Apple veut protéger les enfants mais met en danger le chiffrement

Apple vient de subir un tir de barrage nourri de la part des défenseurs de la vie privée alors que ce géant du numérique semble animé des intentions les plus louables…

Qui oserait contester un dispositif destiné à éradiquer les contenus incitant à des abus sexuels sur les enfants ? Après tout, les autres géants du numérique, Google et Microsoft entre autres, ont déjà des outils de détection pour ces contenus (voir ici et là)… Alors comment se fait-il que la lettre ouverte que nous traduisons ici ait réuni en quelques heures autant de signatures d'organisations comme d'individus, dont Edward Snowden ?

Deux raisons au moins.

D'abord, Apple a construit sa réputation de protecteur intransigeant de la vie privée au point d'en faire un cheval de bataille de sa communication : « Ce qui se passe dans votre iPhone reste sur votre iPhone ». Souvenons-nous aussi qu'en février 2016 Apple a fermement résisté aux pressions du FBI et de la NSA qui exigeaient que l'entreprise fournisse un logiciel de déchiffrement des échanges chiffrés (un bon résumé par ici). La surprise et la déception sont donc grandes à l'égard d'un géant qui il y a quelques années à peine co-signait une lettre contre la loi anti-chiffrement que des sénateurs états-uniens voulaient faire passer.

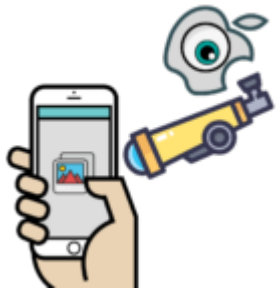
Mais surtout, et c'est sans doute plus grave, Apple risque selon les experts de mettre en péril le chiffrement de bout en bout. Alors oui, on entend déjà les libristes ricaner doucement que c'est bien fait pour les zélateurs

inconditionnels d'Apple et qu'ils n'ont qu'à renoncer à leur dispendieuse assuétude… mais peu nous importe ici. Le dispositif envisagé par Apple aura forcément des répercussions sur l'ensemble de l'industrie numérique qui ne mettra que quelques mois pour lui emboîter le pas, et en fin de compte, toute personne qui souhaite protéger sa vie privée sera potentiellement exposée aux risques que mentionnent les personnalités citées dans cette lettre ouverte…

Lettre ouverte contre la technologie de l'analyse du contenu d'Apple qui porte atteinte à la vie privée

Source : https://appleprivacyletter.com/

Des experts en sécurité et en protection de la vie privée, des spécialistes en cryptographie, des chercheurs, des professeurs, des experts juridiques et des utilisateurs d'Apple dénoncent le projet lancé par Apple qui va saper la vie privée des utilisateurs et le chiffrement de bout en bout.



Cher Apple,

Le 5 août 2021, Apple a annoncé de nouvelles mesures technologiques censées s'appliquer à la quasi-totalité de ses appareils sous le prétexte affiché de « Protections étendues pour les enfants ».

Bien que l'exploitation des enfants soit un problème sérieux, et que les efforts pour la combattre relèvent incontestablement d'intentions louables, **la proposition d'Apple introduit une porte dérobée qui menace de saper les protections fondamentales de la vie privée pour tous les utilisateurs de produits Apple.**

La technologie que se propose d'employer Apple fonctionne par la surveillance permanente des photos enregistrées ou partagées sur l'iPhone, l'iPad ou le Mac. Un système détecte si un certain nombre de photos répréhensibles sont repérées dans le stockage iCloud et alerte les autorités. Un autre système avertit les parents d'un enfant si iMessage est utilisé pour envoyer ou recevoir des photos qu'un algorithme d'apprentissage automatique considère comme contenant de la nudité.

Comme les deux vérifications sont effectuées sur l'appareil de l'utilisatrice, elles ont le potentiel de contourner tout chiffrement de bout en bout qui permettrait de protéger la vie privée de chaque utilisateur.

