Décodons le discours anti-chiffrement

La secrétaire d'État à l'Intérieur du Royaume-Uni demandait fin juillet aux entreprises du numérique de renoncer au chiffrement de bout en bout. Aral Balkan a vivement réagi à ses propos.

L'intérêt de son analyse sans concessions n'est ni anecdotique ni limité au Royaume-Uni. Il s'agit bien de décoder le discours contre le chiffrement dont on abreuve les médias majeurs, que ce soit outre-Manche ou ici même en France, comme presque partout ailleurs en Europe. Un discours qui repose sur le terrorisme comme épouvantail et sur Internet comme bouc-émissaire. Alors que s'empilent des lois répressives qui rendent légale une surveillance de tous de plus en plus intrusive, sans pour autant hélas éradiquer le terrorisme, il est urgent de dénoncer avec force et publiquement la manipulation des esprits par le discours sécuritaire. Il en va de notre liberté.

Ce travail qu'assument courageusement des associations comme la Quadrature du Net et que nous devons tous soutenir est ici plutôt bien mené par Aral Balkan qui « traduit » les déclarations de la ministre pour ce qu'elles signifient réellement : l'appel à la collusion entre le capitalisme de surveillance et le contrôle étatique de la vie de chacun.

Article original paru sur le blog d'Aral Balkan : Decrypting Amber Rudd
Traduction Framalang : hello, mo, FranBAG, goofy, Éric, Bromind, Lumibd, audionuma, karlmo, Todd

[EDIT] Décidément Amber Rudd est toujours prête à récidiver, comme le montre ce tout récent article de Numérama

où elle déclare en substance qu'elle n'a pas besoin de connaître les technologies comme le chiffrement pour… les interdire !

Amber Rudd entre les lignes

par Aral Balkan

Facebook, Microsoft, Twitter et YouTube (Google/Alphabet, Inc) viennent de créer le Forum Internet Global Contre le Terrorisme et Amber Rudd, la ministre de l'Intérieur britannique, leur demande de renoncer discrètement à assurer le chiffrement de bout en bout de leurs produits. Ne croyez plus un traître mot de ce que ces entreprises racontent sur le chiffrement de bout en bout ou le respect de la vie privée sur leurs plateformes.
PS : WhatsApp appartient à Facebook.

Amber Rudd : « les discussions entre les entreprises IT et le gouvernement… doivent rester confidentielles. » Crédit photo : *The Independent*

Ruddement fouineuse

La tribune sur le chiffrement qu'Amber Rudd a fait paraître dans le *Telegraph* (article en anglais, payant) est tellement tordue qu'elle a de quoi donner le vertige à une boule de billard. Il est évident que Rudd (célèbre pour avoir un jour confondu le concept cryptographique de hachage avec les hashtags) est tout sauf naïve sur ce sujet. Elle est mal intentionnée.

Ce n'est pas qu'elle ne comprenne pas les maths ou le fonctionnement de la cryptographie. C'est plutôt qu'elle (et le gouvernement britannique avec elle) est déterminée à priver les citoyens britanniques du droit humain fondamental à la protection de la vie privée et qu'elle cherche à mettre en place un État surveillance. Ce n'est malheureusement pas un cas isolé, comme en témoignent

les récentes déclarations de Theresa May, de la Chancelière allemande Angela Merkel et d'Emmanuel Macron en faveur d'une régulation similaire à l'échelle européenne, voire mondiale.

Étant donné l'importance de ce qui est en jeu (rien moins que l'intégrité de la personne à l'ère numérique et l'avenir de la démocratie en Europe), je voudrais prendre un moment pour disséquer son article et y répondre point par point.

Petit spoiler pour ceux qui manquent de temps : la partie la plus inquiétante de son article est la deuxième, dans laquelle elle révèle qu'elle a créé le Forum Internet Global Contre le Terrorisme avec Facebook, Microsoft, Twitter et YouTube (Google/Alphabet, Inc.), et qu'elle leur a demandé de supprimer le chiffrement de bout en bout de leurs produits (souvenez vous que c'est Facebook qui détient WhatsApp) sans prévenir personne. Cela a de graves conséquences sur ce que l'on peut attendre de la protection contre la surveillance étatique sur ces plateformes. Si vous n'avez pas le temps de tout lire, n'hésitez pas à sauter directement à la partie II.

