Sécurité de nos données : sur qui compter ?

Un des meilleurs experts indépendants en sécurité informatique résume ici parfaitement ce qui selon lui constitue un véritable problème : notre dépendance aux *commodités* que nous offrent les entreprises hégémoniques de l'Internet. Nous bradons bien facilement nos données personnelles en échange d'un confort d'utilisation dont on ne peut nier sans hypocrisie qu'il nous rend la vie quotidienne plus facile.

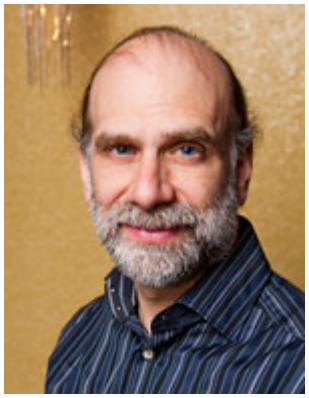
Dès lors que nous ne pouvons renoncer aux facilités que nous procurent Google, Facebook et tous les autres, pouvons-nous espérer que les technologies de sécurité nous épargnent un pillage de nos données personnelles ? Rien n'est moins sûr, selon Bruce Schneier, qui en appelle plutôt à la loi qu'à la technique.

Goofy.

Traduction Framalang : Simon, Docendo, KoS, goofy, audionuma, seb, panini, lamessen, Obny, r0u

Article original : Everyone Wants You To Have Security, But Not from Them

Ils veulent tous notre sécurité, mais pas grâce à d'autres



par Bruce Schneier

En décembre dernier, le PDG de Google Eric Schmidt a été interviewé lors d'une conférence sur la surveillance de l'Institut CATO. Voici une des choses qu'il a dites, après avoir parlé de certaines des mesures de sécurité que son entreprise a mises en place après les révélations de Snowden : « si vous avez des informations importantes, l'endroit le plus sûr pour les garder, c'est chez Google. Et je peux vous assurer que l'endroit le plus sûr pour ne pas les conserver en sécurité, c'est partout ailleurs ».

J'ai été surpris, parce que Google collecte toutes vos informations pour vous présenter la publicité la plus ciblée possible. La surveillance est le modèle économique d'Internet, et Google est l'une des entreprises les plus performantes en la matière. Prétendre que Google protège vos données mieux que quiconque, c'est méconnaître profondément ce pourquoi Google conserve vos données gratuitement.

Je m'en suis souvenu la semaine dernière lorsque je participais à l'émission de Glenn Back avec le pionnier de la cryptographie Whitfield Diffie. Diffie a déclaré :

> *Vous ne pouvez pas avoir de vie privée sans sécurité, et je pense que nous avons des défaillances flagrantes en sécurité informatique, pour des problèmes sur lesquels nous travaillons depuis 40 ans. Vous ne devriez pas vivre avec la peur d'ouvrir une pièce jointe dans un message. Elle devrait être confinée ; votre ordinateur devrait être en mesure de la*

> *traiter. Et si nous avons continué depuis des dizaines d'années sans résoudre ces problèmes, c'est en partie parce que c'est très difficile, mais aussi parce que beaucoup de gens veulent que vous soyez protégés contre tout le monde… sauf eux-mêmes. Et cela inclut tous les principaux fabricants d'ordinateurs qui, grosso modo, veulent contrôler votre ordinateur pour vous. Le problème, c'est que je ne suis pas sûr qu'il existe une alternative viable.*

Cela résume parfaitement Google. Eric Schmidt veut que vos données soient sécurisées. Il veut que Google soit le lieu le plus sûr pour vos données tant que vous ne vous préoccupez pas du fait que Google accède à vos données. Facebook veut la même chose : protéger vos données de tout le monde sauf de Facebook. Les fabricants de matériels ne sont pas différents. La semaine dernière, on a appris que Lenovo avait vendu des ordinateurs avec un logiciel publicitaire préinstallé, appelé Superfish, qui casse la sécurité des utilisateurs pour les espionner à des fins publicitaires.

