in Mobile Wireless Networks +, Communications of the ACM, juin 2007, vol. 50, no 6, p. 41.

Feuille-info

est publié par **le Bureau du commissaire à l'information et à la protection de la vie privée.**

Pour nous faire part de vos observations, nous informer d'un changement d'adresse ou pour que votre nom soit ajouté à la liste d'envoi, veuillez communiquer avec :

**Service des communications**
*Commissaire à l'information et à la protection de la vie privée/Ontario*
2 rue Bloor Est, Bureau 1400
Toronto (Ontario) M4W 1A8
Téléphone : 416-326-3333 • 1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca
***This publication is also available in English.***

papier recyclé à 30%

ISSN 1188-3006