Smartphone : l'utilisateur localisé à tout instant

Description

La géolocalisation est la « reine des données du smartphone *» comme le démontrent des tests menés par la CNIL et l'Inria.*

« *Si ces technologies offrent des services extraordinaires aux individus et sont bénéfiques pour la société, elles ne peuvent se développer que dans le respect de la vie privée et des libertés individuelles. Rendre la technologie plus transparente et plus compréhensible aux citoyens est un défi commun pour la recherche et pour l'autorité de régulation* » peut-on lire en introduction de la présentation des récents travaux menés par la CNIL et l'Inria.

En moyenne, une trentaine d'applications sont installées aujourd'hui sur un téléphone portable ou une tablette. La CNIL mène depuis trois ans une étude pour en connaître les conséquences quant au respect de la vie privée. Conduit avec l'Inria qui a conçu l'outil d'analyse, le projet Mobilitics montre l'ampleur de l'accès aux données personnelles permis, ou plutôt imposé, par les smartphones. L'étude a fait ce constat : si cette pratique est généralisée par les éditeurs d'applications et les fournisseurs de services, elle est pourtant rendue peu visible aux utilisateurs de smartphone. Il faut principalement déplorer le manque d'informations : les éditeurs de système d'exploitation pour smartphones et tablettes (Apple, Google, Microsoft, Mozilla) ne fournissent pas aux utilisateurs les moyens suffisants de contrôler l'accès à leurs données personnelles lié à l'usage des applications qu'ils ont téléchargées.

Grâce à l'outil d'analyse Mobilitics, installé sur les smartphones utilisés pour l'expérience par des agents de la CNIL, deux vagues de tests d'une durée de trois mois ont été menées sur 189 applications sous iOS 5 (novembre 2012-janvier 2013) et sur 121 applications sous Android « Jelly Bean » (juin-septembre 2014). A la suite de la première vague de tests sous iOS, la CNIL et l'Inria ont tiré trois enseignements majeurs en ce qui concerne d'abord le cas particulier de la géolocalisation, « *reine des données du smartphone* », puis les stratégies d'identification menées par les développeurs et les éditeurs d'applications répondant à des objectifs très divers, tels que la mesure d'audience, des statistiques d'utilisation, la monétisation et la publicité et, enfin, la difficulté à déterminer un lien entre l'accès aux données et l'action de l'utilisateur ou le bon fonctionnement des applications.

L'étude de la CNIL et de l'Inria révèle « *une course aux identifiants* ». Il existe de nombreux identifiants, techniques, matériels ou logiciels, pour chaque appareil, parmi lesquels l'identifiant alphanumérique de l'appareil (UDID – Unique Device Identifier – pour iOS, et Android ID), l'Advertising identifier pour la publicité, l'Identifier for vendor pour chaque éditeur d'applications, l'IMEI (International Mobile Equipment Identity) pour bloquer un téléphone perdu ou volé, l'IMSI (International Mobile Subscriber Identity) stocké dans la carte SIM permettant à un opérateur d'identifier un abonné, l'ICCID (Integrated Circuit Card ID), numéro unique de la carte SIM, etc. Sur iOS comme sur Android, plus de la moitié des applications testées accèdent à des identifiants du téléphone.

Si les utilisateurs d'un smartphone ont en principe la possibilité de régler leur appareil afin de limiter le traçage publicitaire, la démarche à suivre n'est pas simple à trouver ni facile à comprendre. En outre, « *la coexistence de nombreux identifiants facilite grandement les possibilités de contournement de ce type de cloisonnement* », selon les auteurs de l'étude, qui explique que « *en dehors des garanties juridiques, seule la bonne volonté des développeurs permet de garantir qu'ils ne contournent pas les réglages mis en œuvre par les utilisateurs pour limiter le ciblage publicitaire* ».

D'après les résultats des deux vagues de tests, entre un quart et un tiers des applications présentes sur les différents appareils, fonctionnant sous iOS ou Android, ont eu accès à la localisation de l'appareil, par le GPS, la détection des antennes du réseau cellulaire ou des bornes Wi-Fi. Ce recours à la géolocalisation se caractérise à la fois par son intensité et sa fréquence. Cela se traduit par plus de 1 million d'accès à la géolocalisation en trois mois pour une seule et même application, et par plus de 700 000 fois pour une autre application, soit près d'un accès par minute en moyenne, sans qu'il s'agisse d'applications spécifiques de navigation ou de recherche d'itinéraire. Donnée la plus collectée, la localisation de l'utilisateur d'un smartphone représente, à elle seule, plus de 30 % de l'ensemble des informations délivrées par les appareils portables. Et cela, sans que les fonctionnalités inhérentes à l'application le justifient et sans aucune demande effective de la part de l'utilisateur. Le plus souvent, la géolocalisation ne se limite pas au temps nécessaire à l'utilisation d'une application, elle peut être quasiment permanente. Ainsi, des applications relatives à la géolocalisation offrant une alternative (« *toujours* » ou seulement « *lorsque l'app est en marche* ») constituent une avancée, comme le propose le système d'exploitation iOS8 depuis septembre 2014.

Les applications installées par défaut sur les smartphones, impossibles à supprimer, notamment celles donnant accès au magasin d'applications, figurent également parmi les plus grosses consommatrices de données, sans qu'aucun réglage type opt in/opt out ne soit possible. En trois mois, l'application Play Store de Google a accédé 1 300 000 fois à la localisation pour un seul utilisateur.

C'est pourquoi, comme le souligne l'étude, « *les grands systèmes d'exploitation et magasins d'applications ont un rôle clé et des responsabilités lourdes. Ils définissent le cadre d'action des autres acteurs en décidant ce qui est techniquement possible et ce qui ne l'est pas, les outils d'information et de maîtrise qui sont disponibles et le moment auquel il est possible d'y accéder (au téléchargement, à l'installation, par des alertes à l'écran, dans les réglages de l'appareil).* […] *Les développeurs et éditeurs d'applications doivent quant à eux adopter une approche de privacy by design et notamment minimiser les données en s'interdisant la collecte des données qui ne sont pas liées au service rendu par l'application* ».

Source :

- « Mobilitics, saison 2 : Les smartphones et leurs apps sous le microscope de la CNIL et d'Inria », Geoffrey Delcroix et Stéphane Petitcolas, Inovation & Prospective, n° 08, CNIL, cnil.fr, novembre 2014.

Categorie

1. Usages

date créée
9 juin 2015
Auteur
francoise