Comment Firefox peut améliorer le respect de la vie privée en ligne

Voici comment se termine cette nouvelle traduction de Jenny Boriss, qui s'occupe de l'expérience utilisateur de Firefox chez Mozilla :

« Notre objectif pour Firefox 4.0 est de conférer aux utilisateurs davantage de contrôle sur leurs données, à la fois en leur passant à proprement parler les commandes et, plus important encore, en faisant en sorte que la vie privée et l'anonymat soient respectés par défaut sans casser les fonctionnalités du Web. J'espère vraiment que le simple fait d'indiquer à quelles données les sites ont accès sera positif pour le Web, en réduisant la fausse impression de sécurité que de nombreux sites essaient de donner à leurs utilisateurs. Cela permettra aussi de susciter une prise de conscience et de contrôler comment, où et quand les données sont partagées. »

Facebook et Google peuvent-ils en dire autant ?

Halte à l'invasion des cookies ! Comment Firefox peut améliorer le respect de la vie privée en ligne

Defeating the Cookie Monster: How Firefox can Improve Online Privacy

Jenny Boriss – 2 juin 2010 – Boriss' Blog

(Traduction Framalang : Pandark, Berettonawak, Joan, Goofy et Don Rico)

À l'heure où nous déterminons les priorités pour les fonctionnalités et le développement de la prochaine version de

notre navigateur, l'équipe de Firefox a analysé l'état du Web et recherché les domaines pour lesquels le contenu disponible en ligne a évolué plus vite que les fonctions du navigateur. L'un de ces domaines préoccupants est l'usage croissant des données privées de l'utilisateur, en particulier par la publicité. La transmission muette et permanente des données de l'utilisateur entre les sites et les annonceurs publicitaires est très dérangeante pour ceux qui s'intéressent au libre choix de l'utilisateur et à la transparence sur le Web.

Vie privée vs. Sécurité

Même s'ils sont liés, la vie privée et la sécurité sont des sujets distincts. Le terme Sécurité renvoie à la prévention des dommages matériels que peut subir l'utilisateur. Éviter le vol, la fraude, la perte d'informations… relève du domaine de la sécurité. Depuis des années, les navigateurs travaillent à l'amélioration de la sécurité, motivés par des dangers toujours plus sophistiqués : virus, programmes malveillants, et autres exploitations de failles.

Le respect de la vie privée est quant à lui un sujet plus vaste. Il concerne le contrôle qu'exercent les utilisateurs sur ce qu'ils révèlent d'eux-mêmes en ligne, que ces données puissent ou non être utilisées à de mauvais desseins. Tous les usagers d'Internet dévoilent des informations sur eux-mêmes sur certains sites, mais chacun maîtrise sa confidentialité s'il sait distinguer quelles informations partager ou non, et avec qui.

Firefox assure la confidentialité locale mais doit aussi assurer la confidentialité en ligne.

L'équipe de Firefox a déjà bien fait progresser les choses dans le domaine de la confidentialité locale, avec des fonctions comme le mode de navigation privée, la suppression de l'historique récent et l'option « Oublier ce site ». Ces fonctions permettent aux utilisateurs d'exercer un meilleur

contrôle sur les circonstances où leurs données doivent être dévoilées ou bien cachées dans leur ordinateur. Cependant, des soucis de confidentialité plus sérieux apparaissent quand des données sont échangées sur un réseau.

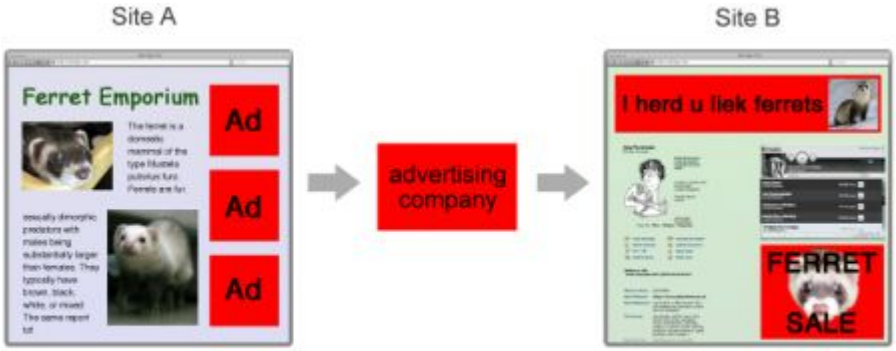
Un problème majeur que pose le Web moderne est la possibilité pour les régies publicitaires de collecter les données privées des utilisateurs avec des cookies de sites tiers.

