L’internet des objets nous surveille aussi

Bruce Schneier est un spécialiste reconnu de la sécurité informatique auquel nous donnons souvent un écho sur ce blog. Il chronique régulièrement les avancées et les risques de l’Internet des objets dont la montée en puissance semble irrésistible. On peut présager que dans un délai sans doute très rapproché ces objets vont centupler le volume des données collectées sur nous, puisque non seulement ils nous environnent ou vont le faire, mais ils participeront à notre propre construction sensorielle et mentale du monde, jusqu’au plus secret de notre intimité. (1)

La vitesse de développement de ce marché en fait le nouveau Far-west des géants comme Intel, Cisco, Microsoft ou HP, et bien sûr des fabricants d’électronique. L’espoir de profit qui les anime les fait franchir sans scrupules la barrière de la vie privée (2) : non seulement l’implémentation de la sécurité sur ces objets est minime voire inexistante, mais ils sont aussi de parfaits petits espions programmés pour moucharder.

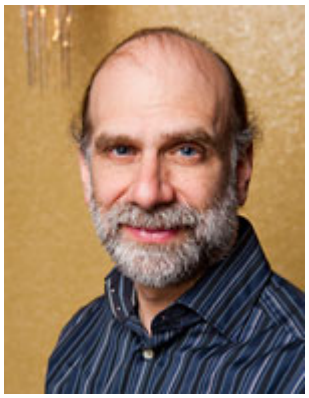
Nous n’échapperons pas plus à l’Internet des objets que nous n’avons échappé à l’ubiquité des smartphones. Faut-il cependant renoncer définitivement à notre vie privée au profit de ces objets intrusifs ? Quelles limites poser et comment ? Au fait, existe-t-il des objets connectés libres et éthiques ?

Voici l’Internet des objets qui parlent derrière votre dos

Par Bruce Schneier

Source : The Internet of Things that Talk About You Behind Your Back (cet article a fait l’objet d’une première publication sur Vice Motherboard).

Traduction Framalang : r0u, goofy, teromene, et un anonyme



SilverPush est une *startup* indienne qui essaie de lister les différents appareils que vous possédez. Elle embarque des sons inaudibles dans des pages web que vous lisez et dans les publicités télévisées que vous regardez. Un logiciel secrètement embarqué dans vos ordinateurs, tablettes, et smartphones récupère ces signaux, et utilise des cookies pour transmettre ces informations à SilverPush. Au final, cette société peut vous pister d'un appareil à l'autre. Elle peut associer les publicités télévisées que vous regardez avec les recherches web que vous effectuez. Elle peut relier ce que vous faites sur votre tablette avec ce que vous faites sur votre ordinateur.

Vos données numériques parlent de vous derrière votre dos, et la plupart du temps, vous ne pouvez pas les arrêter… ni même savoir ce qu'elles disent.
Ce n'est pas nouveau, mais cela empire.

La surveillance est le *business model* d'Internet, et plus ces sociétés en savent sur les détails intimes de votre vie, plus elles peuvent en tirer profit. Il existe déjà des dizaines de sociétés qui vous espionnent lorsque vous surfez sur Internet, reliant vos comportements sur différents sites et utilisant ces informations pour cibler les publicités. Vous le découvrez quand vous cherchez quelque chose comme des vacances à Hawaï, et que des publicités pour des vacances similaires vous suivent sur tout Internet pendant des semaines. Les sociétés comme Google et Facebook font d'énormes profits en reliant les sujets sur lesquels vous écrivez et qui vous intéressent avec des sociétés qui veulent vous vendre des choses.

Le pistage entre tous les appareils est la dernière obsession des commerciaux sur internet. Vous utilisez probablement plusieurs appareils connectés à Internet : votre ordinateur, votre smartphone, votre tablette, peut-être même votre télévision connectée… et de plus en plus, des appareils connectés comme les thermostats intelligents et consorts. Tous ces appareils vous espionnent, mais ces différents espions ne sont pas reliés les uns aux autres. Les *startups* comme SilverPush, 4Info, Drawbridge, Flurry et Cross Screen Consultants, ainsi que les mastodontes comme Google, Facebook et Yahoo sont tous en train de tester différentes technologies pour « régler » ce problème.

Les revendeurs sont très intéressés par ces informations. Ils veulent savoir si leur publicité télévisée incite les gens à rechercher leurs produits sur internet. Ils veulent corréler ce que les gens recherchent sur smartphone avec ce qu'ils achètent sur ordinateur. Ils veulent pister les positions des personnes grâce aux capacités de surveillance de leur téléphone, et utiliser cette information pour envoyer des publicités ciblées géographiquement sur leur ordinateur. Ils veulent que les données de surveillance des appareils connectés soient reliées avec tout le reste.
C'est là que l'Internet des objets aggrave le problème. Comme les ordinateurs sont de plus en plus embarqués dans les objets que nous utilisons au quotidien, et pénètrent encore plus d'aspects de nos vies, encore plus de sociétés veulent les utiliser pour nous espionner sans que nous soyons au courant et sans notre consentement.

