

Le chiffrement ne suffira pas

Le chiffrement, s'il n'est pas encore dans tous nos usages – et loin s'en faut, chez la plupart des utilisateurs, est nettement devenu un argument marketing et une priorité pour les entreprises qui distribuent logiciels et services. En effet, le grand public est beaucoup plus sensible désormais à l'argument de la sécurité de la vie privée. Donc les services qui permettent la communication en ligne rivalisent d'annonces pour promettre et garantir une sécurité toujours plus grande et que l'on puisse activer d'un simple clic.

Que faut-il croire, à qui et quoi pouvons-nous confier nos communications ?

L'article de Hannes Hauswedell que nous avons traduit nous aide à faire un tri salutaire entre les solutions logicielles du marché, pointe les faux-semblants et les failles, puis nous conduit tranquillement à envisager des solutions fédérées et pair à pair reposant sur des logiciels libres. Des réseaux de confiance en somme, ce qui est proche de l'esprit de l'initiative [C.H.A.T.O.N.S](#) portée par Framasoft et qui suscite déjà un intérêt grandissant.

Comme d'habitude les commentaires sont ouverts et libres si vous souhaitez par exemple ajouter vos découvertes à ce recensement critique forcément incomplet.

Préserver sa vie privée, au-delà du chiffrement

par Hannes Hauswedell

d'après l'article publié sur son blog : [Why Privacy is more than Crypto](#)

Traduction Framalang : egilli, Lumi, goofy, roptat, lyn, tchevalier, touriste, Edgar Lori, Penguin

Au cours de l'année dernière on a pu croire que les poules avaient des dents quand les grandes entreprises hégémoniques comme Apple, Google et Facebook ont toutes mis en œuvre le chiffrement à un degré ou un autre. Pour Facebook avec [WhatsApp](#) et Google avec [Allo](#), le chiffrement de la messagerie a même été implémenté par rien moins que le célèbre Moxie Marlinspike, un hacker anarchiste qui a [la bénédiction d'Edward Snowden](#) !

Donc tout est pour le mieux sur le front de la défense de la vie privée !... Euh, vraiment ?

Sommaire

[1. Le chiffrement](#)

[2. Logiciels libres et intégrité des appareils](#)

[3. Décentralisation, contrôle par les distributeurs et métadonnées](#)

[4. En deux mots](#) (pour les moins courageux)

J'ai [déjà développé](#) mon point de vue sur la sécurité de la messagerie mobile et j'en ai parlé dans [un podcast \(en allemand\)](#). Mais j'ai pensé qu'il fallait que j'y revienne, car il existe une certaine confusion sur ce que signifient sécurité et confidentialité (en général, mais particulièrement dans le contexte de la messagerie), et parce que les récentes annonces dans ce domaine ne donnent selon moi qu'un sentiment illusoire de sécurité.

Je vais parler de WhatsApp et de Facebook Messenger (tous deux propriétés de Facebook), de Skype (possédé par Microsoft), de Telegram, de Signal (Open Whisper systems), Threema (Threema GmbH), Allo (possédé par Google) et de quelques clients XMPP, je dirai aussi un mot de ToX et Briar. Je n'aborderai pas les diverses fonctionnalités mêmes si elles sont liées à la confidentialité, comme les notifications évidemment mal

conçues du type « le message a été lu ». Je n'aborderai pas non plus les questions d'anonymat qui sont connexes, mais selon moi moins importantes lorsqu'il s'agit d'applications de substitution aux SMS, puisque vous connaissez vos contacts de toutes façons.

Le chiffrement

Quand on parle de confidentialité ou de sécurité des communications dans les messageries, il s'agit souvent de chiffrement ou, plus précisément, du chiffrement des données qui se déplacent, de la protection de vos messages pendant qu'ils voyagent vers vos contacts.



Il existe trois moyens classiques pour faire cela :

1. pas de chiffrement : tout le monde sur votre réseau WIFI local ou un administrateur système quelconque du réseau internet peut lire vos données
2. le chiffrement en transit : la connexion au et à partir du fournisseur de service, par exemple les serveurs WhatsApp, et entre les fournisseurs de services est sécurisée, mais le fournisseur de service peut lire le message
3. le chiffrement de bout en bout : le message est lisible uniquement par ceux à qui la conversation est adressée,

mais le moment de la communication et les participants sont connus du fournisseur de service

Il y a aussi une propriété appelée « confidentialité persistante » (*perfect forward secrecy* en anglais) qui assure que les communications passées ne peuvent être déchiffrées, même si la clef à long terme est révélée ou volée.

À l'époque, la plupart des applications, même WhatsApp, appartenaient à la première catégorie. Mais aujourd'hui presque toutes les applications sont au moins dans la deuxième. La probabilité d'un espionnage insoupçonné en est réduite (c'est toujours possible pour les courriels par exemple), mais ce n'est évidemment pas suffisant, puisque le fournisseur de service peut [être malveillant](#) ou [forcé de coopérer](#) avec des gouvernements malveillants ou des agences d'espionnage sans contrôle démocratique.

C'est pour cela que vous voulez que votre messagerie fasse du chiffrement de bout en bout. Actuellement, les messageries suivantes le font (classées par taille supposée) : WhatsApp, Signal, Threema, les clients XMPP avec GPG/OTR/Omemo (ChatSecure, Conversations, Kontalk).

Les messageries qui disposent d'un mode spécifique (« chat secret » ou « mode incognito ») sont Telegram et Google Allo. Il est vraiment dommage qu'il ne soit pas activé par défaut, donc je ne vous les recommande pas. Si vous devez utiliser l'un de ces programmes, assurez-vous toujours d'avoir sélectionné le mode privé. Il est à noter que les experts considèrent que [le chiffrement de bout en bout de Telegram est moins robuste](#), même s'ils s'accordent à dire que les attaques concrètes pour récupérer le texte d'un message ne sont pas envisageables.

D'autres programmes populaires, comme la messagerie de Facebook ou Skype n'utilisent pas de chiffrement de bout en bout, et devraient être évités. Il a été prouvé que [Skype](#)

[analyse vos messages](#), je ne m'attarderai donc pas sur ces deux-là.

Logiciels libres et intégrité des appareils

Donc maintenant, les données sont en sécurité tant qu'elles voyagent de vous à votre ami. Mais qu'en est-il avant et après leur envoi ? Ne pouvez-vous pas aussi tenter d'espionner le téléphone de l'expéditeur ou du destinataire avant qu'elles ne soient envoyées et après leur réception ? Oui c'est possible et en Allemagne le gouvernement a déjà activement utilisé la « [Quellen-Telekommunikationsüberwachung](#) » (surveillance des communications à la source) précisément pour passer outre le chiffrement.