Partie I : entente public-privé ; surveillance de masse et contrôle traditionnel.

Amber commence par poser une équivalence entre la lutte contre la propagande publique en ligne des organisations terroristes et la nécessité d'accéder aux communications privées de la population dans son ensemble. Elle prône aussi la surveillance de masse, dont nous savons qu'elle est inefficace, et reste étrangement silencieuse sur la police de proximité, dont nous savons qu'elle est efficace.

> **Rudd** : *Nous ne cherchons pas à interdire le chiffrement, mais si nous sommes dans l'impossibilité de voir ce que préparent les terroristes, cela met en danger notre sécurité.*

Traduction : Nous voulons interdire le chiffrement parce que si nous le faisons nous serons mieux armés pour attraper les terroristes.

Par où commencer ? Faut-il rappeler qu'on court plus de risques de mourir en tombant de son lit qu'en tombant sur un terroriste ? Ou que la surveillance de masse (ce que Rudd demande) est totalement inapte à enrayer le terrorisme ? (Après tout, quand on cherche une aiguille, une plus grosse botte de foin est la dernière chose dont on ait besoin.)

Voici ce qu'en pense Bruce Schneier, un expert reconnu en cryptologie :

> *En raison de la très faible occurrence des attaques terroristes, les faux positifs submergent complètement le système, quel qu'en soit le degré de précision. Et quand je dis « complètement », je n'exagère pas : pour chacun des complots terroristes détectés par le système, si tant est qu'il en découvre jamais, des millions de gens seront accusés à tort.*

Si vous n'êtes toujours pas convaincu et pensez que le gouvernement britannique devrait avoir le droit d'espionner tout un chacun, ne vous inquiétez pas : il le fait déjà. Il a le pouvoir de contraindre les entreprises IT à introduire des portes dérobées dans tous les moyens de communication grâce à l'Investigatory Powers Act (d'abord connu sous le nom de projet de loi IP et plus familièrement appelé charte des fouineurs). Peut-être n'avez-vous jamais entendu parler de cette loi car elle est passée relativement inaperçue et n'a pas suscité d'opposition dans les rangs du parti travailliste.

Toujours est-il que vos droits sont déjà passés à la trappe. Amber Rudd s'occupe maintenant de désamorcer vos réactions pour le jour où ils décideront d'appliquer les droits qu'ils ont déjà.

> **Rudd** : *Les terribles attentats terroristes de cette année confirment que les terroristes utilisent les plateformes Internet pour répandre leur détestable idéologie et planifier des attaques.*

Traduction : Nous voulons faire d'internet un bouc émissaire, en faire la source de nos problèmes avec le terrorisme.

Internet n'est pas la cause sous-jacente du terrorisme. Selon Emily Dreyfuss dans *Wired*, « les experts s'accordent à dire que l'internet ne génère pas de terrorisme et contribue même assez peu aux phénomènes de radicalisation. »

Emily explique :

Les chercheurs spécialisés dans le terrorisme ont remarqué que la violence en Europe et au Royaume-Uni suit un schéma classique. Cela peut donner des clés aux gouvernements pour contrer le problème, à condition d'allouer les crédits et les ressources là où ils sont le plus utiles. La plupart des djihadistes européens sont de jeunes musulmans, souvent masculins, vivant dans des quartiers pauvres défavorisés où le taux de chômage est élevé. Ils sont souvent de la deuxième ou troisième génération de migrants, issus de pays où ils n'ont jamais vécu ; ils ne sont pas bien intégrés dans la société ; quand ils ne sont pas au chômage, leur niveau d'éducation est faible. Leurs vies sont dépourvues de sens, de but.

