

Chiffrement : Apple refuse d'aider le FBI à casser la sécurité de l'iPhone

Après les pressions politiques ou celles des services de police, les injonctions de la justice. Un juge fédéral américain vient en effet d'ordonner à Apple de fournir une « *assistance technique raisonnable* » afin d'aider les forces de police à accéder aux données chiffrées d'un iPhone 5c employé par Syed Rizwan Farook, un des auteurs de la tuerie de San Bernardino en décembre dernier. Rappelons que 14 personnes avaient trouvé la mort le 2 décembre dernier dans cette ville de Californie, suite à une fusillade à laquelle participaient Syed Rizwan Farook et son épouse Tashfeen Malik.

La justice demande à Apple d'utiliser son expertise technique pour **contourner la fonction d'auto-effacement** du téléphone et pour permettre au FBI de réaliser un **nombre illimité de tentatives d'accès** – via des codes aléatoires – en vue de débloquent le smartphone. Les experts du bureau fédéral veulent pouvoir soumettre des codes d'accès à la chaîne, via le port physique du terminal, Bluetooth ou WiFi, sans que l'OS n'introduise de délai entre deux essais. Cupertino est prié de se creuser la tête pour y parvenir... La firme californienne a déjà annoncé son intention de se battre contre cette injonction, Tim Cook, son Pdg, estimant qu'elle menace la sécurité des utilisateurs Apple et qu'elle a « *des implications bien au-delà du cas en question* ».

Demandes du FBI : Apple est resté sourd

Même s'il ne s'agit plus ici d'affaiblir le chiffrement via l'introduction d'une backdoor – la justice réclamant plutôt à Apple les moyens de contourner les sécurités qu'il a mises en place en vue d'enrayer les attaques par force brute -, [l'injonction](#) de la justice américaine relance le débat sur les moyens cryptologiques offerts aux utilisateurs. Suite aux révélations Snowden sur les pratiques de la NSA, les industriels de la high tech américaine ont déployé des technologies de chiffrement qu'ils ne peuvent plus contourner, les clefs étant par exemple placées entre les mains des utilisateurs.

C'est notamment la direction prise par Apple. Depuis iOS 8, Apple a changé son procédé de chiffrement : la clef étant désormais liée au mot de passe de l'utilisateur, Apple affirme ne plus pouvoir récupérer les données chiffrées sur ses terminaux sans connaître ce sésame. Selon la justice américaine, la firme a par ailleurs « *refusé de fournir l'assistance technique (réclamée par le FBI, NDLR) de façon volontaire* ».

Protéger les utilisateurs... ou aider les criminels ?

Au passage, l'escarmouche judiciaire apparaît comme une démonstration concrète de la volonté de l'industriel de protéger ses utilisateurs, quitte à opposer une fin de non-recevoir aux services de police. La solidité des technologies déployées dans iOS, qui résiste depuis plus de deux mois aux experts du FBI, trouve également confirmation.

En août dernier, dans une tribune publiée par le *New York Times*, Cyrus Vance, procureur de

Manhattan, Javier Zaragoza, procureur de la Haute Cour en Espagne, Adrian Leppard, commissaire de police de la ville de Londres, et **François Molins**, le procureur de la République de Paris, [s'alarmaient de la puissance des outils de chiffrement](#) disponibles sur les smartphones, des outils qui, selon eux, ralentissent les enquêtes et que les malfaiteurs ont appris à exploiter à leur profit.

A lire aussi :

[Apple prend la tête du combat contre les backdoors dans le chiffrement](#)

[Après les attentats : faut-il mieux encadrer le chiffrement ?](#)

[Chiffrement : la NSA plaide pour un cadre légal d'accès aux communications](#)

Crédit photo : Lester Balajadia / Shutterstock