Revenons à la distinction entre (2) et (3). La différence principale entre le chiffrement en transit et de bout en bout est que vous n'avez plus besoin de faire confiance au fournisseur de service... FAUX : Dans presque tous les cas, la personne qui fait tourner le serveur est la même que celle qui fournit le programme. Donc forcément, vous devez croire que le logiciel fait bien ce qu'il dit faire. Ou plutôt, il doit y avoir des moyens sociaux et techniques qui vous donnent suffisamment de certitude que le logiciel est digne de confiance. Sinon, la valeur ajoutée du chiffrement de bout en bout est bien maigre.

« logiciel libre » fait référence à **quatre libertés** :

- **liberté 0** : la liberté d'**exécuter** le programme, pour tous les usages
- **liberté 1** : la liberté d'**étudier** le fonctionnement du programme, et de l'**adapter** à ses besoins
=> l'accès au code source est nécessaire
- **liberté 2** : la liberté de **redistribuer** des copies, donc d'aider son voisin
- **liberté 3** : la liberté d'**améliorer** le programme et de **publier** ses améliorations, pour en faire profiter toute la communauté
=> l'accès au code source est nécessaire

Diapo par Hedi Magroun
<http://fr.slideshare.net/hmagroun/linux-h-magrounauf2008>

La liberté des logiciels

C'est maintenant que [le logiciel libre](#) entre en jeu. Si le code source est publié, il y aura un grand nombre de hackers et de volontaires pour vérifier que le programme chiffre vraiment le contenu. Bien que ce contrôle public ne puisse vous donner une sécurité parfaite, ce processus est largement reconnu comme étant le meilleur pour assurer qu'un programme est globalement sûr et que les problèmes de sécurité sont découverts (et aussi corrigés). Le logiciel libre permet aussi de créer des versions non officielles ou rivales de l'application de messagerie, qui seront compatibles. S'il y a certaines choses que vous n'aimez pas ou auxquelles vous ne faites pas confiance dans l'application officielle, vous pourrez alors toujours en choisir une autre et continuer de chatter avec vos amis.

Certaines compagnies comme Threema qui ne fournissent pas leurs sources assurent évidemment qu'elles ne sont pas nécessaires pour avoir confiance. [Elles affirment](#) que leur code a été audité par une autre compagnie (qu'ils ont généralement payée pour cela), mais si vous ne faites pas confiance à la première, pourquoi faire confiance à une autre engagée par celle-ci ? Plus important, comment savoir que la version vérifiée par le tiers est bien la même version que

celle installée sur votre téléphone ? (Vous recevez des mises à jours régulières ou non ?)

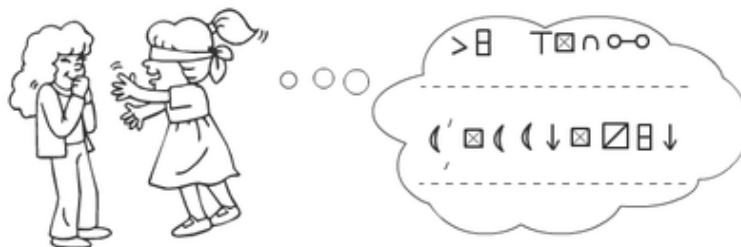
Cela vaut aussi pour les gouvernements et les entités publiques qui font ce genre d'audits. En fonction de votre modèle de menace ou de vos suppositions sur la société, vous pourriez être enclins à faire confiance aux institutions publiques plus qu'aux institutions privées (ou inversement), mais si vous regardez vers l'Allemagne par exemple, avec le TÜV il n'y a en fait qu'une seule organisation vérificatrice, que ce soit sur la valeur de confiance des applications de messagerie ou concernant la quantité de pollution émise par les voitures. Et nous savons bien à quoi cela a mené !

Message codé

En t'aidant du code secret, déchiffre ce que Marine dit à son amie Sarah.

Code secret

a	b	c	d	e	f	g	h	i	j	k	l	m
☐	☆	∅	◻	⊞	○	∠	⊥	∩	>	←	▲	‡
n	o	p	q	r	s	t	u	v	w	x	y	z
⊖	∩	☒	↑	↓	∞	◀	∩	T	◌	⊞	◊	ℵ



Jeu gratuit à imprimer du site turbulus.com

La confiance

Quand vous décidez si vous faites confiance à un tiers, vous devez donc prendre en compte :

- la bienveillance : le tiers ne veut pas compromettre votre vie privée et/ou il est lui-même concerné
- la compétence : le tiers est techniquement capable de protéger votre vie privée et d'identifier et de corriger les problèmes

- l'intégrité : le tiers ne peut pas être acheté, corrompu ou infiltré par des services secrets ou d'autres tiers malveillants

Après les révélations de Snowden, il est évident que le public est le seul tiers qui peut remplir collectivement ces prérequis ; donc la mise à disposition publique du code source est cruciale. Cela écarte d'emblée WhatsApp, Google Allo et Threema.

« Attendez une minute... mais n'existe-t-il aucun autre moyen de vérifier que les données qui transitent sont bien chiffrées ? » Ah, bien sûr qu'il en existe, comme Threema [le fera remarquer](#), ou [d'autres personnes pour WhatsApp](#). Mais l'aspect important, c'est que le fournisseur de service contrôle l'application sur votre appareil, et peut intercepter les messages avant le chiffrement ou après le déchiffrement, ou simplement « voler » vos clés de chiffrement. « Je ne crois pas que X fasse une chose pareille. » Gardez bien à l'esprit que, même si vous faites confiance à Facebook ou Google (et vous ne devriez pas), pouvez-vous vraiment leur faire confiance pour ne pas obéir à des décisions de justice ? Si oui, alors pourquoi vouliez-vous du chiffrement de bout en bout ? « Quelqu'un s'en apercevrait, non ? » Difficile à dire ; s'ils le faisaient tout le temps, vous pourriez être capable de vous en apercevoir en analysant l'application. Mais peut-être qu'ils font simplement ceci :

```
si (listeDeSuspects.contient(utilisateurID))  
    envoyerClefSecreteAuServeur() ;
```

Alors seules quelques personnes sont affectées, et le comportement ne se manifeste jamais dans des « conditions de laboratoire ». Ou bien la génération de votre clé est trafiquée, de sorte qu'elle soit moins aléatoire, ou qu'elle adopte une forme plus facile à pirater. Il existe plusieurs approches, et la plupart peuvent facilement être déployées dans une mise à jour ultérieure, ou cachée parmi d'autres

fonctionnalités. Notez bien également qu'il est assez facile de se retrouver dans la liste de suspects, car le règlement actuel de la NSA assure de pouvoir y ajouter [plus de 25 000 personnes](#) pour chaque suspect « originel ».

