Les géants du Web nous veulent du bien

Lourdement mises en cause pour avoir laissé les agences gouvernementales accéder aux données de leurs clients, les grandes entreprises du Web ont vite senti qu'elles risquaient gros à passer aux yeux du monde entier pour des complices de l'espionnage de masse. Elles ont donc défendu leur position avec une belle énergie en clamant leur bonne foi : elles auraient été les victimes non consentantes des intrusions de la NSA.

Dans cette recherche d'une crédibilité essentielle pour leur survie économique – car à chaque utilisateur perdu c'est la monétisation d'un profil qui disparaît, elles multiplient les déclarations hostiles aux pressions, de plus en plus fortes aux USA, pour limiter voire interdire le chiffrement de haut niveau, comme pour leur imposer des portes dérobées. C'est ce que nous pouvons voir dans cette compilation réunie par l'EFF.

> L'*Electronic Frontier Foundation* est une organisation non gouvernementale qui mène depuis vingt-cinq ans un combat sur de multiples fronts pour les libertés numériques, comme le fait La Quadrature du Net, qui est un peu son équivalent pour la France et l'Europe.

À lire cette suite d'extraits choisis, on hésite un peu à donner pleine absolution à toutes ces entreprises à but parfaitement lucratif. Ces déclarations sont-elles sincères, et surtout sont-elles concrètement suivies d'effets ? Sciemment ou non, elles ont laissé l'espionnage s'installer au cœur de leur activité, et même au cœur d'un système d'exploitation hégémonique. Aujourd'hui elles voudraient préserver le chiffrement comme outil indispensable aux transactions économiques, soit. Mais on sait bien que par ailleurs elles n'ont guère de scrupules à faire commerce de

nos données privées. Ce que ces entreprises états-uniennes redoutent surtout c'est que l'administration Obama (elle-même sous la pression des agences d'espionnage) « tue le business ».
Quoi qu'il en soit, l'EFF trouve en elles des alliées inattendues puissantes pour faire pression sur le plan politique : l'enjeu est de taille et peut justifier une aussi paradoxale alliance de circonstance. En effet, le chiffrement fort, attaqué par de nombreux gouvernements dans le monde sous prétexte de sécurité, demeure un rempart qui protège nos libertés numériques.

Où en sont les grandes entreprises du numérique sur la question du chiffrement ?

Une comparaison des positions affichées par 21 des plus importantes entreprises du numérique

Article original sur le site de l'EFF : Where Do Major Tech Companies Stand on Encryption?
Traduction Framalang : Luke, Obny, goofy, KoS, Niilos, McGregor

En ce moment même une bataille décisive fait rage autour du chiffrement.

Les services de police essaient d'imposer des « portes dérobées » (*backdoors*) pour accéder à nos données et nos communications sensibles, tandis que les groupes de défense des libertés individuelles répliquent par une campagne intitulée SaveCrypto. Quant au président Obama, il s'efforce de trouver un compromis, en évitant de donner à ces demandes la force d'une loi, mais en continuant de façon informelle à faire pression sur les entreprises pour qu'elles fournissent un accès sans chiffrement aux données qu'elles récoltent.

Où en sont donc les entreprises du numérique sur ce front ?

Elles sont les seules à être à la fois en position de connaître et de résister aux pressions officieuses exercées par le gouvernement pour qu'elles donnent accès aux données de leurs utilisateurs. Nous leur offrons sur un plateau de gigantesques quantités de données sensibles tout en leur faisant confiance pour qu'elles les gardent en sécurité. Quelles sont les entreprises qui souhaitent afficher publiquement leur opposition aux portes dérobées ?

Nous avons rassemblé les politiques publiques des 21 plus importantes entreprises du numérique pour que vous puissiez les comparer. Certaines des déclarations proviennent de notre rapport annuel *Who has your back* et quelques-unes de blogs et de rapports sur la transparence issus des entreprises..