Rudd déroule son argument :

> **Rudd** *: Le numérique est présent dans quasi tous les complots que nous mettons au jour. En ligne, vous pouvez trouver en un clic de souris votre propre set du « parfait petit djihadiste. » Les recruteurs de Daesh (État islamique) déploient leurs tentacules jusque dans les ordinateurs portables des chambres de garçons (et, de plus en plus souvent, celles des filles), dans nos villes et nos cités, d'un bout à l'autre du pays. Les fournisseurs d'extrémisme de droite abreuvent la planète de leur marque de haine sans jamais avoir à sortir de chez eux.*

Tous les exemples qui précèdent concernent des *informations publiques* librement accessibles en ligne. Pas besoin de portes dérobées, pas besoin de fragiliser le chiffrement pour que les services judiciaires y aient accès. Tout l'intérêt, justement, c'est qu'elles soient faciles à trouver et à lire. La propagande n'aurait pas beaucoup d'intérêt si elle restait cachée.

> ***Rudd*** *: On ne saurait sous-estimer l'ampleur du phénomène.*

Traduction : Il est impossible d'exagérer davantage l'ampleur du phénomène.

Vous vous souvenez qu'on court davantage de risques de mourir en tombant de son lit qu'en tombant aux mains d'un terroriste ? Tout est dit.

> ***Rudd*** *: Avant d'abattre des innocents sur Westminster Bridge et de poignarder l'agent de police Keith Palmer, Khalid Masood aurait regardé des vidéos extrémistes.*

Premièrement, l'article du *Telegraph* dont Amber Rudd fournit le lien ne fait nulle part mention de vidéos extrémistes que Khalid Masood aurait regardées (que ce soit en ligne, sur le Web, grâce à un quelconque service chiffré, ni où que ce soit d'autre). Peut-être Rudd s'imaginait-elle que personne ne le lirait pour vérifier. À vrai dire, en cherchant sur le Web, je n'ai pas pu trouver un seul article qui mentionne des vidéos extrémistes visionnées par Khalid Massood. Et même si c'était le cas, ce ne serait qu'un exemple de plus de contenu public auquel le gouvernement a accès sans l'aide de portes dérobées et sans compromettre le chiffrement.

Ce que j'ai découvert, en revanche, c'est que Masood « était dans le collimateur du MI5 pour « extrémisme violent », mais n'était pas considéré comme une menace par les services de sécurité. » Voici donc un exemple parfait s'il en est : l'érosion des droits de tout un chacun dans notre société, sous l'effet de la surveillance de masse, n'aurait en rien contribué à son arrestation. Les services de renseignement le connaissaient déjà, mais ne le jugeaient pas menaçant.

Et ce n'est pas la première fois. D'après un article publié en 2015 dans *The Conversation* :

> *On se heurte régulièrement au problème de l'analyse et de la hiérarchisation des informations déjà amassées. Il n'est plus rare d'apprendre qu'un terroriste était déjà connu des services de police et de renseignement. C'était le cas des kamikazes du 7 juillet 2005 à Londres, Mohammed Siddique Khan et Shezhad Tanweer, et de certains des présumés coupables des attentats de Paris, Brahim Abdeslam, Omar Ismail Mostefai et Samy Amimour.*

Plus récemment, les cinq terroristes qui ont perpétré les attentats de Londres et Manchester étaient tous « connus de la police ou des services de sécurité. » L'un d'entre eux apparaissait dans un documentaire de Channel 4 où il déployait un drapeau de l'État islamique. On nous rebat les oreilles de l'expression « passé à travers les mailles du filet. » Peut-être devrions-nous nous occuper de resserrer les mailles du filet et de mettre au point de meilleures méthodes pour examiner ce qu'il contient au lieu de chercher à fabriquer un plus grand filet.

> **Rudd** *: Daesh prétend avoir ouvert 11000 nouveaux comptes sur les réseaux sociaux durant le seul mois de mai dernier. Notre analyse montre que trois quarts des récits de propagande de Daesh sont partagés dans les trois heures*

> *qui suivent leur publication – une heure de moins qu'il y a un an.*

Une fois encore, ce sont des comptes publics. Utilisés à des fins de propagande. Les messages ne sont pas chiffrés et les portes dérobées ne seraient d'aucun secours.