À la lumière de ces informations, on comprend qu'il est très regrettable que Open Whisper Systems et Moxie Marlinspike (le célèbre auteur de Signal, mentionné précédemment) fassent publiquement les louanges de Facebook et de Google, augmentant ainsi la confiance en leurs applications [bien qu'il ne soit pas mauvais en soi qu'ils aient aidé à mettre en place le chiffrement, bien sûr]. Je suis assez confiant pour dire qu'ils ne peuvent pas exclure un des scénarios précédents, car ils n'ont pas vu le code source complet des applications, et ne savent pas non plus ce que vont contenir les mises à jour à l'avenir – et nous ne voudrions de toutes façons pas dépendre d'eux pour nous en assurer !

La messagerie Signal

« OK, j'ai compris. Je vais utiliser des logiciels libres et open source. Comme le Signal d'origine ». C'est là que ça se complique. Bien que le code source du logiciel client Signal soit libre/ouvert, il dépend d'autres composants non libres/fermés/propriétaires pour fonctionner. Ces composants ne sont pas essentiels au fonctionnement, mais ils (a) fournissent des métadonnées à Google (plus de détails sur les métadonnées plus loin) et (b) compromettent l'intégrité de votre appareil.

Le dernier point signifie que si même une petite partie de votre application n'est pas digne de confiance, alors le reste ne l'est pas non plus. C'est encore plus critique pour les composants qui ont des privilèges système, puisqu'ils peuvent faire tout et n'importe quoi sur votre téléphone. Et il est particulièrement impossible de faire confiance à ces composants non libres qui communiquent régulièrement des données à d'autres ordinateurs, comme ces services Google.

Certes, il est vrai que ces composants sont déjà inclus dans la plupart des téléphones Android dans le monde, et il est aussi vrai qu'il y a très peu d'appareils qui fonctionnent vraiment sans aucun composant non libre, donc de mon point de vue, ce n'est pas problématique en soi de les utiliser quand ils sont disponibles. Mais rendre leur utilisation obligatoire implique d'exclure les personnes qui ont besoin d'un niveau de sécurité supérieur (même s'ils sont disponibles !) ; ou qui utilisent des versions alternatives plus sécurisées d'Android, comme CopperheadOS ; ou simplement qui ont un téléphone sans ces services Google (très courant dans les pays en voie de développement). Au final, Signal crée un « effet réseau » qui dissuade d'améliorer la confiance globale d'un appareil mobile, parce qu'il punit les utilisateurs qui le font. Cela discrédite beaucoup de promesses faites par ses auteurs.

Et voici le pire : Open Whisper Systems, non seulement, ne supporte pas les systèmes complètement libres, mais a également menacé de prendre des mesures légales afin d'empêcher les développeurs indépendants de proposer une version modifiée de l'application client Signal qui fonctionnerait sans les composants propriétaires de Google et pourrait toujours interagir avec les autres utilisateurs de Signal ([1] [2] [3]). À cause de cela, des projets indépendants comme [LibreSignal](#) sont actuellement bloqués. En contradiction avec [leur licence libre](#), ils s'opposent à tout client du réseau qu'ils ne distribuent pas. De ce point de vue, l'application Signal est moins utilisable et moins fiable que par exemple **Telegram** qui [encourage les clients indépendants](#) à utiliser leurs serveurs et qui propose des [versions entièrement libres](#).

Juste pour que je ne donne pas de mauvaise impression : je ne crois pas qu'il y ait une sorte de conspiration entre Google et Moxie Marlinspike, et je les remercie de mettre au clair leur position de manière amicale (au moins dans leur dernière déclaration), mais je pense que la protection agressive de

leur marque et leur insistance à contrôler tous les logiciels clients de leur réseau met à mal la lutte globale pour des communications fiables.

Décentralisation, contrôle par les distributeurs et métadonnées

Un aspect important d'un réseau de communication est sa topologie, c'est-à-dire la façon dont le réseau est structuré. Comme le montre l'image ci-dessous, il y a plusieurs approches, toutes (plus ou moins) largement répandues. La section précédente concernait ce qui se passe sur votre téléphone, alors que celle-ci traite de ce qui se passe sur les serveurs, et du rôle qu'ils jouent. Il est important de noter que, même dans des réseaux centralisés, certaines communications ont lieu en pair-à-pair (c'est-à-dire sans passer par le centre) ; mais ce qui fait la différence, c'est qu'il nécessitent des serveurs centraux pour fonctionner.

Réseaux centralisés

Les réseaux centralisés sont les plus courants : toutes les applications mentionnées plus haut (WhatsApp, Telegram, Signal, Threema, Allo) reposent sur des réseaux centralisés. Bien que beaucoup de services Internet ont été décentralisés dans le passé, comme l'e-mail ou le World Wide Web, beaucoup de services centralisés ont vu le jour ces dernières années. On peut dire, par exemple, que Facebook est un service centralisé construit sur la structure WWW, à l'origine décentralisée.

Les réseaux centralisés font souvent partie d'une marque ou d'un produit plus global, présenté comme une seule solution (au problème des SMS, dans notre cas). Pour les entreprises qui vendent ou qui offrent ces solutions, cela présente l'avantage d'avoir un contrôle total sur le système, et de pouvoir le changer assez rapidement, pour offrir (ou imposer) de nouvelles fonctionnalités à tous les utilisateurs.

Même si l'on suppose que le service fournit un chiffrement de bout en bout, et même s'il existe une application cliente en logiciel libre, il reste toujours les problèmes suivants :

métadonnées : le contenu de vos messages est chiffré, mais l'information qui/quand/où est toujours accessible pour votre fournisseur de service

déni de service : le fournisseur de service ou votre gouvernement peuvent bloquer votre accès au service

Il y a également ce problème plus général : un service centralisé, géré par un fournisseur privé, peut décider quelles fonctionnalités ajouter, indépendamment du fait que ses utilisateurs les considèrent vraiment comme des fonctionnalités ou des « anti-fonctionnalités », par exemple en indiquant aux autres utilisateurs si vous êtes « en ligne » ou non. Certaines de ces fonctionnalités peuvent être supprimées de l'application sur votre téléphone si c'est du logiciel libre, mais d'autres sont liées à la structure centralisée. J'écrirai peut-être un jour un autre article sur ce sujet.

