La confidentialité bientôt twitterminée ?

Le succès de Twitter est toujours aussi impressionnant (des statistiques nombreuses et significatives ici), même si l'entreprise continue d'enregistrer des pertes, trimestre après trimestre. Ce qui est constant aussi avec Twitter c'est sa désinvolture caractérisée vis-à-vis des données que nous lui laissons récolter.

Calimaq analysait déjà en 2012, à l'occasion de la revente de données à des tierces parties, les multiples entorses au respect de la vie privée dont Twitter est familier.

Un pas nouveau est sur le point d'être franchi, Twitter annonce qu'il va renoncer au Do Not Track.

> Pour tout savoir sur *Do Not Track*, en français *Ne pas me pister*, vous pouvez parcourir la page DNT de Wikipédia ou encore cette page d'information de Mozilla Firefox.

Do Not Track ? Cette sorte d'avertissement figure dans l'en-tête de requête HTTP, et revient un peu à déclarer « Hep, je ne veux pas être pisté par vos régies publicitaires ». Emboîtant le pas à d'autres entreprises du Web bien décidées à ne pas tenir compte de cette demande des utilisateurs et utilisatrices, Twitter préfère un autre protocole hypocrite et malcommode et prend date : le DNT, c'est fini à partir du **18 juin**.

18 juin… Bon sang, voilà qui nous rappelle les heures les plus sombres de… euh non, justement ce serait plutôt le contraire : voilà une date marquante de l'Histoire de France,

celle du fameux Appel de Londres du général de Gaulle.

Et si nous profitions de cette coïncidence pour ranimer la flamme de la résistance à Twittter ? OK les trolls, Twitter n'est pas une armée d'occupation, mais avouez que ce serait assez drôle si nous lancions une campagne avec un appel à quitter Twitter pile le 18 juin ?

Ça vous dirait d'y participer un peu partout sur les réseaux sociaux ? Ouvrez l'œil et le bon, on va s'organiser

En attendant, parcourez la traduction de cet article paru sur le site de l'*Electronic Frontier Foundation* : New Twitter Policy Abandons a Longstanding Privacy Pledge

Le billet s'achève par quelques recommandations pour échapper au pistage de Twitter. Mais la meilleure solution ne serait-elle pas de fermer son compte Twitter et d'aller retrouver les copains sur des réseaux sociaux plus respectueux comme Mastodon et Diaspora* ?

Traduction Framalang : goofy, mo, roptat, Opsylac, xi, Asta, FranBAG, fushia, Glouton

La nouvelle politique de Twitter abandonne un engagement de confidentialité longtemps maintenu

par Jacob Hoffman-Andrews

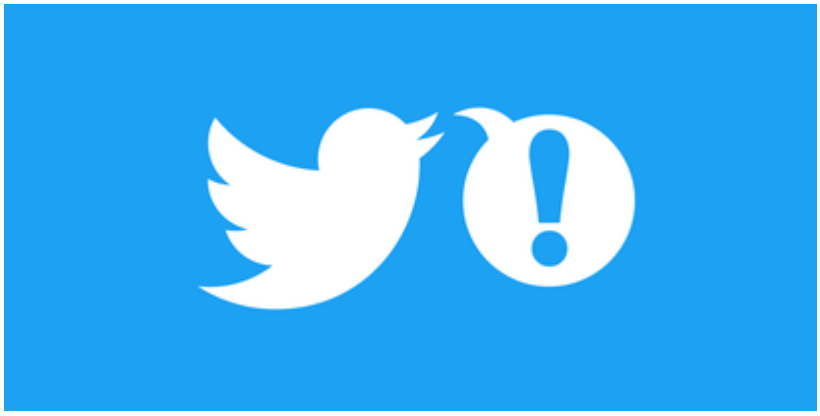
Twitter a l'intention de mettre en œuvre sa nouvelle politique de confidentialité à partir du 18 juin 2017, et, dans le même élan, reviendra probablement sur son engagement pris depuis longtemps de se conformer à la politique de confidentialité associée à l'en-tête DNT. L'entreprise préfère adopter le programme d'auto-régulation *Digital Advertising Alliance*, boiteux et inefficace. L'entreprise profite aussi de cette

l’occasion pour ajouter une nouvelle option de pistage et deux nouvelles possibilités de ciblage, qui seront l’une et l’autre activées par défaut. Cette méthode est indigne d’une entreprise censée respecter les choix de confidentialité des personnes.