Dès l'annonce d'Apple, des experts du monde entier ont tiré la sonnette d'alarme car les dispositifs proposés par Apple pourraient transformer chaque iPhone en un appareil qui analyse en permanence toutes les photos et tous les messages qui y passent pour signaler tout contenu répréhensible aux forces de l'ordre, ce qui crée ainsi un précédent où nos appareils personnels deviennent un nouvel outil radical de surveillance invasive, avec très peu de garde-fous pour empêcher d'éventuels abus et une expansion déraisonnable du champ de la surveillance.

L'Electronic Frontier Foundation a déclaré « **Apple ouvre la porte à des abus plus importants** » :

> *« Il est impossible de construire un système d'analyse côté client qui ne puisse être utilisé que pour les images*

> *sexuellement explicites envoyées ou reçues par des enfants. En conséquence, même un effort bien intentionné pour construire un tel système va rompre les promesses fondamentales du chiffrement de la messagerie elle-même et ouvrira la porte à des abus plus importants […] Ce n'est pas une pente glissante ; c'est un système entièrement construit qui n'attend qu'une pression extérieure pour apporter le plus petit changement. »*

Le Center for Democracy and Technology a déclaré qu'il était « profondément préoccupé par les changements projetés par Apple qui créent en réalité de nouveaux risques pour les enfants et tous les utilisateurs et utilisatrices, et qui représentent un tournant important par rapport aux protocoles de confidentialité et de sécurité établis de longue date » :

> *« Apple remplace son système de messagerie chiffrée de bout en bout, conforme aux normes de l'industrie, par une infrastructure de surveillance et de censure, qui sera vulnérable aux abus et à la dérive, non seulement aux États-Unis, mais dans le monde entier », déclare Greg Nojeim, codirecteur du projet Sécurité et surveillance de la CDT. « Apple devrait abandonner ces changements et rétablir la confiance de ses utilisateurs dans la sécurité et l'intégrité de leurs données sur les appareils et services Apple. »*

Le Dr. Carmela Troncoso, experte en recherche sur la sécurité et la vie privée et professeur à l'EPFL à Lausanne, en Suisse, a déclaré que **« le nouveau système de détection d'Apple pour les contenus d'abus sexuel sur les enfants est promu sous le prétexte de la protection de l'enfance et de la vie privée, mais il s'agit d'une étape décisive vers une surveillance systématique et un contrôle généralisé ».**

Matthew D. Green, un autre grand spécialiste de la recherche sur la sécurité et la vie privée et professeur à l'université Johns Hopkins de Baltimore, dans le Maryland, a déclaré :

> *« Hier encore, nous nous dirigions peu à peu vers un avenir où de moins en moins d'informations devaient être contrôlées et examinées par quelqu'un d'autre que nous-mêmes. Pour la première fois depuis les années 1990, nous récupérions notre vie privée. Mais aujourd'hui, nous allons dans une autre direction […] La pression va venir du Royaume-Uni, des États-Unis, de l'Inde, de la Chine. Je suis terrifié à l'idée de ce à quoi cela va ressembler. Pourquoi Apple voudrait-elle dire au monde entier : « Hé, nous avons cet outil » ?*

Sarah Jamie Lewis, directrice exécutive de l'Open Privacy Research Society, a lancé cet avertissement :

> *« Si Apple réussit à introduire cet outil, combien de temps pensez-vous qu'il faudra avant que l'on attende la même chose des autres fournisseurs ? Avant que les applications qui ne le font pas ne soient interdites par des murs de protection ? Avant que cela ne soit inscrit dans la loi ? Combien de temps pensez-vous qu'il faudra avant que la base des données concernées soit étendue pour inclure les contenus « terroristes » ? « les contenus « préjudiciables mais légaux » ? « la censure spécifique d'un État ? »*

Le Dr Nadim Kobeissi, chercheur sur les questions de sécurité et de confidentialité, a averti :

> *« Apple vend des iPhones sans FaceTime en Arabie saoudite, car la réglementation locale interdit les appels téléphoniques chiffrés. Ce n'est qu'un exemple parmi tant d'autres où Apple s'est plié aux pressions locales. Que se passera-t-il lorsque la réglementation locale en Arabie Saoudite exigera que les messages soient scannés non pas pour des abus sexuels sur des enfants, mais pour homosexualité ou pour offenses à la monarchie ? »*