Métadonnées

Comme expliqué précédemment, les métadonnées sont toutes les données qui ne sont pas le message. On pourrait croire que ce ne sont pas des données importantes, mais [de récentes études](#) montrent l'inverse. Voici des exemples de ce qu'incluent les métadonnées : quand vous êtes en ligne, si votre téléphone a un accès internet, la date et l'heure d'envoi des messages et avec qui vous communiquez, une estimation grossière de la taille du message, votre adresse IP qui peut révéler assez précisément où vous vous trouvez (au travail, à la maison, hors de la ville, et cætera), éventuellement aussi des informations liées à la sécurité de votre appareil (le système d'exploitation, le modèle...). Ces informations sont une grande menace contre votre vie privée et les services secrets américains les utilisent réellement pour justifier des

meurtres ciblés (voir ci-dessus).

La quantité de métadonnées qu'un service centralisé peut voir dépend de leur implémentation précise. Par exemple, les discussions de groupe avec Signal et probablement Threema sont implémentées dans le client, donc en théorie le serveur n'est pas au courant. Cependant, le serveur a l'horodatage de vos communications et peut probablement les corrélérer. De nouveau, il est important de noter que si le fournisseur de service n'enregistre pas ces informations par défaut (certaines informations doivent être préservées, d'autres peuvent être supprimées immédiatement), il peut être forcé à enregistrer plus de données par des agences de renseignement. Signal (comme nous l'avons vu) ne fonctionne qu'avec des composants non-libres de Google ou Apple qui ont alors toujours une part de vos métadonnées, en particulier votre adresse IP (et donc votre position géographique) et la date à laquelle vous avez reçu des messages.

Pour plus d'informations sur les métadonnées, regardez [ici](#) ou [là](#).

Déni de service

Un autre inconvénient majeur des services centralisés est qu'ils peuvent décider de ne pas vous servir du tout s'ils le veulent ou qu'ils y sont contraints par la loi. Comme nombre de services demandent votre numéro lors de l'enregistrement et sont opérés depuis les États-Unis, ils peuvent vous refuser le service si vous êtes cubain par exemple. C'est particulièrement important puisqu'on parle de chiffrement qui est [grandement régulé](#) aux États-Unis.

L'Allemagne vient d'introduire [une nouvelle loi](#) antiterroriste dont une partie oblige à décliner son identité lors de l'achat d'une carte SIM, même prépayée. Bien que l'hypothèse soit peu probable, cela permettrait d'établir une liste noire de personnes et de faire pression sur les entreprises pour les

exclure du service.

Plutôt que de travailler en coopération avec les entreprises, un gouvernement mal intentionné peut bien sûr aussi cibler le service directement. Les services opérés depuis quelques serveurs centraux sont bien plus vulnérables à des blocages nationaux. C'est ce qui s'est passé pour [Signal](#) et [Telegram](#) en Chine.

Réseaux déconnectés

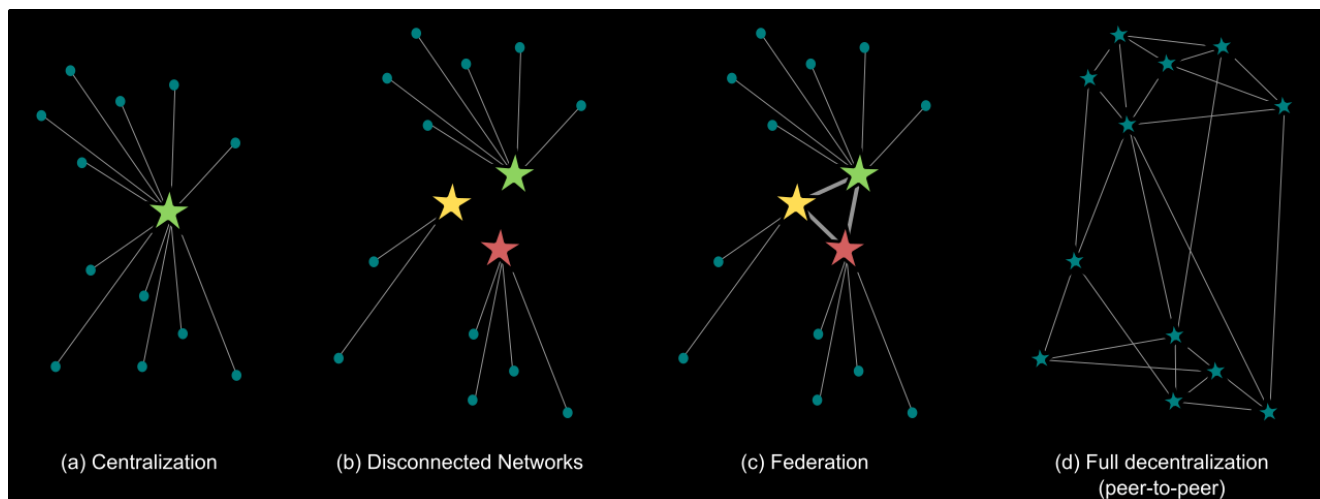
Lorsque le code source du serveur est libre, vous pouvez monter votre propre service si vous n'avez pas confiance dans le fournisseur. Ça ressemble à un gros avantage, et [Moxie Marlinspike le défend](#) ainsi :

Avant vous pouviez changer d'hébergeur, ou même décider d'utiliser votre propre serveur, maintenant les utilisateurs changent simplement de réseau complet. [...] Si un fournisseur centralisé avec une infrastructure ouverte modifiait affreusement ses conditions, ceux qui ne seraient pas d'accord ont le logiciel qu'il faut pour utiliser leur propre alternative à la place.

Et bien sûr, c'est toujours mieux que de ne pas avoir le choix, mais la valeur intrinsèque d'un réseau « social » vient des gens qui l'utilisent et ce n'est pas évident de changer si vous perdez le lien avec vos amis. C'est pour cela que les alternatives à Facebook ont tant de mal. Mme si elles étaient meilleures sur tous les aspects, elles n'ont pas vos amis.

