Internet est (devenu) un État policier

Un article qui ne nous apprend à priori rien de nouveau mais dont les exemples et les arguments enchaînés aboutissent à quelque chose d'absolument terrifiant.

Ce n'est pas un cauchemar c'est la réalité. Une réalité, née d'un accord tacite entre le public (les États) et le privé (les multinationales), qui s'est mise en place sans véritablement rencontrer consciences ni oppositions.

Raison de plus pour soutenir tous ceux qui voient le monde autrement et participer à faire en sorte que nous soyons de plus en plus nombreux à réclamer une éthique et faire vivre le bien commun…

Internet est un État policier

The Internet is a surveillance state

Bruce Schneier – 16 mars 2013 – CNN Opinion
(Traduction : Antoine, Neros, Sky, guillaume, audionuma, Asta + anonymes)

Note de la rédaction : Bruce Schneier est un expert en sécurité et l'auteur de Liars and Outliers: Enabling the Trust Society Needs to Survive *(NdT : Menteurs et Atypiques : mettre en œuvre la confiance dont la société à besoin pour survivre)*.

Je vais commencer par trois points factuels.

Un : certains des hackers militaires chinois qui ont été récemment impliqués dans une attaque d'envergure contre le gouvernement et des entreprises des États-Unis ont été identifiés car ils accédaient à leur compte Facebook depuis la même infrastructure réseau qu'ils utilisaient pour leurs attaques.

Deux : Hector Monsegur, un des dirigeants du mouvent hacker LulzSec, a été identifié et arrêté par le FBI l'année dernière. Bien qu'il prenait de fortes mesures de sécurité informatique et un relais anonyme pour protéger son identité, il s'est quand même fait prendre.

Et trois : Paula Broadwell, qui avait une relation extra-conjugale avec David Petraeus, le directeur de la CIA, a également pris de nombreuses mesures pour masquer son identité. Elle ne se connectait jamais à son service de courriel anonyme depuis le réseau de son domicile. À la place, elle utilisait les réseaux publics des hôtels lorsqu'elle lui envoyait un courriel. Le FBI a effectué une corrélation entre les données d'enregistrement de différents hôtels pour y trouver que son nom était le point commun.

Internet est en état de surveillance. Internet est un état de

surveillance. Que nous l'admettions ou non, et que cela nous plaise ou non, nous sommes traqués en permanence. Google nous trace, tant sur ses propres pages que sur celles auxquelles il a accès. Facebook fait de même, en traçant même les utilisateurs non inscrits chez lui. Apple nous trace sur nos iPhones et iPads. Un journaliste a utilisé un outil appelé Collusion *(NdT : de Mozilla)* pour déterminer qui le traçait : 105 entreprises ont tracé son usage internet sur une seule période de 36 heures !

De plus en plus, nos activités sur Internet sont croisées avec d'autres données nous concernant. La découverte de l'identité de Broadwell a nécessité de croiser son activité sur internet avec ses séjours dans des hôtels. Tout ce que nous faisons aujourd'hui implique l'usage d'un ordinateur, et les ordinateurs ont comme effet secondaire de produire naturellement des données. Tout est enregistré et croisé, et de nombreuses entreprises de big data font des affaires en reconstituant les profils de notre vie privée à partir de sources variées.

Facebook, par exemple, met en corrélation votre comportement en ligne avec vos habitudes d'achat hors-ligne. Et, plus encore, Il y a les données de localisation de votre téléphone portable, les enregistrements de vos mouvements par les caméras de surveillance…

C'est de la surveillance omniprésente : nous sommes tous surveillés, tout le temps, et ces données sont enregistrées de façon permanente. C'est ce à quoi un état de surveillance ressemble, et c'est plus efficace que dans les rêves les plus fous de George Orwell.

Bien sûr, nous pouvons agir pour nous y prémunir. Nous pouvons limiter ce que nous cherchons sur Google depuis nos iPhones, et utiliser à la place les navigateurs Web de nos ordinateurs, qui nous permettent de supprimer les cookies. Nous pouvons utiliser un alias sur Facebook. Nous pouvons éteindre nos

téléphones portables et payer en liquide. Mais plus le temps passe et moins de gens s'en soucient.

Il y a simplement trop de façons d'être pisté. L'Internet, les courriels, les téléphones portables, les navigateurs Web, les sites de réseaux sociaux, les moteurs de recherche : ils sont devenus nécessaires, et il est fantaisiste d'attendre des gens qu'ils refusent simplement de s'en servir juste parce qu'ils n'aiment pas être espionnés, d'autant plus que l'ampleur d'un tel espionnage nous est délibérément cachée et qu'il y a peu d'alternatives commercialisées par des sociétés qui n'espionnent pas.

C'est quelque chose que le libre marché ne peut pas réparer. Nous, les consommateurs, n'avons pas de choix en la matière. Toutes les grandes sociétés qui nous fournissent des services Internet ont intérêt à nous pister. Visitez un site Web et il saura certainement qui vous êtes; il y a beaucoup de façons de vous pister sans cookie. Les compagnies de téléphones défont de façon routinière la protection de la vie privée sur le Web. Une expérience à Carnegie Mellon a pris des vidéos en temps réél d'étudiants sur le campus et a permis d'identifier un tiers d'entre eux en comparant leurs photos avec leurs photos publiques taguées sur Facebook.

Garder sa vie privée sur Internet est désormais presque impossible. Si vous oubliez ne serait-ce qu'une fois d'activer vos protections, ou si vous cliquez sur le mauvais lien, vous attachez votre nom de façon permanente à quelque service anonyme que vous utilisez. Monsegur a dérapé une fois, et le FBI l'a choppé. Si même le directeur de la CIA ne peut garder sa vie privée sur Internet, nous n'avons aucun espoir.

Dans le monde d'aujourd'hui, les gouvernements et les multinationales travaillent de concert pour garder les choses telles qu'elles sont. Les gouvernements sont bien contents d'utiliser les données que les entreprises collectent – en demandant occasionnellement d'en collecter plus et de les

garder plus longtemps – pour nous espionner. Et les entreprises sont heureuses d'acheter des données auprès des gouvernements. Ensemble, les puissants espionnent les faibles, et ils ne sont pas prêts de quitter leurs positions de pouvoir, en dépit de ce que les gens souhaitent.

Résoudre ces questions nécessite une forte volonté gouvernementale, mais ils sont aussi assoiffés de données que les entreprises. Mis à part quelques amendes au montant risible, personne n'agit réellement pour des meilleures lois de protection de la vie privée.

Alors c'est ainsi. Bienvenue dans un monde où Google sait exactement quelle sorte de pornographie vous aimez, où Google en sait plus sur vos centres d'intérêt que votre propre épouse. Bienvenue dans un monde où votre compagnie de téléphone portable sait exactement où vous êtes, tout le temps. Bienvenue à l'ère de la fin des conversations privées, puisque vos conversations se font de plus en plus par courriel, SMS ou sites de réseaux sociaux.

Bienvenue dans un monde où tout ce que vous faites sur un ordinateur est enregistré, corrélé, étudié, passé au crible de société en société sans que vous le sachiez ou ayez consenti, où le gouvernement y a accès à volonté sans mandat.

Bienvenue dans un Internet sans vie privée, et nous y sommes arrivés avec notre consentement passif sans véritablement livrer une seule bataille…

Crédit photo : Mixer (Creative Commons By-Sa)