Les sites qui proposent une interaction riche récoltent en général des informations sur l'utilisateur. Le problème survient lorsque les utilisateurs sont d'accord pour partager leurs données avec des sites auxquels ils font confiance, alors que celles-ci sont partagées à leur insu avec d'autres sites et sociétés via des cookies de sites tiers. C'est un système de financement de plus en plus courant en ligne.

C'est en novembre 1999 que les États-Unis l'ont découvert, lorsque la Federal Trade Commission *(NdT: Équivalent de la Direction de la concurrence et de la répression des fraudes)* a mené une étude sur le profilage en ligne et montré que cela présentait des risques pour la vie privée des consommateurs. Cette pratique s'est développée, malgré quelques tentatives avortées de régulation de la Federal Trade Commission américaine, de l'Interactive Advertising Bureau du Canada *(Bureau de la publicité interactive)* et de l'Office of Fair Trading *(Équiv. de la Direction de la concurrence et de la répression des fraudes)* britannique.

Tout site que vous visitez peut contenir des publicités ou d'autres composants qui envoient des cookies de votre session de navigation sur le domaine auquel vous faites confiance vers un domaine publicitaire. Ces cookies de sites tiers peuvent être utilisés pour recouper les données d'un utilisateur entre plusieurs sites et plusieurs sessions, permettant ainsi de d'établir le profil des internautes et de traquer leurs habitudes. Ces données peuvent fournir à des sociétés toutes sortes d'informations telles que ce que vous achetez, ce que

vous lisez, combien vous gagnez, si vous avez postulé pour un emploi, ou encore quels sites de rencontres vous préférez. L'une des conséquences visibles de ce partage des données est la présence de publicités ciblées en fonction d'informations et d'actions de l'utilisateur sur d'autres sites.



By placing ads on two sites, an advertising company can use third-party cookies to track a user's behavior on Site A and display ads based on that behavior on Site B

La capacité des publicitaires à obtenir et utiliser ces données constitue une infraction à la vie privée des utilisateurs, et ce pour plusieurs raisons :

- **La collecte des données est quasi impossible à détecter.** La plupart des opérations de transmission de données s'effectuent en coulisse pendant une session de navigation, sans demander son avis à l'utilisateur ni le prévenir. En général, celui-ci ne découvre ce qui s'est passé qu'au moment où il se trouve face à des publicités ciblées (bien longtemps après le transfert des données).
- **Elle s'effectue sans le consentement de l'utilisateur.** Même parmi les sites qui sont conscients que des tierces parties enregistrent des cookies depuis leur domaine, bien peu donnent aux utilisateurs le contrôle sur la façon dont leurs données sont partagées avec les régies publicitaires. Les sites qui procurent effectivement des options les formulent parfois de telle sorte qu'elles masquent leurs objectifs, comme par exemple « Souhaitez-vous que s'affichent des contenus en rapport avec votre utilisation ? » plutôt que « Voulez-vous que s'affichent des publicités en rapport avec vos données

personnelles ? ».

- **Elle va à l'encontre de ce que l'utilisateur est raisonnablement en droit d'attendre concernant le respect de sa vie privée.** Certains sites qui partagent les données de leurs utilisateurs en connaissance de cause se donnent une image trompeuse de responsabilité concernant ces données. Selon les cas, ils affichent des préférences d'utilisation impliquant un contrôle, assurant les utilisateurs que leurs données sont « sécurisées » ou proposant aux utilisateurs de lire une très longue charte de respect de la vie privée dans le but de dissimuler leurs véritables agissements. Bien sûr, le haut du tableau d'horreur est réservé aux sites qui modifient leur politique de confidentialité pour les rendre plus permissives une fois que les utilisateurs se sont déjà inscrits et ont déjà confié leurs données.

- **Il est pratiquement impossible de l'empêcher.** Même si un utilisateur est très au fait des problèmes de respect de la vie privée, lit consciencieusement toutes les politiques de confidentialité, tient à jour ses préférences relatives aux données privées et évite les sites qui ne lui garantissent pas de confidentialité, il ne sera pas forcément en sécurité. Tout site auquel il a confié ses données est susceptible de les utiliser sans le lui demander, et des cookies tiers pourraient être enregistrés sur son ordinateur par des publicités ou des bogues à l'insu des responsables du site. Bon dieu, n'importe quel site pourrait extraire des informations qui identifient un utilisateur à partir de son empreinte numérique.