Certes, c'est plus simple pour les applications mobiles qui identifient les gens via leur numéro, parce qu'au moins vous pouvez trouver vos amis rapidement sur un nouveau réseau, mais pour toutes les personnes non techniciennes, c'est très perturbant d'avoir 5 applications différentes juste pour rester en contact avec la plupart de ses amis, donc changer de réseau ne devrait qu'être un dernier recours.

Notez qu'OpenWhisperSystems se réclame de cette catégorie, mais en fait [ils ne publient que des parties](#) du code du serveur de Signal, de sorte que vous ne soyez pas capables de monter un serveur avec les mêmes fonctionnalités (plus précisément la partie téléphonie manque).



Centralisation, réseaux déconnectés, fédération, décentralisation en pair à pair

La fédération

La fédération est un concept qui résout le problème mentionné plus haut en permettant en plus aux fournisseurs de service de communiquer entre eux. Donc vous pouvez changer de fournisseur, et peut-être même d'application, tout en continuant à communiquer avec les personnes enregistrées sur votre ancien serveur. L'e-mail est un exemple typique d'un système fédéré : peu importe que vous soyez tom@gmail.com ou jeanne@yahoo.com ou même linda@serveur-dans-ma-cave.com, tout le monde peut parler avec tout le monde. Imaginez combien cela serait ridicule, si vous ne pouviez communiquer qu'avec les personnes qui utilisent le même fournisseur que vous ?

L'inconvénient, pour un développeur et/ou une entreprise, c'est de devoir définir publiquement les protocoles de communication, et comme le processus de standardisation peut être compliqué et très long, vous avez moins de flexibilité pour modifier le système. Je reconnais qu'il devient plus

difficile de rendre les bonnes fonctionnalités rapidement disponibles pour la plupart des gens, mais comme je l'ai dit plus haut, je pense que, d'un point de vue de la vie privée et de la sécurité, c'est vraiment une fonctionnalité, car plus de gens sont impliqués et plus cela diminue la possibilité pour le fournisseur d'imposer des fonctionnalités non souhaitées aux utilisateurs ; mais surtout car cela fait disparaître « l'effet d'enfermement ». Cerise sur le gâteau, ce type de réseau produit rapidement plusieurs implémentations du logiciel, à la fois pour l'application utilisateur et pour le logiciel serveur. Cela rend le système plus robuste face aux attaques et garantit que les failles ou les bugs présents dans un logiciel n'affectent pas le système dans son ensemble.

Et, bien sûr, comme évoqué précédemment, les métadonnées sont réparties entre plusieurs fournisseurs (ce qui rend plus difficile de tracer tous les utilisateurs à la fois), et vous pouvez choisir lequel aura les vôtres, voire mettre en place votre propre serveur. De plus, il devient très difficile de bloquer tous les fournisseurs, et vous pouvez en changer si l'un d'entre eux vous rejette (voir « Déni de service » ci-dessus).

Une remarque au passage : il faut bien préciser que la fédération n'impose pas que des métadonnées soient vues par votre fournisseur d'accès et celui de votre pair. Dans le cas de la messagerie électronique, cela représente beaucoup, mais ce n'est pas une nécessité pour la fédération par elle-même, c'est-à-dire qu'une structure fédérée bien conçue peut éviter de partager les métadonnées dans les échanges entre fournisseurs d'accès, si l'on excepte le fait qu'il existe un compte utilisateur avec un certain identifiant sur le serveur.



XMPP

Alors est-ce qu'il existe un système identique pour la messagerie instantanée et les SMS ? Oui, ça existe, et ça s'appelle [XMPP](#). Alors qu'initialement ce protocole n'incluait pas de chiffrement fort, maintenant on y trouve un chiffrement du même [niveau de sécurité que pour Signal](#). Il existe aussi de très bonnes applications pour mobile sous Android (« [Conversations](#) ») et sous iOS (« [ChatSecure](#) »), et pour d'autres plateformes dans le monde également.

Inconvénients ? Comme pour la messagerie électronique, il faut d'abord vous enregistrer pour créer un compte quelque part et il n'existe aucune association automatique avec les numéros de téléphone, vous devez donc convaincre vos amis d'utiliser ce chouette nouveau programme, mais aussi trouver quels fournisseur d'accès et nom d'utilisateur ils ont choisis. L'absence de lien avec le numéro de téléphone peut être considérée par certains comme une fonctionnalité intéressante, mais pour remplacer les SMS ça ne fait pas l'affaire.

La solution : [Kontalk](#), un client de messagerie qui repose sur XMPP et qui automatise les contacts via votre carnet d'adresses. Malheureusement, cette application n'est pas encore aussi avancée que d'autres mentionnées plus haut. Par exemple, il lui manque la gestion des groupes de discussion et la compatibilité avec iOS. Mais Kontalk est une preuve tangible qu'il est possible d'avoir avec XMPP les mêmes fonctionnalités que l'on trouve avec WhatsApp ou Telegram. Selon moi, donc, ce n'est qu'une question de temps avant que ces solutions fédérées ne soient au même niveau et d'une ergonomie équivalente. [Certains](#) partagent ce point de vue, [d'autres](#) non.

Réseaux pair à pair

Les réseaux pair à pair éliminent complètement le serveur et par conséquent toute concentration centralisée de métadonnées. Ce type de réseaux est sans égal en termes de liberté et il est pratiquement impossible à bloquer par une autorité. [ToX](#) est un exemple d'application pair à pair, ou encore [Ricochet](#) (pas pour mobile cependant), et il existe aussi [Briar](#) qui est encore en cours de développement, mais ajoute l'anonymat, de sorte que même votre pair ne connaît pas votre adresse IP. Malheureusement il existe des problèmes de principe liés aux appareils mobiles qui rendent difficile de maintenir les nombreuses connexions que demandent ces réseaux. De plus il semble impossible pour le moment d'associer un numéro de téléphone à un utilisateur, si bien qu'il est impossible d'avoir recours à la détection automatique des contacts.

Je ne crois pas actuellement qu'il soit possible que ce genre d'applications prenne des parts de marché à WhatsApp, mais elles peuvent être utiles dans certains cas, en particulier si vous êtes la cible de la surveillance et/ou membre d'un groupe qui décide collectivement de passer à ces applications pour communiquer, une organisation politique par exemple.

