Conseils pratiques

Comment gérer les témoins

Le Web connaît une croissance phénoménale. Les internautes peuvent accéder de plus en plus facilement à l'information, mais en retour, les sites Web peuvent recueillir beaucoup de renseignements sur eux. Il est difficile de protéger sa vie privée lorsque des renseignements personnels sont utilisés ou divulgués à son insu ou sans son consentement. Souvent, le consommateur diffuse de tels renseignements sans le savoir par l'entremise d'un outil logiciel de collecte d'information appelé « témoin » (*cookie*).

De nombreux sites Web créent des témoins, qui sont de petits fichiers texte enregistrés sur le disque rigide de votre ordinateur lors de votre première visite. Une fois en place, le témoin demeure inactif jusqu'à ce que vous reveniez au site Web d'origine. À ce moment-là, le contenu du témoin est transmis de votre ordinateur au serveur de la page Web; ainsi, le site peut vous identifier et savoir que vous l'avez déjà visité.

Les témoins ne sont qu'un exemple des empreintes que vous pouvez laisser, mais presque tous vos déplacements sur le Web laissent des traces électroniques qui procèdent de différents facteurs : le fait que vous ayez un compte chez un fournisseur de services Internet ou un service en ligne; les liens ou graphiques sur lesquels vous cliquez (notamment les bandeaux publicitaires); l'envoi de messages à des listes de diffusion, à des forums Usenet ou à d'autres listes de discussion.

Il y a atteinte à la vie privée lorsque des renseignements sur un utilisateur sont recueillis, utilisés ou divulgués à son insu ou sans son consentement. Les témoins recueillent des données généralement inoffensives, mais le risque d'atteinte à la vie privée s'accroît lorsque ces données sont combinées à d'autres éléments d'information comme les données d'enregistrement à un service en ligne, les réponses à un sondage en ligne ou les données provenant du journal du serveur Web (nom du fournisseur Internet de l'utilisateur; type d'ordinateur et de logiciel utilisé; site Web de provenance; fichiers consultés; temps passé à chaque page).

Nous croyons que pour protéger sa vie privée en ligne, il faut d'abord s'informer. En effet, les utilisateurs avertis, qui sont au courant des risques auxquels ils s'exposent en ligne, notamment les témoins, sont très bien placés pour évaluer ces risques et déterminer les mesures à prendre pour protéger leur vie privée. À la fin du présent article, on trouvera une liste de sites Web qui proposent des renseignements détaillés sur les témoins et des questions connexes.

En sachant comment limiter la création de témoins, vous réduirez les traces que vous laissez dans Internet. Cependant, comme c'est souvent le cas en matière de vie privée, les utilisateurs devront déterminer les mesures qu'ils sont disposés à prendre pour se protéger

COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE/ONTARIO

Novembre 1998

ANN CAVOUKIAN, Ph.D.
COMMISSAIRE

lorsqu'ils veulent obtenir des services ou des renseignements d'un fournisseur au moyen de son site Web. Il est prudent toutefois de tenir pour acquis que ses renseignements personnels ne peuvent être tout à fait à l'abri sur le Web.

À quoi servent les témoins?

Les témoins ont été créés pour simplifier et personnaliser la navigation dans les sites Web. Or, on leur a apporté des changements controversés pour en faire un outil de repérage à des fins de marketing. Pour les annonceurs, les témoins représentent un véhicule de marketing personnalisé ou individualisé. Grâce aux témoins, les entreprises qui vendent des produits sur le Web peuvent analyser les habitudes d'achats de leurs clients réguliers et leur offrir des promotions spéciales.

Les témoins sont employés à des fins diverses de façon à vous attribuer (par l'entremise de votre ordinateur) des données qui seront utiles aux sites Web lors de vos visites subséquentes. Sur le Web, les témoins servent au repérage (en permettant de déterminer quand vous avez consulté un site, quelles pages vous avez consultées et combien de temps vous y êtes resté), à la mémorisation de mots de passe, de noms d'utilisateur et des préférences quant à la page d'accueil du navigateur ainsi que pour les emplettes et commandes en ligne.

Le marketing ciblé représente l'un des usages les plus répandus des témoins. Ceux-ci peuvent servir à constituer un profil de vos allées et venues et des bandeaux publicitaires sur lesquels vous cliquez. Des publicités fondées sur ces données vous sont par la suite adressées directement. À l'heure actuelle, les annonceurs ne s'intéressent pas vraiment à vous mais plutôt à ce que vous seriez intéressé à acheter. Il leur faut donc un moyen de vous identifier, comme un numéro ou un identificateur unique, c'est-à-dire un témoin, pour assurer le repérage de vos clics, déplacements et préférences et vous adresser des messages et publicités mieux ciblés.

Que contient un témoin?

Un témoin contient au moins les éléments suivants : 1) son nom (choisi par le programmeur du site Web que vous visitez); 2) sa valeur (c.-à-d. les données emmagasinées qui permettront au serveur Web de vous reconnaître et d'actionner certaines fonctions à votre prochaine visite; 3) sa date d'expiration; 4) l'adresse à laquelle il s'applique, c.-à-d. l'emplacement de la page Web où vous étiez lorsque le témoin vous a été transmis; 5) le nom de domaine auquel il s'applique (il s'agit du domaine du serveur qui a créé et transmis le témoin); 6) la nécessité éventuelle d'établir une connexion sécurisée pour utiliser le témoin (si le témoin est « sécurisé », il ne sera transmis que si l'utilisateur est relié à un serveur sécurisé).