Techniquement, bien sûr, nous avons donné notre accord. Les accords de licence que nous ne lisons pas mais que nous acceptons légalement quand nous cliquons sans y penser sur « J'accepte », ou lorsque nous ouvrons un colis que nous avons acheté, donnent à toutes ces sociétés les droits légaux de procéder à cette surveillance. Et quand on voit la façon dont les lois sur la vie privée aux États-Unis sont actuellement écrites, ils sont propriétaires de toutes ces données et n'ont pas besoin de nous laisser y accéder.

Nous acceptons toute cette surveillance internet parce que nous n'y pensons pas

réellement. S'il y avait des dizaines de personnes provenant d'entreprises publicitaires avec leurs stylos et leurs carnets qui regardent au-dessus de notre épaule lorsqu'on écrit un mail sur Gmail ou tout simplement quand on navigue sur Internet, la plupart d'entre nous s'y opposeraient. Si les sociétés qui fabriquent nos applications sur smartphones nous suivaient réellement toute la journée, ou si les sociétés qui collectent les plaques d'immatriculation pouvaient être vues lorsque nous conduisons, nous exigerions qu'elles arrêtent. Et si nos télévisions, nos ordinateurs et nos appareils mobiles parlaient de nous à voix haute et se coordonnaient d'une manière qu'on peut entendre, nous serions épouvantés.

La commission fédérale du commerce (FTC) est en train d'examiner les technologies de pistage d'un appareil à l'autre, avec la volonté de pouvoir les réguler. Mais si nous nous fions à l'histoire récente, toute résolution prise sera mineure et inefficace pour s'occuper du plus gros du problème.
Nous devons faire mieux. Nous devons avoir un débat sur les implications du pistage entre appareils sur notre vie privée, mais, surtout, nous devons réfléchir à l'éthique du marché de la surveillance. Voulons-nous vraiment que des entreprises connaissent les détails de notre vie, et qu'elles puissent garder ces données éternellement ? Croyons-nous vraiment que nous n'avons pas le droit d'accéder aux données collectées sur nous, de corriger les données erronées, ou de supprimer celles qui sont trop intimes ou embarrassantes ? Au minimum, nous devons mettre des limites sur les données comportementales qui peuvent légalement être récoltées, savoir pour combien de temps, avoir le droit de télécharger les données collectées sur nous, et pouvoir bannir le pistage par des publicités de parties tierces. Le dernier point est crucial : ce sont les entreprises qui nous espionnent de site en site ou d'appareil en appareil qui causent le plus de dommages à notre vie privée.

Le marché de la surveillance d'Internet a moins de 20 ans, et a émergé parce qu'il n'y avait pas de régulation pour limiter son comportement. C'est désormais une industrie puissante, et qui s'étend au-delà des ordinateurs et téléphones, dans tous les aspects de nos vies. Il est grand temps que nous posions des limites sur ce que peuvent dire et faire avec nous dans notre dos depuis longtemps les ordinateurs et les entreprises qui les contrôlent.

(1) Un article parmi d'autres pour en savoir plus sur les objets connectés et

comment ils altèrent sensiblement notre mode de vie : Objets connectés : allons-nous tous devenir idiots ?

(2) Voici un article très récent sur les espoirs et les craintes qu'on peut éprouver : « **Rapport de l'UIT sur Internet des objets : un grand potentiel de le développement mais des risques pour la confidentialité et l'interopérabilité** » (source)

Quelques passages (ma traduction) :

> *L'UIT (Union Internationale des Télécommunications, un organisme qui dépend de l'ONU) a publié aujourd'hui son rapport [pdf] « Exploiter l'internet des objets pour le développement mondial », produite en collaboration avec Cisco Systems.*
>
> *Les appareils connectés qui communiquent les uns avec les autres et avec les êtres humains pourraient résoudre les grands défis mondiaux et être un vecteur pour le développement mondial(…) Toutefois, des questions demeurent, telles que les stratégies visant à protéger la vie privée, et l'interopérabilité entre les dispositifs et systèmes.*
>
> *(…) des défis importants persistent, selon le rapport, en particulier le fait que « la même infrastructure qui permet aux gens de créer, stocker et partager des informations peut également mettre en péril leur vie privée et leur sécurité »*
>
> *« Ces mêmes techniques peuvent être utilisées pour la surveillance, qu'elle soit ciblée ou à grande échelle », dit le rapport.*