En deux mots

- La confidentialité de nos données privées est l'objet d'un intérêt accru et les utilisateurs cherchent activement à se protéger mieux.
- On peut considérer que c'est un bon signe quand les distributeurs principaux de logiciels comprennent qu'ils doivent réagir à cette situation en ajoutant du chiffrement à leurs logiciels ; et qui sait, il est possible que ça complique un peu la tâche de la NSA.
- Toutefois, il n'y a aucune raison de leur faire plus confiance qu'auparavant, puisqu'il n'existe aucun moyen à notre disposition pour savoir ce que font véritablement les applications, et parce qu'il leur reste beaucoup de façons de nous espionner.
- Si en ce moment vous utilisez WhatsApp, Skype, Threema ou Allo et que vous souhaitez avoir une expérience comparable, vous pouvez envisager de passer à Telegram ou Signal. Ils valent mieux que les précédents (pour diverses raisons), mais ils sont loin d'être parfaits, comme je l'ai montré. Nous avons besoin à moyen et long terme d'une fédération.
- Même s'ils nous paraissent des gens sympas et des hackers surdoués, nous ne pouvons faire confiance à OpenWhisperSystem pour nous délivrer de la surveillance, car ils sont aveugles à certains problèmes et pas très ouverts à la coopération avec la communauté.
- Des trucs assez sympas se préparent du côté du XMPP, surveillez Conversations, chatSecure et Kontalk. Si vous le pouvez, soutenez-les avec du code, des dons et des messages amicaux.
- Si vous souhaitez une approche sans aucune métadonnée et/ou anonymat, essayez Tor ou ToX, ou attendez Briar.

La surveillance, vigile de la paix sociale au service des plus riches ?

[Cory Doctorow](#), auteur de science-fiction canadien et américain, cofondateur du site [boing-boing](#), est l'un de ces monstres sacrés du monde du logiciel libre, du partage de la connaissance, bref, de l'époque qu'Internet profile à l'horizon des historiens du futur. Dans le dernier numéro de LocusMag, journal de science-fiction en langue anglaise, il évoque avec son habituelle précision deux sujets qui me sont chers : la stabilité de nos sociétés et la surveillance des populations. Sur l'instabilité de nos sociétés, j'évoque souvent la complexité croissante du droit, Cory va ici beaucoup plus loin. Sur la surveillance de masse, on compare souvent à tort la NSA et la Stasi d'ex-RDA, à nouveau Doctorow enfonce le clou et nous pousse dans nos derniers retranchements, invitant à mots couverts à une révolution du partage et de l'égalité.

Espérant que vous aurez autant de plaisir à le lire que nous avons eu à le traduire, et remerciant Cory d'[avoir accepté](#) la traduction en français de cet article, nous vous invitons au débat...

Benjamin Sonntag

Co-fondateur de la Quadrature du Net

Stabilité et surveillance



par **Cory Doctorow**

article original publié initialement dans le numéro de [mars 2015 du magazine Locus](#)

Traduction collaborative : Benjamin, catalaburro, bruno, Monsieur Tino, goofy, TeSla, Jerry + anonymes

Dans le best-seller économique de Thomas Piketty, paru en 2014, [Le capital au XXI^e siècle](#), l'économiste documente avec soin l'augmentation des inégalités dans le monde, phénomène qui a inspiré le printemps arabe, le mouvement *Occupy*, le Pape François, et de nombreux militants politiques sur toute la planète. Certains critiques de Piketty ont commencé par remettre ses calculs en question, mais sur ce point Piketty semble crédible. L'ensemble de données sur lesquelles il s'est fondé représente un travail de titan, et les données brutes sont en ligne, chacun peut les télécharger, ainsi que les nombreuses notes sur les suppositions et normalisations de données disparates que Piketty a effectuées afin d'obtenir une histoire cohérente. Piketty est l'analyste des analystes, un homme aux chiffres totalement crédibles.

Ensuite vient l'autre critique adressée à Piketty : le « et

alors ? ». *Les riches deviennent plus riches et les pauvres plus pauvres ? Et alors ?* Comme le raille Boris Johnson, le maire de Londres issu d'Eton : « Plus vous secouez le paquet, plus il sera facile à certains cornflakes de remonter à la surface. » En d'autres termes, si le capitalisme rend les riches plus riches, c'est parce qu'ils le méritent, un fait démontré par l'ampleur de leur richesse. Si vous êtes une miette au fond de la boîte, vous devez sûrement être nul quelque part.

Piketty ne répond pas à cette critique de manière directe, mais par des références à « l'instabilité sociale ». Il compare fréquemment les inégalités contemporaines avec celles de la veille de la première guerre mondiale (présentée comme une sorte de guerre commerciale entre les super-riches pour savoir qui empochera les richesses des colonies, dès lors qu'il n'y avait plus de nouveau territoire à conquérir) ; il les compare également à celles qui ont précédé la Révolution Française, une comparaison qui va faire hurler les citoyens français, mais paraîtra plus lointaine au lectorat anglais de ce livre.

Voici ce qu'il dit, lorsqu'on lit entre les lignes : quand le fossé entre riches et pauvres devient trop important, les pauvres se mettent à construire des guillotines. Il revient probablement moins cher de redistribuer une partie de votre fortune, méritée ou non, que de payer tous les gardes qui pourraient s'avérer nécessaires pour éviter de vous faire couper la tête.

En d'autres mots, un grand fossé entre riches et pauvres déstabilise les sociétés, et il est compliqué d'être vraiment riche dans une société en proie au chaos. À moins que la population n'adhère au système qui vous a rendu riche, le peuple ne sera pas gêné par le spectacle du pillage de vos biens, et pourrait même y contribuer.

Historiquement ont existé deux modèles de société très

stables : celles qui sont fortement redistributives, tels les pays scandinaves (où l'écart entre les plus riches et les plus pauvres est comblé par les impôts, les lois protectrices des employés et des locataires et des politiques sociales étendues) ; et d'autre part les sociétés totalitaires, comme l'Irak de Saddam Hussein ou la Lybie de Muammar Kadhafi où, au lieu de redistribuer leurs richesses au reste de la population, les élites dirigeantes dépensent au fond moins d'argent pour s'offrir un vaste dispositif répressif composé de soldats, d'espions, d'officiers de police, de mouchards, de propagande et de surveillance. Tout cela est utilisé pour identifier les protestataires qui réclament des changements politiques, puis pour les neutraliser : emprisonnement, diffamation, mise à l'écart du marché du travail, exil, chantage, torture et enfin assassinat.