Voyez plutôt vous-même :

Adobe

> *Adobe n'a aménagé de « porte dérobée » pour aucun gouvernement – ni étranger ni américain – dans ses produits et ses services. Toutes les demandes du gouvernement pour obtenir des données de nos utilisateurs doivent passer par la grande porte (c'est-à-dire en menant suivant une procédure légale valide auprès du département juridique approprié d'Adobe). Adobe s'oppose vigoureusement à toute législation aux USA ou à l'étranger qui affaiblirait de quelque manière que ce soit la sécurité de nos produits ou la protection de la vie privée de nos utilisateurs.*

Amazon

> *Alors que nous reconnaissons qu'il est légitime et nécessaire pour les autorités de mener des enquêtes sur le crime et les activités terroristes, qu'il est nécessaire de coopérer avec les autorités quand elles respectent le cadre légal pour*

> *mener de telles investigations, nous sommes opposés à une législation qui interdirait les technologies de sécurité et de chiffrement ou les soumettrait à une demande d'autorisation, cela aurait pour effet d'affaiblir la sécurité des produits, systèmes et services qu'utilisent nos clients, qu'ils soient des particuliers ou des entreprises.*

Apple

> *De plus, Apple n'a jamais travaillé avec quelque agence gouvernementale de quelque pays que ce soit pour créer des « portes dérobées » dans nos produits ou services. Nous n'avons non plus jamais permis à un quelconque gouvernement d'accéder à nos serveurs. Et nous ne le ferons jamais.*

L'entreprise Apple mérite d'être saluée pour sa prise de position encore plus ferme contre les portes dérobées sur son nouveau site consacré au respect de la vie privée qui explique la politique de l'entreprise. Cette nouvelle déclaration indique :

> *Le chiffrement sécurise des milliers de milliards de transactions en ligne chaque jour. Que ce soit en passant commande ou en payant, vous utilisez du chiffrement. Vos données sont transformées en un texte indéchiffrable qui ne peut être lu que si on dispose de la bonne clé. Depuis plus de dix ans nous protégeons vos données avec SSL et TLS [liens ici] dans Safari, FileVault pour Mac, et le chiffrement qui existe par défaut dans iOS. Nous refusons également d'ajouter des portes dérobées au moindre de nos produits parce qu'elles sapent les protections que nous avons mises au point. Et nous ne pouvons déverrouiller votre appareil pour personne parce que vous seul en avez la clé, votre unique mot de passe. Nous sommes résolus à utiliser un chiffrement fort parce que vous devez avoir la certitude que les données que contient votre appareil et les informations que vous partagez avec d'autres sont protégées.*

Comcast

> *Comcast ne soutient pas la création de portes dérobées extra-légales ou l'insertion délibérée de failles de sécurité, dans les logiciels open source ou autres, pour faciliter la surveillance sans procédure légale appropriée.*

Dropbox

> *Les gouvernements ne devraient jamais installer de portes dérobées dans les services en ligne ou compromettre les infrastructures pour obtenir des données personnelles. Nous continuerons à travailler pour protéger nos systèmes et pour changer les lois afin d'établir clairement que ce type d'activité est illégal.*
>
> *Nous constatons également que partout dans le monde, des administrations essaient de limiter les mesures de sécurité comme le chiffrement sans pour autant faire de progrès sur le renforcement de la protection légale que méritent les gens. Il en résulte les gouvernements demandent actuellement des informations sur une toute petite partie de nos clients, mais cherchent de plus en plus à perturber l'équilibre entre vie privée et sécurité publique d'une manière qui concerne tout le monde.*
> *Comme nous le disions précédemment, les autorités ont parfois besoin d'accéder aux données privées pour protéger les citoyens. Cependant, cet accès devrait être réglementé par la loi et non en réclamant des « portes dérobées » ou en affaiblissant la sécurité de nos produits et services utilisés par des millions de clients respectueux de la loi. Ceci devrait concerner chacun d'entre nous.*

Pinterest

> *Pinterest s'oppose aux portes dérobées contraintes et soutient les réformes visant à limiter les demandes de*

surveillance de masse.

Slack

La transparence est une valeur clé pour nous et une caractéristique importante de Slack lui-même. C'est cet engagement pour la transparence qui amène mon dernier point — Slack s'oppose aux portes dérobées des pouvoirs publics de toutes sortes, mais particulièrement aux exigences des gouvernements qui pourraient compromettre la sécurité des données.

Snapchat

La confidentialité et la sécurité sont des valeurs essentielles chez Snapshat, et nous nous opposons fermement à toute initiative qui viendrait affaiblir la sécurité de nos systèmes. Nous nous engageons à gérer vos données de manière sécurisée et mettrons à jour ce rapport tous les six mois.