> **Rudd** *: Souvent, les terroristes trouvent leur public avant que nous ayons le temps de réagir.*

Alors cessez de sabrer les budgets de la police locale. Investissez dans la police de proximité – dont on sait qu'elle obtient des résultats – et vous aurez une chance de changer la donne. Ce n'est pas le chiffrement qui pose problème en l'occurrence, mais bien la politique d'austérité délétère de votre gouvernement qui a plongé les forces de police locales dans un « état critique » :

> *Les forces de l'ordre ont du mal à gérer le nombre de suspects recherchés. Le HMIC (NDLT : police des polices anglaise) s'est rendu compte que 67000 suspects recherchés n'avaient pas été enregistrés dans le PNC (Police National Computer, le fichier national de la police). En outre, à la date d'août 2017, le PNC comptait 45960 suspects, où figurent pêle-mêle ceux qui sont recherchés pour* ***terrorisme****, pour meurtre et pour viol.*

Au lieu de se concentrer là-dessus, Amber cherche à détourner notre attention sur le Grand Méchant Internet. Quand on parle du loup…

> **Rudd** *: L'ennemi connecté est rapide. Il est impitoyable. Il cible les faibles et les laissés-pour-compte. Il utilise le meilleur de l'innovation à des fins on ne peut plus maléfiques.*

Grandiloquence ! Hyperbole ! Sensationnalisme !

Tremblez… *tremblez de peur…*

(Non merci, sans façon.)

> **Rudd** : *C'est pour cela que j'ai réuni les entreprises IT en mars : pour commencer à réfléchir à la façon de renverser la vapeur. Elles comprennent les enjeux.*

De quelles entreprises Internet s'agit-il, Amber ? Serait-ce par hasard celles qui

suivent, analysent et monnaient déjà nos moindres faits et gestes ? Les mêmes qui, jour après jour, sapent notre droit à la vie privée ? Un peu, qu'elles comprennent les enjeux ! C'est leur business. Pour reprendre la fameuse analyse de Bruce Schneier : « La NSA ne s'est pas tout à coup réveillée en se disant « On n'a qu'à espionner tout le monde ». Ils ont regardé autour d'eux et se sont dit : « Waouh, il y a des entreprises qui fliquent tout le monde. Il faut qu'on récupère une copie des données. » »

Votre problème, Amber, c'est que ces entreprises n'ont pas envie de partager toutes leurs données et analyses avec vous. Leurs systèmes sont même en partie conçus pour éviter d'avoir à le faire, même si elles le voulaient : certaines données ne leur sont tout simplement pas accessibles (chez Apple, dont le business model est différent de Google et Facebook, les systèmes sont connus pour être conçus de cette façon quand la technologie le permet, mais l'entreprise a démontré récemment qu'elle est capable de livrer la vie privée de ses utilisateurs en pâture pour satisfaire la demande d'un gouvernement répressif.)

Ne vous méprenez pas, Google et Facebook (pour prendre deux des plus gros *siphonneurs* de données perso) se contrefichent de notre vie privée, tout autant que Rudd. Mais ce que réclame Amber, c'est de pouvoir taper gratuitement dans leur butin (et le butin, pour eux, ce sont nos données). Ils n'apprécient pas forcément, mais on les a déjà vus s'en accommoder s'il le faut.

Ce qui est plus grave, c'est que la requête de Rudd exclut l'existence même de services qui cherchent vraiment à protéger notre vie privée : les outils de communication chiffrée de bout en bout comme Signal, par exemple ; ou les outils de communication décentralisés comme Tox.chat.

Plus grave encore, peut-être : si le gouvernement britannique arrive à ses fins et met en œuvre les pouvoirs qui lui sont déjà conférés par l'Investigatory Powers Act, cela fermera la porte à ceux d'entre nous qui veulent construire des systèmes décentralisés, respectueux de la vie privée, interopérables, libres et ouverts, parce que de tels systèmes deviendront illégaux. Or l'avenir de la démocratie à l'ère numérique en dépend.

> **Rudd** *: Grâce au travail accompli avec la cellule anti-terroriste du gouvernement, nous avons pu dépublier 280000 documents à caractère terroriste depuis 2010 et fermer des millions de comptes.*

Ok, donc, si je comprends bien, Amber, ce que vous nous expliquez, c'est que les mesures que vous prenez en collaboration avec les entreprises IT pour lutter contre la propagande publique des organisations terroristes fonctionnent bien. Le tout sans le moindre besoin de compromettre le chiffrement ou d'implémenter des portes dérobées dans les systèmes de communication. Mais continuez donc comme ça !

