Fingerprinting : toutes les questions que vous vous posez

Privés de la solution cookie sur mobile, les spécialistes de la publicité se sont rabattus sur cette technique qui permet de créer une empreinte digitale à l'utilisateur. Explications.

L'absence du cookie au sein des applications, conjuguée au fait que beaucoup de navigateurs mobiles tels que Safari bloquent les cookies tiers par défaut, a obligé les professionnels de la publicité à lui trouver une alternative. C'est ainsi qu'est né il y a quelques années le fingerprinting, pour offrir aux annonceurs mobile peu ou prou les mêmes capacités de ciblages que sur le Web fixe.

De quoi parle-t-on ?

Il s'agit de créer une "empreinte digitale" de l'utilisateur grâce à un algorithme qui recueille une série d'informations dont la combinaison forme une signature unique permettant de "reconnaître" un utilisateur et de suivre son activité sur le web. "Prises séparément, ces informations ne veulent rien dire, précise Jérôme Stioui, fondateur et président de l'agence Ad4Screen. Mises bout à bout et matchées à un instant T, elles permettront de dire quelle est la probabilité que la personne qui a cliqué sur une publicité donnée et celle qui vient d'ouvrir l'application promue par cette publicité ne fassent qu'une".

Quelles sont les données récupérées ?

Jérôme Stioui se contentera de révéler les données suivantes "le user agent ; l'adresse IP ; la langue, la version et l'heure du terminal ; l'heure du serveur", précisant toutefois qu'il peut aller jusqu'à collecter une trentaine d'informations.

L'utilisateur est-il identifié en tant que tel ?

"Absolument pas, rassure Jérôme Stioui. Nous n'utilisons aucune donnée du type adresse email qui permettrait d'identifier l'internaute de manière unique". Surtout, l'empreinte digitale a une durée de vie limitée. Un moyen de rassurer ceux qui déplorent que l'on ne puisse pas échapper à ce fingerprinting ?

Est-ce un procédé sûr à 100% ?

Non, tout simplement parce que le fingerprinting est un modèle statistique, à l'inverse du cookie qui est tout ce qu'il y a de plus factuel. Le degré de fiabilité varie de 80 à 99%, en fonction du nombre d'informations récoltées. Pour cause, si deux collègues détenteurs d'un iPhone 5 chez le même opérateur téléchargent une application en utilisant le même Wifi et la même version de l'OS, au même moment, il sera très difficile de les distinguer sans élargir la collecte d'informations. "D'autant que ce degré de fiabilité de réconciliation diminue à mesure que le temps passé entre le clic sur la publicité et l'ouverture de l'application est important", précise Jérôme Stioui. Pour autant, Jérôme Stioui estime à 90% le nombre de personnes qui ouvrent une application moins d'une heure après l'avoir téléchargée.

Dans quels cas de figure les annonceurs y ont-ils recours ?

Si le fingerprinting est aujourd'hui largement démocratisé, il y a quasiment autant de manières de le pratiquer que d'acteurs. Difficile dans des telles conditions de dégager une méthode universelle qui serait efficace au sein de toutes les applications. Impossible donc de s'en servir pour faire du retargeting au sein d'une galaxie d'applications. "Cela impliquerait de convaincre tous les éditeurs de télécharger notre SDK, explique Jérôme Stioui. C'est d'autant plus fastidieux qu'Apple et Android proposent, via l'IDFA et l'Android ID, des identifiants qui permettent de faire ce travail de reciblage". La pratique du fingerprinting est donc aujourd'hui essentiellement cantonnée à l'attribution.

Quelle différence avec le "canvas fingerprinting" qui a fait polémique cet été ?

Une bonne partie du Web s'est fait l'écho cet été d'un article de Julia Angwin pour ProPublica, stigmatisant l'apparition d'une nouvelle technique de pistage, "le canvas fingerprinting", "pratiquement impossible à bloquer". Une pratique en tout point similaire à celle d'Ad4Screen, à ceci près qu'elle s'applique au Web fixe. Jérôme Stioui ne préfère pas juger sans connaître mais précise que sa solution respecte en tous points la vie privée de l'internaute. "Nous ne collectons que des données publiques, non nominatives".

La solution va-t-elle un jour remplacer les cookies ?

Il est pratiquement sûr que non. La fragmentation des solutions empêche tout déploiement à grande échelle. L'utilisation croissante d'identifiants tels que l'IDFA et l'Android ID, bien plus fiables, devrait circonscrire la pratique du fingerprinting au domaine de l'attribution.

Comment choisir son prestataire ?

Même si l'agence que vous consultez ne consentira sans doute jamais à vous révéler les secrets de son arrière-boutique, n'hésitez pas à effectuer des campagnes tests voire à contacter certains de ses clients. Dans tous les cas, ne jamais s'engager sur la seule foi des propos de votre agence.