Sonic

Enfin, nous déclarons publiquement notre position concernant l'inclusion forcée de portes dérobées, failles de sécurité volontaires ou divulgation de clés de chiffrement. Sonic ne soutient pas ces pratiques.

Tumblr

Sécurité : nous croyons qu'aucun gouvernement ne devrait installer de portes dérobées dans les protocoles de sécurité du web, ou encore compromettre l'infrastructure d'internet. Nous combattrons les lois qui permettraient cela, et nous travaillerons à sécuriser les données de nos utilisateurs contre de telles intrusions.

Wickr

> *Nous croyons au chiffrement robuste et généralisé et exhortons le gouvernement des États-Unis à adopter des normes de chiffrement fort pour assurer l'intégrité de l'information des particuliers, des entreprises et des organismes gouvernementaux à travers le monde.*

WordPress

> *Certains gouvernements ont récemment cherché à affaiblir le chiffrement, au nom de l'application de la loi. Nous sommes en désaccord avec ces suggestions et ne croyons pas qu'il soit possible d'inclure une quelconque faille de sécurité délibérée ou autres portes dérobées dans les technologies de chiffrement, même pour le « seul » bénéfice des services de sécurité. Comme l'a dit un sage, « il n'existe pas de faille technologique qui puisse être utilisée uniquement par des personnes bienveillantes respectueuses de la loi ». Nous sommes entièrement d'accord.*

Yahoo

> *Nous avons chiffré beaucoup de nos principaux produits et services pour les protéger de l'espionnage des gouvernements et autres acteurs. Ceci inclut le chiffrement du trafic entre les centres de données de Yahoo ; l'utilisation de HTTPS par défaut sur Yahoo Mail et la page d'accueil de Yahoo ; et l'implémentation de règles de bonne pratique en matière de sécurité, y compris le support de TLS 1.2, de la Confidentialité persistante et d'une clé RSA 2048 bits pour la plupart de nos services tels que la page d'accueil, la messagerie et les magazines numériques. Nous avons également mis en place une extension de chiffrement de bout en bout (e2e) pour Yahoo Mail, disponible sur GitHub. Notre but est de fournir une solution de chiffrement e2e intuitive à tous nos utilisateurs d'ici la fin 2015. Nous sommes engagés sur*

> *la sécurité de cette solution et nous opposons aux demandes de l'affaiblir délibérément ainsi que tout autre système de chiffrement.*

Credo Mobile, Facebook, Google, LinkedIn, Twitter, WhatsApp, et la Wikimedia Foundation ont tous signé une lettre proposée par l'Open Technology Institute (OTI) qui s'oppose à l'affaiblissement volontaire des mesures de sécurité :

> *Nous vous exhortons à rejeter toute proposition poussant les entreprises américaines à affaiblir délibérément la sécurité de leurs produits… Que vous les appeliez portes avant ou portes dérobées, le fait d'introduire délibérément des vulnérabilités à usage gouvernemental dans des produits sécurisés à l'intention du gouvernement rendra ces produits moins sécurisés face à d'autres attaquants. Tous les experts en sécurité qui se sont exprimés sur cette question sont d'accord, y compris ceux du gouvernement.*

Que pouvons-nous en conclure ? Il existe une très forte opposition des entreprises technologiques aux portes dérobées imposées.

La semaine dernière, l'EFF, accompagnée d'une coalition formée d'entreprises technologiques et de groupes de défense des libertés, a lancé SaveCrypto.org, une pétition en ligne où les parties concernées peuvent faire savoir au président Obama que l'administration devrait se prononcer en faveur d'un chiffrement fort. Alors qu'Obama a clarifié sa position initiale, il a aussi promis de répondre à toute pétition qui recueillerait plus de 100 000 signatures. Cela signifie qu'il est encore temps pour de l'influencer.

Dans une ère de piratage omniprésent et de violation des données sensibles, il est temps pour le président Obama d'écouter les utilisateurs d'Internet et les entreprises qui se battent pour la sécurité des utilisateurs et leur vie

privée.

Vous pouvez ajouter votre voix à la pétition ci-dessous.
https://savecrypto.org/