> **Rudd** *: Mais il y a bien plus à faire. Voilà pourquoi, lors de la réunion de mars dernier, les entreprises IT les plus puissantes de la planète se sont portées volontaires pour créer le Forum Internet Global Contre le Terrorisme.*

Les multinationales n'ont pas à fliquer les citoyens du monde, ce n'est pas leur rôle. Elles aimeraient bien amasser encore plus de données et de renseignements sur la population mondiale, légitimer les structures de surveillance déjà en place et exercer un contrôle encore plus grand. Ça va sans dire. Mais c'est cet avenir que nous devons à tout prix éviter.

Sous prétexte de nous préserver d'un risque statistiquement négligeable, ce qui est envisagé est un panoptique mondial sans précédent. Dans un tel système, nous pourrons dire adieu à nos libertés individuelles (la liberté de parole, le droit à la vie privée…) et à notre démocratie.

> **Rudd** *: Le Forum se réunit aujourd'hui pour la première fois et je suis dans la Silicon Valley pour y assister.*

Non seulement vous plaidez pour que les entreprises privées s'acoquinent avec les gouvernements pour jouer un rôle actif dans le flicage des citoyens ordinaires, mais vous faites appel à des entreprises américaines, ce qui revient à donner un sceau d'approbation officiel à l'implication d'entreprises étrangères dans le flicage des citoyens britanniques. (Merkel et Macron ont l'intention de saper les droits des citoyens européens de la même façon si on les laisse faire.)

> **Rudd** *: Les entreprises IT veulent aller plus vite et plus loin dans la mise au point de solutions technologiques susceptibles d'identifier, de faire disparaître, d'endiguer la diffusion de contenus extrémistes.*

Soit ! Mais ça ne nécessite toujours pas de portes dérobées ni de chiffrement moins performant. Encore une fois, il s'agit de contenus publics.

Il faudrait un jour prendre le temps de débattre beaucoup plus longuement de qui est habilité à décréter qu'un contenu est extrémiste, et de ce qui arrive quand les algorithmes se plantent et stigmatisent quelqu'un à tort comme auteur de propos extrémistes en laissant sous-entendre que cette personne est extrémiste alors qu'elle ne l'est pas.

À l'heure actuelle, ce sont des entreprises américaines qui définissent ce qui est acceptable ou pas sur Internet. Et le problème est bien plus vaste que ça : il nous manque une sphère publique numérique, puisque les Facebook et autres Google de la planète sont des espaces privés (pas publics) – ce sont des centres commerciaux, pas des parcs publics.

Ce que nous devrions faire, c'est financer la création d'espaces publics en ligne, encourager la souveraineté individuelle, promouvoir un usage équitable du bien commun. Vous, Madame Rudd, vous êtes bien sûr à des années-lumière de ce genre d'initiatives, mais au moment où je vous parle, certains d'entre nous travaillons à créer un monde aux antipodes de celui que vous appelez de vos vœux.

> **Rudd** : *Leur attitude mérite félicitations mais ils doivent également savoir que nous leur demanderons des comptes. Cependant notre défi ne se limite pas à cela. Car au-delà des contenus pernicieux auxquels tout le monde a accès, il y a ceux que nous ne voyons pas, ceux qui sont chiffrés.*

Ah, nous y voilà ! Après avoir consacré la moitié de l'article au combat victorieux du gouvernement contre l'expansion en ligne de la propagande publique des organisations terroristes, Rudd passe à son dada : la nécessité d'espionner les communications privées en ligne de chaque citoyen pour garantir notre sécurité.

Partie II : la guerre contre le chiffrement de bout en bout avec la complicité de Facebook, Microsoft, Twitter et YouTube (Google/Alphabet, Inc.)

C'est là qu'il faut prendre un siège si vous êtes sujet au vertige car Mme Rudd va faire mieux qu'un derviche tourneur. Elle va également lâcher une bombe qui

aura de graves répercussions sur votre vie privée si vous êtes adeptes des services fournis par Facebook, Microsoft, Twitter ou YouTube (Google/Alphabet, Inc.)