Que peut-on faire pour gérer les témoins?

Comme toujours, il n'existe pas de solution miracle pour protéger sa vie privée en ligne, mais en général, il est préférable de donner le moins possible de renseignements, même s'il est alors plus difficile d'accéder à toutes les fonctionnalités des sites.

Il existe deux grands moyens de limiter les témoins. Ils varient légèrement selon l'ordinateur et le navigateur que vous utilisez.

1. Avertissement

Les choix qu'offrent Netscape Navigator et Microsoft Internet Explorer pour limiter les témoins varient selon la version. Netscape 3.x et Microsoft Internet Explorer 3.x peuvent avertir l'utilisateur lorsqu'un témoin lui est transmis. Si cette fonction d'avertissement est en marche, l'utilisateur peut cliquer sur *OK* pour accepter le témoin ou sur *Annuler* (*Cancel*) pour le rejeter. Pour ce faire, il faut aller dans le menu *Options*/*Préférences du réseau*/*Protocoles* (*Options*/*Network Preferences*/*Protocols*) de Netscape ou dans le menu *Options Internet*/*Options avancées* (*Internet Options*/*Advanced*) de Microsoft Internet Explorer.

Les versions 4.x de ces deux navigateurs proposent plus d'options. Par exemple, dans Netscape Navigator, la fonction d'avertissement se met en marche en allant dans le menu *Édition* (*Edit*) et en cliquant sur *Préférences* (*Preferences*) puis sur *Avancées* (*Advanced Settings*) au bas de la boîte de dialogue. On peut alors choisir parmi quatre options : « accepter tous les cookies [sic] », « accepter uniquement les cookies qui sont renvoyés au serveur d'origine », « désactiver les cookies » et « m'avertir avant d'accepter un cookie (dans la version anglaise, « accept all cookies »; « accept only cookies that get sent back to the originating server »; « disable cookies »; « warn me before accepting a cookie »).

Dans Microsoft Internet Explorer 4.x, allez dans *Affichage*/*Options Internet*/*Options avancées* (*View*/*Internet Options*/*Advanced*) où vous pouvez choisir d'accepter tous les témoins, de recevoir un avertissement avant de les accepter ou de les rejeter tous.

2. Vérification périodique du fichier de témoins

Si vous utilisez Netscape, allez dans le menu Démarrer, faites *Recherche* (*Find*) puis *Fichiers ou dossiers* (*Files Or Folders*). Tapez « cookies. txt » dans la case *Nommé* (*Named*) puis cliquez sur *Rechercher* (*Find Now*). Une fois le fichier ouvert, regardez chaque ligne. Vous verrez le nom du site Web qui vous a transmis le témoin, suivi de divers caractères incompréhensibles. Pour vous débarrasser du témoin, effacez toute la ligne. Pour supprimer tous les témoins, effacez tout le contenu du fichier cookies.txt. Ensuite, faites *Sauvegarder* (*Save*) dans le menu *Fichier* (*File*) puis *Quitter* (*Exit*) pour sortir.

Dans Microsoft Explorer, les témoins sont sauvegardés à différents endroits selon la version que vous utilisez. Par exemple, Explorer 3.x les sauvegarde dans le dossier *c:\windows\cookies*.

Il est un peu plus difficile d'effacer les témoins sauvegardés dans les ordinateurs Macintosh; il est alors préférable d'utiliser un partagiciel utilitaire. Différents logiciels sont offerts; bon nombre sont décrits au site Web *Cookie Central*.

Renseignez-vous

À notre époque où l'interaction sociale se fait de plus en plus par voie numérique, le meilleur moyen de s'adapter consiste sans doute à se tenir bien informé. Voici comment obtenir des renseignements sur la protection de votre vie privée en ligne :

- *Déclarations de confidentialité :* Certains sites Web affichent une telle déclaration ou politique, qui mentionne souvent les témoins. Par exemple, la déclaration de Microsoft est

affichée à http://www.microsoft.com/info/can-fr/privacy.htm; et celle de Netscape à http://home.netscape.com/privacy/index.html.

- Le site *Cookie Central* (en anglais), à www.cookiecentral.com, propose une foule de renseignements sur les témoins, et notamment sur les logiciels de blocage, une foire aux questions, l'usage fait des témoins et des méthodes permettant d'y faire obstacle. Il contient également des exemples de témoins.
- Le site *Junkbusters* (essentiellement en anglais, sauf une page d'explications), à www.junkbusters.com/ht/en/index.html, traite de plusieurs sujets touchant la vie privée sur le Web, notamment les témoins, les bandeaux publicitaires, le télémarketing et les polluriels (*spam*).
- Le site *Les « cookies » démystifiés*, à http://www.tactika.com/cookie/, décrit les témoins en détail, traite de divers aspects liés à la protection de la vie privée et propose des techniques de blocage.
- Le site *Links2Go* (en anglais), à www.links2go.com/topic/cookies, offre une longue liste de ressources qui traitent de divers aspects des témoins.
- Le site *Anonymizer*, dont la version française se trouve à http://www.secuser.com/anonymizer/, propose un service qui permet aux internautes de naviguer incognito dans Internet.
- Le site du *Centre for Democracy and Technology*, à snoop.cdt.org, propose une démonstration qui montre aux utilisateurs les renseignements qu'un site Web est en mesure de recueillir sur ses visiteurs.

Conseils pratiques

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, pour nous informer d'un changement d'adresse, ou pour s'abonner à notre liste de distribution éléctronique, prière de communiquer avec :

La direction 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 %