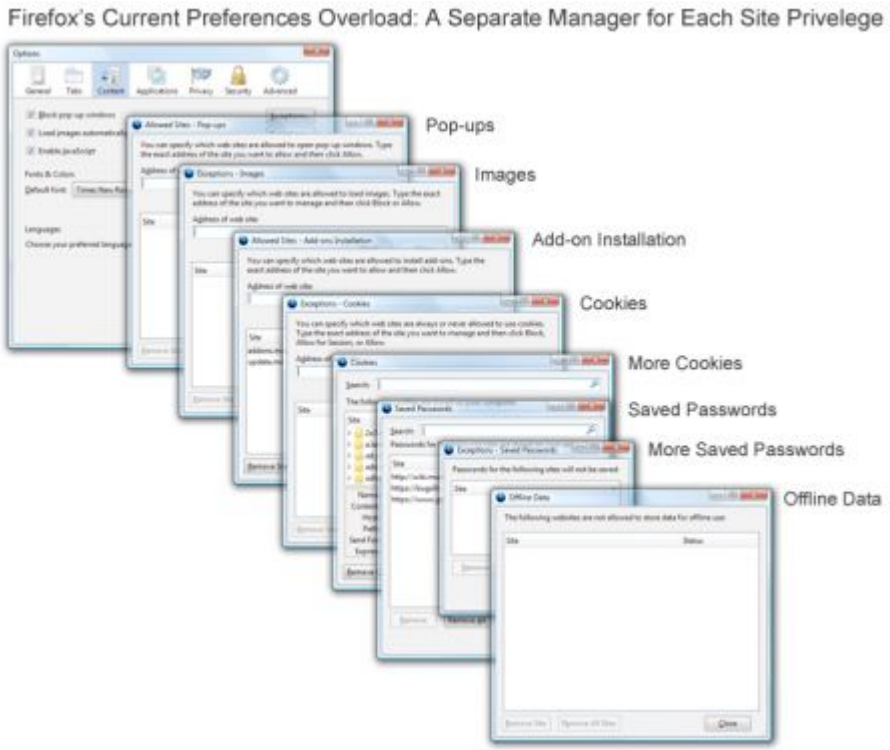
- **Elle est potentiellement embarrassante pour l'utilisateur.** La transmission des données par des cookies tiers prend les informations fournies par l'utilisateur à un instant T et les dévoile à un autre moment. Alors que l'utilisateur peut être discret

concernant les sites où il parcourt certains contenus, et même utiliser le mode de navigation privée pour que les éléments n'apparaissent pas dans l'historique, les régies publicitaires qui utilisent des cookies tiers peuvent dévoiler son comportement à des moments qui échappent à son contrôle.

Que peut faire Firefox pour améliorer la gestion des données privées ?

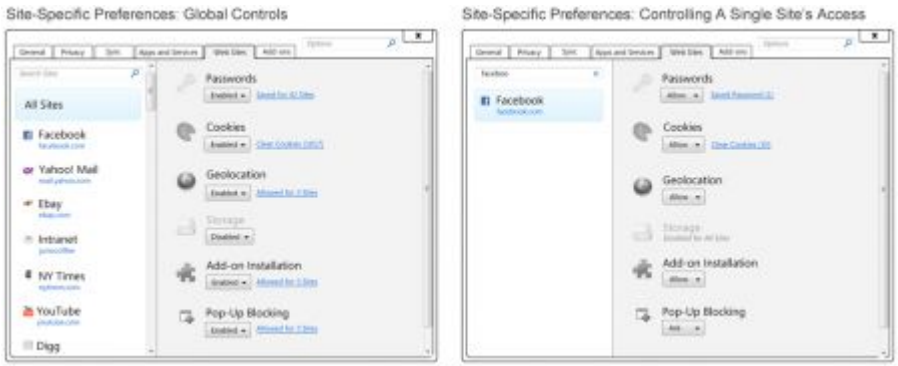
- **1. Offrir des réglages par défaut bien pensés pour les cookies de sites tiers**
  Se contenter de désactiver les cookies tiers n'est pas la solution. Les cookies tiers sont indispensables pour légitimer les fonctions Web telles que les contenus embarqués, la gestion de sessions, les sites hybrides, etc. La plupart des sites bancaires ont besoin des cookies de sites tiers pour des fonctionnalités telles que le payement de factures. Le but ne devrait pas être de désactiver directement les cookies tiers, mais de gérer plus intelligemment quels comportements sont autorisés.
  Le groupe de travail HTTP State s'applique actuellement à créer une spécification définissant la manière dont les clients doivent se comporter concernant les cookies (voir ici les documents de travail). Dan Witte, responsable du module Cookie chez Mozilla, est en liaison étroite avec le groupe et travaille de son côté à définir un standard moderne pour les cookies. Son objectif est de tracer les grandes lignes que peut suivre Mozilla en restant fidèle à notre Manifeste pour protéger le choix de l'utilisateur sur le Web. Dan travaille déjà à une stratégie que pourrait suivre Firefox pour régler le problème en autorisant les cookies tiers mais seulement de façon temporaire. Son idée est de n'activer les cookies tiers que pour la durée d'ouverture d'un onglet. À la fermeture de