> **Rudd** *: le chiffrement joue un rôle fondamental dans la protection de tout un chacun en ligne. C'est un élément essentiel de la croissance de l'économie numérique et de la fourniture de services publics en ligne.*

Parfaitement, Amber. La discussion devrait s'arrêter là. Il n'y a pas de « mais » qui tienne.

Mais …

> **Rudd** : *Mais, comme beaucoup d'autres technologies efficaces, les services de chiffrement sont utilisés et détournés par une petite minorité d'utilisateurs.*

Oui, et donc ?

> **Rudd** : *Il existe un enjeu particulier autour de ce qu'on appelle le « chiffrement de bout en bout » qui interdit même au fournisseur de service d'accéder au contenu d'une communication.*

Le chiffrement de bout en bout a aussi un autre nom : le seul qui protège votre vie privée à l'heure actuelle (au moins à court terme, jusqu'à ce que la puissance de calcul soit démultipliée de façon exponentielle ou que de nouvelles vulnérabilités soient découvertes dans les algorithmes de chiffrement).

Incidemment, l'autre garant important de la vie privée, dont on parle rarement, est la décentralisation. Plus nos données privées échappent aux silos de centralisation, plus le coût de la surveillance de masse augmente – exactement comme avec le chiffrement.

> **Rudd** : *Que ce soit bien clair : le gouvernement soutient le chiffrement fort et n'a pas l'intention d'interdire le chiffrement de bout en bout.*

Ah bon, alors est-ce qu'on peut en rester là et rentrer chez nous maintenant … ?

> **Rudd** : *Mais l'impossibilité d'accéder aux données chiffrées dans certains cas ciblés et bien particuliers (même avec un mandat signé par un ministre et un haut magistrat) constitue un obstacle de taille dans la lutte anti-terroriste et la*

traduction en justice des criminels.

Oui, mais c'est la vie. On ne peut pas avoir le beurre et l'argent du beurre.

> **Rudd** : *Je sais que certains vont soutenir qu'on ne peut pas avoir le beurre et l'argent du beurre, que si un système est chiffré de bout en bout, il est à jamais impossible d'accéder au contenu d'une communication. C'est peut-être vrai en théorie. Mais la réalité est différente.*

Vrai en théorie ? Mme Rudd, c'est vrai en théorie, en pratique, ici sur Terre, sur la Lune et dans l'espace. C'est vrai, point final.

« Mais la réalité est différente », ce doit être la glorieuse tentative d'Amber Rudd pour battre le premier ministre australien, Malcolm Turnbull, dans la course aux âneries sur le chiffrement . M. Turnbull a en effet récemment fait remarquer que « les lois mathématiques sont tout à fait estimables, mais que la seule loi qui s'applique en Australie est la loi australienne. »

Turnbull et Rudd, bien sûr, suivent la même partition. C'est aussi celle que suivent May, Merkel et Macron. Et, après sa remarque illogique, Turnbull a laissé entendre de quelle musique il s'agit quand il a ajouté : « Nous cherchons à nous assurer de leur soutien. » (« leur », en l'occurrence, fait référence aux entreprises IT).

Rudd développe son idée dans le paragraphe qui suit :

> **Rudd** : *Dans la vraie vie, la plupart des gens sont prêts à troquer la parfaite inviolabilité de leurs données contre une certaine facilité d'utilisation et un large éventail de fonctionnalités. Il ne s'agit donc pas de demander aux entreprises de compromettre le chiffrement ou de créer de prétendues « portes dérobées ». Qui utilise WhatsApp parce qu'il est chiffré de bout en bout ? On l'utilise plutôt que parce que c'est un moyen incroyablement convivial et bon marché de rester en contact avec les amis et la famille. Les entreprises font constamment des compromis entre la sécurité et la « facilité d'utilisation » et c'est là que nos experts trouvent des marges de manœuvres possibles.*

Traduction : Ce que nous voulons, c'est que les entreprises n'aient pas recours au chiffrement de bout en bout.

Voilà donc la pierre angulaire de l'argumentaire de Rudd : les entreprises IT devraient décider d'elles-mêmes de compromettre la sécurité et la protection de la vie privée de leurs usagers, en n'implémentant pas le chiffrement de bout en bout. Et, pour faire bonne mesure, détourner l'attention des gens en créant des services pratiques et divertissants.