La déclaration de l'Electronic Frontier Foundation sur la

question va dans le même sens que les inquiétudes exposées ci-dessus et donne des exemples supplémentaires sur la façon dont la technologie proposée par Apple pourrait conduire à des abus généralisés :

> *« Prenez l'exemple de l'Inde, où des règlements récemment adoptés prévoient des obligations dangereuses pour les plateformes d'identifier l'origine des messages et d'analyser préalablement les contenus. En Éthiopie, de nouvelles lois exigeant le retrait des contenus de « désinformation » sous 24 heures peuvent s'appliquer aux services de messagerie. Et de nombreux autres pays – souvent ceux dont le gouvernement est autoritaire – ont adopté des lois comparables. Les changements projetés par Apple permettraient de procéder à ces filtrages, retraits et signalements dans sa messagerie chiffrée de bout en bout. Les cas d'abus sont faciles à imaginer : les gouvernements qui interdisent l'homosexualité pourraient exiger que l'algorithme de classement soit formé pour restreindre le contenu LGBTQ+ apparent, ou bien un régime autoritaire pourrait exiger que le qu'il soit capable de repérer les images satiriques populaires ou les tracts contestataires. »*

En outre, l'Electronic Frontier Foundation souligne qu'elle a déjà constaté cette dérive de mission :

« L'une des technologies conçues à l'origine pour scanner et *hacher* les images d'abus sexuels sur les enfants a été réutilisée pour créer une base de données de contenus « terroristes » à laquelle les entreprises peuvent contribuer et accéder dans l'objectif d'interdire ces contenus. Cette base de données, gérée par le Global Internet Forum to Counter Terrorism (GIFCT), ne fait l'objet d'aucune surveillance externe, malgré les appels lancés par la société civile. »

Des défauts de conception fondamentaux de l'approche proposée par Apple ont été soulignés par des experts, ils affirment que

« **Apple peut de façon routinière utiliser différents ensembles de données d'empreintes numériques pour chaque utilisatrice. Pour un utilisateur, il pourrait s'agir d'abus d'enfants, pour un autre, d'une catégorie beaucoup plus large** », ce qui permet un pistage sélectif du contenu pour des utilisateurs ciblés.

Le type de technologie qu'Apple propose pour ses mesures de protection des enfants dépend d'une infrastructure extensible qui ne peut pas être contrôlée ou limitée techniquement. Les experts ont averti à plusieurs reprises que le problème n'est pas seulement la protection de la vie privée, mais aussi le manque de responsabilité de l'entreprise, les obstacles techniques au développement, le manque d'analyse ou même de prise en considération du potentiel d'erreurs et de faux positifs.

Kendra Albert, juriste à la Harvard Law School's Cyberlaw Clinic, a averti que « ces mesures de « protection de l'enfance » vont faire que les enfants homosexuels seront mis à la porte de leur maison, battus ou pire encore », […] Je sais juste (je le dis maintenant) que ces algorithmes d'apprentissage automatique vont signaler les photos de transition. Bonne chance pour envoyer une photo de vous à vos amis si vous avez des « tétons d'aspect féminin » ».

Ce que nous demandons

Nous, les soussignés, demandons :

1. **L'arrêt immédiat du déploiement par Apple de sa technologie de surveillance du contenu proposée.**
2. **Une déclaration d'Apple réaffirmant son engagement en faveur du chiffrement de bout en bout et de la protection de la vie privée des utilisateurs.**

La voie que choisit aujourd'hui Apple menace de saper des décennies de travail effectué par des spécialistes en technologies numériques, par des universitaires et des

militants en faveur de mesures strictes de préservation de la vie privée, pour qu’elles deviennent la norme pour une majorité d’appareils électroniques grand public et de cas d’usage. Nous demandons à Apple de reconsidérer son déploiement technologique, de peur qu’il ne nuise à cet important travail.

–> Signer la lettre sur GitHub

–> Liste des signataires à ce jour