l’onglet, les cookies sont supprimés – les régies publicitaires ne pourront alors plus suivre à la trace les utilisateurs d’un site à l’autre. Dan abordera bientôt tout cela sur son blog avec davantage de détails.



- **2. Donner aux utilisateurs, via les préférences, un meilleur contrôle sur la manière dont les sites peuvent accéder à leurs informations privées**
  Pour l’instant, Firefox donne aux utilisateurs un contrôle précis sur les multiples façons dont les sites peuvent accéder à leurs données. Tout ce que l’utilisateur doit faire, c’est modifier celles-ci dans chacun des panneaux de préférences qui affectent les privilèges des sites.
  Comme on peut le voir ci-dessus, l’interface actuelle de Firefox donne à chaque type de privilège – l’enregistrement des mots de passe, les cookies, etc. – une fenêtre de préférences distincte. Cette conception repose sur des considérations *d’implémentation* plutôt que sur le *schéma mental* de l’utilisateur, ce qui signifie qu’elle correspond au mode de développement et

non à la manière dont les utilisateurs perçoivent l'action qu'ils veulent entreprendre. Avoir une fenêtre individuelle distincte pour chaque permission est cohérent du point de vue de l'implémentation, car chaque privilège de site est distinct dans le code.
Pour l'utilisateur, en revanche, il est impossible de voir de quels privilèges dispose un site donné. Une meilleure présentation pourrait montrer les paramètres de contrôle regroupés par site plutôt que par technologie. Si un utilisateur décide de ne pas faire confiance au site X et refuse qu'il ait accès à quoi que ce soit, il serait plus efficace de contrôler tous les accès du site X au même endroit – et non dans 15 fenêtres différentes. Alex Faaborg a réalisé la maquette ci-dessous pour illustrer à quoi une interface utilisateur centrée sur les sites pourrait ressembler.
Bien que l'ensemble des préférences aient besoin d'être améliorées, l'intégration d'un contrôle des données privées par site, comme Alex le montre ci-dessus pour Firefox 4.0, serait un grand pas en avant vers la reconquête du contrôle des données personnelles par les utilisateurs.



- 3. **Donner un meilleur contrôle de leurs données aux utilisateurs pendant la navigation**
  Grâce à un panneau de préférences spécifique par site, les utilisateurs bénéficieraient d'un contrôle plus fin de ce qui est exposé de leur vie privée par le biais de la configuration de Firefox, certaines options et informations pourraient être accessibles pendant que

l’utilisateur est en train de surfer. Si un site a par exemple accès à la position géographique, cela devrait être indiqué en permanence dans l’interface de Firefox. Si un site conserve un mot de passe, cela devrait être facile à modifier ou désactiver sans avoir à ouvrir le menu des préférences. Le bouton d’identité du site, qui fournit actuellement très peu d’informations, pourrait être amélioré pour informer des privilèges liés à ce site et permettre de les modifier.

Notre objectif pour Firefox 4.0 est de conférer aux utilisateurs davantage de contrôle sur leurs données, à la fois en leur passant à proprement parler les commandes et, plus important encore, en faisant en sorte que la vie privée et l’anonymat soient respectés par défaut sans casser les fonctionnalités du Web. J’espère vraiment que le simple fait d’indiquer à quelles données les sites ont accès sera positif pour le Web, en réduisant la fausse impression de sécurité que de nombreux sites essaient de donner à leurs utilisateurs. Cela permettra aussi de susciter une prise de conscience et de contrôler comment, où et quand les données sont partagées.