Inutile de préciser que ce n'est pas très loin de ce que font aujourd'hui les entreprises de la Silicon Valley qui exploitent les données des gens. En fait, ce que dit Rudd aux entreprises comme Facebook et Google, c'est : « Hé, vous appâtez déjà les gens avec des services gratuits pour pouvoir leur soutirer des données. Continuez, mais faites en sorte que nous aussi, nous puissions accéder à la fois aux métadonnées et aux contenus de leurs communications. Ne vous inquiétez pas, ils ne s'en apercevront pas, comme ils ne se rendent pas compte aujourd'hui que vous leur offrez des bonbons pour mieux les espionner. »

De même, l'argument de l'indispensable « compromis entre la sécurité et la facilité d'utilisation » relève d'un choix fallacieux. Une nouvelle génération d'apps sécurisées et respectueuses de la vie privée, comme Signal, prouvent qu'un tel compromis n'est pas nécessaire. En fait c'est Rudd, ici, qui perpétue ce mythe à dessein et incite les entreprises IT à s'en servir pour justifier leur décision d'exposer leurs usagers à la surveillance gouvernementale.

Pas besoin de réfléchir bien longtemps pour se rendre compte que l'argumentation d'Amber s'écroule d'elle-même. Elle demande « Qui utilise WhatsApp parce que c'est chiffré de bout en bout et non parce que c'est un moyen incroyablement convivial et bon marché de rester en contact avec les amis et la famille ? » Retournons-lui la question : « Qui s'abstient d'utiliser WhatsApp aujourd'hui sous prétexte que le chiffrement de bout en bout le rendrait moins convivial ? » (Et, tant que nous y sommes, n'oublions pas que Facebook, propriétaire de Whatsapp, fait son beurre en récoltant le plus d'informations possible sur vous et en exploitant cet aperçu de votre vie privée pour satisfaire son avidité financière et ses objectifs politiques. N'oublions pas non plus que les métadonnées – interlocuteurs, fréquence et horaires des appels – ne sont pas chiffrées dans WhatsApp, que WhatsApp partage ses données avec Facebook et que votre profil de conversation et votre numéro de téléphone sont liés à votre compte Facebook.`

Rudd *: Donc, nous avons le choix. Mais ces choix seront le fruit de discussions*

> *réfléchies entre les entreprises IT et le gouvernement – et ils doivent rester confidentiels.*

Traduction : Quand les entreprises supprimeront le chiffrement de bout en bout de leurs produits, nous ne souhaitons pas qu'elles en avertissent leurs usagers.

Voilà qui devrait vous faire froid dans le dos.

Les services dont Amber Rudd parle (comme WhatsApp) sont des applications propriétaires dont le code source est privé. Cela signifie que même d'autres programmeurs n'ont aucune idée précise de ce que font ces services (même si certaines techniques de rétro-ingénierie permettent d'essayer de le découvrir). Si la plupart des gens font confiance au chiffrement de bout en bout de WhatsApp c'est qu'un cryptographe très respecté du nom de Moxie Marlinspike l'a implémenté et nous a dit qu'il n'y avait pas de problème. Or, le problème avec les applications, c'est qu'elles peuvent être modifiées en un clin d'œil… et qu'elles le sont. WhatsApp peut très bien supprimer le chiffrement de bout en bout de ses outils demain sans nous en avertir et nous n'en saurons rien. En fait, c'est précisément ce que demande Amber Rudd à Facebook et compagnie.

À la lumière de ces informations, il y a donc deux choses à faire :

Regardez quelles entreprises participent au Forum Internet Global Contre le Terrorisme et cessez de croire un traître mot de ce qu'elles disent sur le chiffrement et les garanties de protection de la vie privée qu'offrent leurs produits. Ces entreprises sont Facebook, Microsoft, Twitter et YouTube (Google/Alphabet, Inc.)