Samuel Bowles, un économiste du Santa Fe Institute, utilise le terme « travail de protection » [NDT : proposition de traduction pour *guard labor*, voir [cet article](#)] pour décrire toutes les activités destinées à contraindre à la paix sociale les personnes émettant des réserves sur la légitimité d'une société. Faute d'un cadre éthique proclamant que la pauvreté et les souffrances qu'elle provoque doivent être combattues, une élite éclairée devrait chercher à utiliser une combinaison de la redistribution des richesses et du travail de protection pour assurer la stabilité sociale. Si une infime minorité de la société est assez riche, et que tout le reste est assez pauvre, il sera plus coûteux pour la riche minorité d'engager des gardes pour maintenir les masses affamées à l'écart de leurs palais que de nourrir et d'éduquer une partie de la masse, ce qui crée une classe moyenne, une certaine mobilité sociale, ainsi que le sentiment que les riches sont riches parce qu'ils l'ont mérité. Et si vous jouez le jeu, vous pourriez bien en être.

Il en existe des quantités d'exemples, mais mon préféré reste Joseph Williamson, qui a payé pour le creusement de tunnels

sous Liverpool après la Première Guerre Mondiale. Williamson était un magnat local qui avait compris que le retour des *Tommies* traumatisés par l'enfer des tranchées, dans une ville où aucun travail ne les attendait, était probablement une mauvaise nouvelle pour la stabilité de la cité. Williamson utilisa donc une part de sa colossale fortune pour engager les vétérans pour trouser le sol sous Liverpool tel un gruyère, avec des kilomètres et des kilomètres de tunnels ne débouchant sur rien. Le raisonnement – probablement sensé – de Williamson était qu'il était moins coûteux de donner à ces vétérans un salaire et la dignité de travailler plutôt que d'engager des gardes pour se défendre de ces soldats démobilisés qui se sentaient abandonnés par leur patrie.

Tous les emplois de protection ne sont pas forcément coercitifs. Certains jouent sur la persuasion. L'accroissement soudain de la disparité des richesses de l'ère post-Reagan a aussi coïncidé avec la dérégulation des médias de masse, à la fois en termes de renforcement de la propriété et pour l'étendue et la nature des obligations qui incombent aux services publics de programmes, associées à leur licence de diffusion. Il en a résulté une gigantesque révolution économique et technologique dans le monde des médias, qui s'est achevée par la création de cinq énormes empires médiatiques qui détiennent virtuellement à l'échelle du globe toutes les musiques, les films, la diffusion des nouvelles, la presse écrite, l'édition, les câbles et les satellites, et même, dans de nombreux cas, ces entreprises possèdent aussi les tuyaux – ceux du téléphone et du câble.

Cette révolution a rendu plus facile que jamais la diffusion de messages socialement apaisants. De très nombreuses études, l'une après l'autre, ont montré que la presse était favorable au mythe des riches méritants, assimilait les impôts à du vol et se montrait hostile au travail et à la réglementation. L'ascension de Fox News et de son équivalent planétaire Sky News, comme l'effondrement de l'industrie de la presse écrite

tombée aux mains de quelques entreprises largement sous la coupe de fonds de pension et de milliardaires, nous a poussés dans une situation où les thèses qui remettent en question la légitimité des grandes fortunes ont une bien faible visibilité.

À la fin du XX^e siècle, la révolution des télécoms et des médias a abaissé le coût du travail de protection, modifiant l'équilibre entre la redistribution et le maintien de la stabilité sociale. Quand il devient moins coûteux de protéger votre fortune, vous pouvez vous permettre d'envoyer paître davantage de gens en devenant de plus en plus riche au lieu de partager avec eux.

Le XXI^e siècle a été très bienveillant pour le travail de protection. En plus d'avoir permis aux polices locales l'obtention d'armes militaires, le XXI^e siècle a vu l'émergence d'Internet et, grâce au manque de régulation, l'émergence d'un petit nombre de géants d'Internet qui savent presque tout ce que fait chacune des 7 milliards de personnes sur terre.

La surveillance massive d'Internet révélée par le lanceur d'alerte Edward Snowden montre que les gouvernements – et les riches qui dominent les cercles politiques en proportion directe du volume de richesse nationale dont ils disposent – ont remarqué que la seule chose dont ils aient besoin pour mettre la terre entière sous surveillance est de corrompre ces géants de l'Internet, que ce soit ouvertement (comme quand l'agence d'espionnage britannique GCHQ paye British Telecom pour pouvoir mettre sur écoute les fibres optiques qui sont sur le territoire britannique) ou secrètement (comme quand la NSA a secrètement mis sur écoute les fibres optiques entre les centres de données informatique utilisés par Google, Yahoo et Facebook).

Il est difficile d'exagérer l'efficacité de la surveillance au XXI^e siècle. Les opposants à la surveillance de masse

d'Internet aiment comparer la NSA et ses alliés à la Stasi, la police secrète de l'ex-RDA, connue pour son omniprésence dans le quotidien des gens et la surveillance totale dont elle étouffait le pays. Mais la Stasi opérait dans une surveillance *pré-Internet*, et selon les critères d'aujourd'hui, leur travail de surveillance était extrêmement coûteux.

En 1989, qui fut la dernière année d'activité de la Stasi, il y avait 16 111 000 habitants en Allemagne de l'Est, et 264 096 opérateurs qui d'une manière ou d'une autre étaient rémunérés par la Stasi, dont 173 000 « informateurs officieux » (des mouchards). Ce qui faisait une proportion d'un espion pour 60 personnes.

Il est difficile de savoir avec précision combien de personnes travaillent pour la NSA – une majeure partie de son budget est inconnue, et de nombreuses opérations sont menées par des partenaires privés comme Booz Allen, l'ancien employeur d'Edward Snowden. Mais nous savons combien d'Américains ont une habilitation de sécurité (4,9 millions), et combien sont habilités « Top Secret » (1,4 millions), ce qui fait que nous pouvons être sûrs que moins de 1,4 millions de personnes travaillent sur ces sujets (parce que ces personnes, avec des habilitations « Top Secret », se trouvent réparties entre la CIA, le FBI, la défense fédérale, etc.). De plus, la surveillance menée par la NSA est épaulée par des espions étrangers, en particulier ceux des pays dits des « [*five eyes*](#) » (Canada, Royaume-Uni, Australie et Nouvelle-Zélande [NdT, en plus des États-Unis]), mais ils ne sont qu'une goutte d'eau dans l'océan comparée au dispositif de surveillance américain – les États-Unis représentent à eux seuls un tiers des dépenses mondiales dans le domaine militaire, quand seulement deux autres pays des *five eyes* (le Royaume-Uni et l'Australie) apparaissent dans les 15 pays aux plus fortes dépenses militaires.