Twitter implémente diverses méthodes de pistage dont l’une des plus importantes est l’utilisation de boutons : Tweet, Suivre, et les Tweets embarqués pour enregistrer une bonne partie de votre historique de navigation. Lorsque vous visitez une page dotée de l’un de ces éléments, votre navigateur envoie une requête aux serveurs de Twitter. Cette requête contient un en-tête qui dit à Twitter quel est le site que vous visitez. En vous attribuant un cookie unique, Twitter peut construire un résumé de votre historique de navigation, même si vous n’utilisez pas Twitter. Twitter a été le premier à mettre en place ce pistage : à l’époque, Facebook et Google+ étaient prudents et n’utilisaient pas leurs boutons sociaux pour pister, dû aux préoccupations sur la vie privée. Twitter a adouci sa nouvelle initiative de pistage pour les internautes soucieux du respect de leur vie privée en adoptant *Do Not Track*. Cependant, quand les autres réseaux sociaux ont discrètement emboîté le pas à Twitter, l’oiseau bleu a décidé d’ignorer *Do Not Track*.

Maintenant Twitter envisage d’abandonner le standard *Do Not Track* pour utiliser l’outil « WebChoices », qui fait partie du

programme d'auto-régulation *Digital Advertising Alliance* (DAA), c'est-à-dire une alliance d'entreprises pour la publicité numérique. Ce programme est inefficace car le seul choix qu'il permet à ses utilisateurs et utilisatrices est de refuser les « publicités personnalisées » alors que la plupart souhaitent refuser carrément le pistage. Beaucoup d'entreprises qui participent au DAA, et Twitter en fait partie, continuent de collecter vos informations même si vous avez manifesté votre refus, mais cacheront cette pratique car ne vous seront proposées que des publicités non ciblées. C'est comme demander à quelqu'un d'arrêter d'espionner ouvertement vos conversations et le voir se cacher derrière un rideau pour continuer à vous écouter.



De plus, WebChoices est déficient : il est incompatible avec les autres outils de gestion de la vie privée et nécessite une vigilance constante pour être utilisé. Il repose sur l'utilisation d'un cookie tiers de désinscription sur 131 sites publicitaires. Ce qui est incompatible avec l'une des fonctionnalités les plus basiques des navigateurs web : la désactivation des cookies tiers. D'ailleurs, même si vous acceptez les cookies tiers, votre désinscription ne durera que jusqu'à la prochaine fois où vous effacerez vos cookies, autre comportement habituel que beaucoup utilisent pour protéger leur vie privée en ligne. Sans compter que de nouveaux sites de publicité apparaissent tout le temps. Vous devrez donc recommencer et répéter votre désinscription lorsque le 132e site sera ajouté à WebChoices, ce dont, à moins de suivre la

presse sur les publicitaires, vous ne serez pas au courant. Ces problèmes avec le programme DAA sont justement la raison pour laquelle *Do Not Track* existe. Il est simple, compatible avec les autres mesures de protection de la vie privée et fonctionne sur tous les navigateurs.

Twitter connaît la différence entre une vraie désinscription et une fausse : pendant des années, Twitter a implémenté DNT comme une véritable option de « stop au pistage », et vous pouvez toujours choisir cette option dans l'onglet « Données » des paramètres Twitter, que vous soyez ou non utilisateur ou utilisatrice de Twitter. Cependant, si vous utilisez la nouvelle option de désinscription DAA que Twitter envisage de proposer à la place de DNT, l'entreprise traitera ce choix comme une *fausse désinscription* : Twitter continuera de vous pister, mais ne vous montrera pas de publicités en rapport avec les données collectées.

Que pouvez-vous faire à titre individuel pour vous protéger du pistage de Twitter ? Pour commencer, allez dans les paramètres de votre compte Twitter pour tout désactiver :

Ensuite, installez Privacy Badger, l'extension pour navigateur de l'Electronic Frontier Foundation qui, en plus d'activer

DNT, essaie de détecter et de bloquer automatiquement tout comportement de pistage sur un site provenant de tierces parties. Privacy Badger remplace aussi certains *widgets* des réseaux sociaux par des versions statiques non-intrusives.

Twitter fait faire un grand bond en arrière à la confidentialité des internautes en abandonnant *Do Not Track*. L'entreprise devrait plutôt envisager une nouvelle politique de confidentialité avant le 18 juin pour conserver le respect de DNT et considérer tant DNT que DAA comme de vraies options clairement destinées à dire STOP au pistage.