C'est la même chose pour les gouvernements. Le FBI veut que les gens utilisent un chiffrement fort, mais veut des portes dérobées pour pouvoir accéder à vos données. Le Premier ministre britannique David Cameron veut que vous ayez une sécurité efficace, tant qu'elle n'est pas trop forte pour vous protéger de son gouvernement. Et bien sûr, la NSA dépense beaucoup d'argent pour s'assurer qu'il n'y a pas de sécurité qu'elle ne puisse casser.

Les grandes entreprises veulent avoir accès à vos données pour leurs profits ; les gouvernements les veulent pour des raisons de sécurité, que ces raisons soient bonnes ou moins bonnes. Mais Diffie a soulevé un point encore plus important : nous laissons beaucoup d'entreprises accéder à nos informations parce que cela nous facilite la vie.

J'ai abordé ce point dans mon dernier livre, *Data and Goliath*

:

> *Le confort est l'autre raison pour laquelle nous cédons volontairement des données hautement personnelles à des intérêts privés, en acceptant de devenir l'objet de leur surveillance. Comme je ne cesse de le dire, les services basés sur la surveillance sont utiles et précieux. Nous aimons pouvoir accéder à notre carnet d'adresses, notre agenda, nos photos, nos documents et tout le reste sur n'importe quel appareil que nous avons à portée de la main. Nous aimons des services comme Siri et Google Now, qui fonctionnent d'autant mieux quand ils savent des tonnes de choses sur nous. Les applications de réseaux sociaux facilitent les sorties entre amis. Les applications mobiles comme Google Maps, Yelp, Weather et Uber marchent bien mieux et plus rapidement lorsqu'elles connaissent notre localisation. Permettre à des applications comme Pocket ou Instapaper de connaître nos lectures semble un prix modique à payer pour obtenir tout ce que l'on veut lire à l'endroit qui nous convient. Nous aimons même quand la publicité cible précisément ce qui nous intéresse. Les bénéfices de la surveillance dans ces applications, et d'autres, sont réels et non négligeables.*

Comme Diffie, je doute qu'il existe une alternative viable. Si Internet est un exemple de marché de masse à l'échelle de la planète, c'est parce que toute l'infrastructure technique en

est invisible. Quelqu'un d'autre s'en occupe pour vous. On veut une sécurité forte, mais on veut aussi que les entreprises aient accès à nos ordinateurs, appareils intelligents et données. On veut que quelqu'un d'autre gère nos ordinateurs et smartphones, organise nos courriels et photos, et nous aide à déplacer nos données entre nos divers appareils.
Tous ces « quelqu'un d'autre » vont nécessairement avoir la capacité de violer notre vie privée, soit en jetant carrément un coup d'œil à nos données soit en affaiblissant leur sécurité de façon à ce qu'elles soient accessibles aux agences nationales de renseignements, aux cybercriminels, voire les deux. La semaine dernière, on apprenait que la NSA s'était introduite dans l'infrastructure de la société néerlandaise Gemalto pour voler les clés de chiffrement de milliards, oui, des milliards de téléphones portables à travers le monde. Cela a été possible parce que nous, consommateurs, ne voulons pas faire l'effort de générer ces clés et configurer notre propre sécurité lorsque nous allumons pour la première fois nos téléphones ; nous voulons que ce soit fait automatiquement par les fabricants. Nous voulons que nos données soient sécurisées, mais nous voulons que quelqu'un puisse les récupérer intégralement lorsque nous oublions notre mot de passe.

Nous ne résoudrons jamais ces problèmes de sécurité tant que nous serons notre pire ennemi. C'est pourquoi je crois que toute solution de sécurité à long terme ne sera pas seulement technologique, mais aussi politique. Nous avons besoin de lois pour protéger notre vie privée de ceux qui respectent les lois, et pour punir ceux qui les transgressent. Nous avons besoin de lois qui exigent de ceux à qui nous confions nos données qu'ils protègent nos données. Certes, nous avons besoin de meilleures technologies de sécurité, mais nous avons également besoin de lois qui imposent l'usage de ces technologies.

Crédit photo : Nicubunu (CC BY-SA 2.0)