Le chiffrement, maintenant (1)

Internet est dans un sale état. Tout cassé, fragmenté, explosé en parcelles de territoires dont des géants prédateurs se disputent âprement les lambeaux : Google, Apple, Facebook, Amazon, et tous ceux qui sont prêts à tout pour ravir leur monopole ne voient en nous que des profils rentables et dans nos usages que des consommations. La captation par ces entreprises de nos données personnelles a atteint un degré de sophistication auquel il devient difficile d'échapper.

Mais désormais une autre menace pèse sur tous les usagers du net, celle de la surveillance généralisée. Sans remonter aux années où était révélé et contesté le réseau Echelon, depuis longtemps on savait que les services secrets (et pas seulement ceux des pays de l'Ouest) mettaient des moyens technologiques puissants au service de ce qu'on appelait alors des « écoutes ». Ce qui est nouveau et dévastateur, c'est que nous savons maintenant quelle ampleur inouïe atteint cette surveillance de tous les comportements de notre vie privée. Notre vie en ligne nous permet tout : lire, écrire, compter, apprendre, acheter et vendre, travailler et se détendre, communiquer et s'informer… Mais aucune de nos pratiques numériques ne peut échapper à la surveillance. et gare à ceux qui cherchent à faire d'Internet un outil citoyen de contestation ou de dévoilement : censure politique du net en Chine et dans plusieurs autres pays déjà sous prétexte de lutte contre la pédopornographie, condamnation à des peines disproportionnées pour Manning, exil contraint pour Assange et Snowden, avec la complicité des gouvernements les systèmes de surveillance piétinent sans scrupules les droits fondamentaux inscrits dans les constitutions de pays plus ou moins démocratiques.

Faut-il se résigner à n'être que des *consommateurs-suspects* ? Comment le simple utilisateur d'Internet, qui ne dispose pas de compétences techniques sophistiquées pour installer des contre-mesures, peut-il préserver sa « bulle » privée, le secret de sa vie intime, sa liberté de communiquer librement sur Internet — qui n'est rien d'autre que la forme contemporaine de la liberté d'expression ?

Oui, il est difficile au citoyen du net de s'installer un réseau virtuel privé, un serveur personnel de courrier, d'utiliser TOR, de chiffrer ses messages de façon sûre, et autres dispositifs que les geeks s'enorgueillissent de maîtriser (avec,

n’est-ce pas, un soupçon de condescendance pour *les autres*… Souvenez-vous des réactions du type : « — Hadopi ? M’en fous… je me fais un tunnel VPN et c’est réglé »).

Aujourd’hui que *tout le monde* a compris à quelle double surveillance nous sommes soumis, c’est *tout le monde* qui devrait pouvoir accéder à des outils simples qui, à défaut de protéger intégralement la confidentialité, la préservent pour l’essentiel.

Voilà pourquoi une initiative récente de la Fondation pour la liberté de la presse (Freedom of the Press Foundation) nous a paru utile à relayer. **Encryption works** (« le chiffrement, ça marche ») est un petit guide rédigé par Micah Lee (membre actif de l’EFF et développeur de l’excellente extension HTTPS Everywhere) qui propose une initiation à quelques techniques destinées à permettre à chacun de protéger sa vie privée.

Nous vous en traduisons aujourd’hui le préambule et publierons chaque semaine un petit chapitre. Répétons-le, il s’agit d’une première approche, et un ouvrage plus conséquent dont la traduction est en cours sera probablement disponible dans quelques mois grâce à Framalang. Mais faisons ensemble ce premier pas vers la maîtrise de notre vie en ligne.

Contributeurs : Slystone, Asta, peupleLa, lamessen, Calou, goofy, Lolo

Le chiffrement, ça marche

Comment protéger votre vie privée à l’ère de la surveillance par la NSA

par Micah Lee

> *Le chiffrement, ça marche. Correctement configurés, les systèmes de chiffrement forts font partie des rares choses sur lesquelles vous pouvez compter. Malheureusement, la sécurité des points d’accès est si horriblement faible que la NSA peut la contourner fréquemment.*
>
> — Edward Snowden, répondant en direct à des questions sur le site du Guardian

La NSA est la plus importante et la plus subventionnée des agences d'espionnage que le monde ait pu connaître. Elle dépense des milliards de dollars chaque année dans le but d'aspirer les données numériques de la plupart des gens de cette planète qui possèdent un accès à Internet et au réseau téléphonique. Et comme le montrent des articles récents du Guardian et du Washington Post, même les plus banales communications américaines n'échappent pas à leur filet.

Vous protéger de la NSA, ou de toute autre agence gouvernementale de renseignements, ce n'est pas simple. Et ce n'est pas un problème que l'on peut résoudre en se contentant de télécharger une application. Mais grâce au travail de cryptographes civils et de la communauté du FLOSS, il reste possible de préserver sa vie privée sur Internet. Les logiciels qui le permettent sont librement accessibles à tous. C'est particulièrement important pour des journalistes qui communiquent en ligne avec leurs sources.

(à suivre…)