Les experts en sécurité informatique ne doivent pas se porter garants du chiffrement de bout en bout de ces produits sauf s'ils peuvent s'engager à vérifier individuellement chaque nouvelle version exécutable. Pour limiter la casse, les individus comme Moxie Marlinspike, qui a pu se porter garant d'entreprises comme Facebook et WhatsApp, doivent publiquement prendre leurs distances par rapport à ces entreprises et les empêcher de devenir complices de la surveillance gouvernementale. Il suffit d'une seule compilation de code pour supprimer discrètement le chiffrement de bout en bout, et c'est exactement ce que souhaite Amber Rudd.

> **Rudd** : *Ce qu'il faut bien comprendre c'est qu'il ne s'agit pas de compromettre la sécurité en général.*

Ces actions compromettraient totalement la vie privée et la sécurité des militants et des groupes les plus vulnérables de la société.

> **Rudd** : *Il s'agit travailler ensemble pour que, dans des circonstances bien particulières, nos services de renseignement soient en mesure d'obtenir plus d'informations sur les agissements en ligne de grands criminels et de terroristes.*

Une fois encore, ni la suppression du chiffrement de bout en bout ni la mise en place de portes dérobées ne sont nécessaires pour combattre le terrorisme. Si Rudd veut arrêter des terroristes, elle devrait plutôt cesser de raboter le budget de la police de proximité, le seul moyen qui ait fait ses preuves. Je me demande si Rudd se rend seulement compte qu'en appelant à la suppression du chiffrement de bout en bout dans les outils de communications en ligne, ce qu'elle fait en réalité, c'est exposer le contenu des communications de tout un chacun à la surveillance continue par – au minimum – les fournisseurs et les hébergeurs de ces services. Sans parler du fait que ces communications peuvent être manipulées par d'autres acteurs peu recommandables, y compris des gouvernements étrangers ennemis.

> **Rudd** : *Parer à cette menace à tous les niveaux relève de la responsabilité conjointe des gouvernements et des entreprises. Et nous avons un intérêt commun : nous voulons protéger nos citoyens et ne voulons pas que certaines plateformes puissent servir à planifier des attaques contre eux. La réunion du Forum qui a lieu aujourd'hui est un premier pas dans la réalisation de cette mission.*

Je n'ai rien de plus à ajouter, pas plus que Rudd.

Pour conclure, je préfère insister sur ce que j'ai déjà dit :

Ce que souhaite Amber Rudd ne vous apportera pas plus de sécurité. Ça ne vous protégera pas des terroristes. Ça permettra aux gouvernements d'espionner plus facilement les militants et les minorités. Ça compromettra la sécurité de tous et aura des effets glaçants, dont la destruction du peu de démocratie qui nous reste. Ça nous conduira tout droit à un État Surveillance et à un panoptique mondial,

tels que l'humanité n'en a jamais encore connu.

Quant aux entreprises membres du Forum Internet Global Contre le Terrorisme (Facebook, Microsoft, Twitter et YouTube (Google/Alphabet, Inc.) – il faudrait être fou pour croire ce qu'elles disent du chiffrement de bout en bout sur leur plateformes ou des fonctionnalités « vie privée » de leurs apps. Vu ce qu'a dit Amber Rudd, sachez désormais que le chiffrement de bout en bout dont elles se targuent aujourd'hui peut être désactivé et compromis à tout moment lors d'une prochaine mise à jour, et que vous n'en serez pas informés.

C'est particulièrement préoccupant pour WhatsApp, de Facebook, dont certains recommandent fréquemment l'usage aux militants.

Vu ce qu'a dit Amber Rudd et ce que nous savons à présent du Forum Internet Global Contre le Terrorisme, continuer à recommander WhatsApp comme moyen de communication sécurisé à des militants et à d'autres groupes vulnérables est profondément irresponsable et menace directement le bien-être, voire peut-être la vie, de ces gens.

P.S. Merci pour ce beau travail, Amber. Espèce de marionnette !

(Un grand merci, non ironique cette fois, à Laura Kalbag pour sa relecture méticuleuse et ses corrections.)

À propos de l'auteur

Aral Balkan est militant, designer et développeur. Il représente ⅓ de Ind.ie, une petite entreprise sociale œuvrant à la justice sociale à l'ère du numérique.

Contacter Aral Balkan

Email *(pour les questions urgentes, merci de mettre laura@ind.ie en CC)*

Clé publique *(94E9AA31)*

Mastodon*.ar.al*
Twitter