En prenant une estimation large, nous pouvons dire qu'il y a 1,4 million d'espions travaillant pour la NSA et ses associés,

five eyes compris. 1,4 millions de personnes pour surveiller sept milliards d'humains.

Ceci nous donne un ratio espion/sujet d'environ 1/5000, deux ordres de grandeurs de plus qu'à l'époque de l'activité de la Stasi. Celle-ci utilisait une armée pour surveiller un pays ; la NSA utilise un bataillon pour surveiller la planète. Par rapport à la NSA, la Stasi fait figure de bricoleurs du dimanche.

Bien qu'il soit admis que l'arsenal de surveillance américain s'est beaucoup étoffé depuis la présidence Reagan – certaines agences ont vu leurs budgets multipliés par quatre depuis la chute du Mur de Berlin – il n'a certainement pas été centuplé. Même en ne disposant que de budgets obscurs et mensongers, il est évident que l'augmentation géométrique du volume d'espionnage ne s'est accompagné que d'une augmentation linéaire des coûts associés.

En d'autres termes, le coût des éléments clés du travail de protection est en chute libre depuis l'avènement d'Internet. Nous voici revenus à Piketty et à la stabilité sociale. Les riches ont besoin de stabilité, du moins suffisamment pour que leurs banques et leur business continuent de tourner rond.

Les écarts de richesse déstabilisent la société ; pour retrouver retrouver la stabilité il faut faire un choix : ou bien on paie le prix pour faire sortir les gens de la pauvreté, ou bien on s'assure qu'on a une longueur d'avance sur eux avant qu'ils ne ressortent les guillotines (ou qu'ils abattent le Mur de Berlin). Lorsque le coût du travail de protection diminue, le fossé acceptable entre les riches et les pauvres s'élargit. Une baisse de deux ordres de grandeur du coût nécessaire pour maintenir séparés les loups et les moutons chez les pauvres est un puissant argument contre les programmes sociaux, ou les lois sur le travail, ou les droits des locataires. Bien entendu, la privation rend les populations agitées, mais il est possible, avec une fiabilité incroyable et pour seulement quelques sous, d'identifier les

personnes à arrêter, discréditer, faire chanter, ou neutraliser : « Qu'ils consomment des réseaux sociaux ! »

Ce sont de mauvaises nouvelles, car la grande disparité des richesses ne déstabilise pas la société uniquement à cause de la pauvreté, cela la déstabilise aussi à cause de la corruption. Dans une société où les juristes doivent lever des dizaines de millions de dollars pour s'installer et exercer, l'influence des riches grandit. Les régimes autocratiques en sont un bon exemple : vous pouvez aller en prison en Thaïlande pour avoir critiqué le Roi, et dénoncer les conditions de travail esclavagistes au Qatar est un délit.

Mais c'est aussi vrai aux États-Unis. En avril 2014, des universitaires de Princeton et Northwestern ont publié *Test des théories des politiques américains : élites, groupes d'intérêts, et citoyens de base* (1), dans la revue *Perspectives and Politics*. Il s'agissait d'une étude massive de plus de 20 années de combats politiques au sein du Congrès américain et de l'administration, et sa conclusion était que l'issue de ces combats politiques était immanquablement favorable aux 10% des Américains les plus riches. Les décisions politiques favorables aux classes moyennes étaient si rares qu'elle ne dépassaient même pas le niveau de bruit statistique.

L'augmentation de la surveillance implique que les mécanismes de combat contre les inégalités, déjà insuffisants, ont été détournés au profit d'une oligarchie.

Dans une société extrêmement inégalitaire, les seuls projets qui peuvent se développer doivent avoir un vrai modèle économique. Ils doivent rendre riche une personne extérieure au Parlement, pour qu'elle utilise cet argent à influencer les hommes politiques qui vont maintenir et propager ce projet politique.

Il est possible que certaines mesures prises par les États

génèrent un surplus de capital pour un nombre restreint de personnes mais demeurent bénéfiques à la société, cependant il y a d'autres domaines où ce n'est sûrement pas le cas. L'éducation, par exemple : vous pouvez tout à fait diriger une école comme une entreprise, ne jurer que par sa « rentabilité », avec des tests standardisés et une surveillance des taux d'absentéisme, plutôt que par le jugement des enseignants, ou les résultats effectifs des apprentissages.

En utilisant cette méthodologie, vous pouvez assurer de confortables profits aux entreprises qui ont compris comment améliorer artificiellement les résultats des tests standardisés, et comment réduire l'absentéisme. Par exemple, en bourrant le crâne des étudiants avec des tests, au lieu de leur enseigner les arts ou le sport, et en mettant à la porte les étudiants qui ont des problèmes avec ces méthodes, ou ceux dont des problèmes personnels leur font manquer de nombreux cours. Cela augmentera encore vos résultats trimestriels d'une façon qui réchaufferait le cœur d'un analyste de Wall Street, mais bonne chance pour trouver quelqu'un avec une certaine crédibilité pédagogique qui pourra prétendre que ces enfants « apprennent ».

Alors voilà, avec les copains on voudrait
un modèle social réellement participatif
avec un revenu de base garanti pour assurer à chacun
les conditions d'une vie citoyenne digne
et puis la monnaie faudrait...



Je réagis comme vous : ça me fait flipper. L'augmentation de la surveillance implique que les mécanismes de combat contre les inégalités, déjà insuffisants, ont été détournés au profit d'une oligarchie. C'est une bonne raison pour inciter vos amis à utiliser des outils de chiffrement, particulièrement ceux qui sont disponibles en logiciel libre et *open source*. À l'heure où j'écris ces lignes, en janvier 2015, Obama, l'Avocat général de New York et le patron du FBI ont appelé à l'interdiction de la cryptographie pour le grand public, avec le soutien du Premier Ministre britannique David Cameron. Interdire la cryptographie est un projet ambitieux qui ne risque pas de se concrétiser (il combine les aspects les plus idiots de la guerre contre certaines drogues et ceux de la guerre contre le partage de fichiers), mais cela ne veut pas dire que cette volonté de nous rendre tous vulnérables à la surveillance ne fera pas de mal.

Le temps passe. Il est bientôt minuit. Avez-vous chiffré votre disque dur ?

Note

(1) Lien direct vers le PDF en anglais : [Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens](#)

Crédit photo

* Cory Doctorow par [Joi Ito](#) (CC BY 2.0)