Afin que les applications de nos smartphones n’abusent pas l’utilisateur

Il est aujourd’hui question des logiciels installés dans nos téléphones portables intelligents, on parle alors plutôt des *apps* de nos smartphones.

Ils sont intelligents parce que ces applications peuvent désormais rendre toutes sortes de services. Sauf que parfois, voire souvent, elles collectent au passage les données personnelles de l’utilisateur sans que ce dernier soit forcément au courant de tels agissements[1].

En effet si l’on savait clairement que telle apps a accès à nos contacts, nos photos ou nos localisations géographiques, informations envoyées on ne sait trop où de manière non sécurisée, on y réfléchirait peut-être à deux fois avant de l’installer d’un simple clic dans notre téléphone[2].

La faute aux utilisateurs non vigilants[3] mais surtout aux développeurs de ces applications qui sont encore loin de tous adopter les quelques recommandations ci-dessous de l’Electronic Frontier Foundation.

Remarque : On notera que Mozilla, avec ses prometteurs et vertueux projets Do Not Track et Boot 2 Gecko, se démarque une fois de plus de ses petits camarades.

Déclaration des droits de la vie privée des utilisateurs de téléphones mobiles

Mobile User Privacy Bill of Rights

Parker Higgins – 2 mars 2012 – EFF.org
(Traduction Framalang/Twitter : kamui57, Pascal, goofy, Ak:kes, Thibo, Sylvain, Céline, Jonathan, Gatitac, Antoine, BlackMouse)

Les applications pour smartphones représentent une technologie puissante qui va devenir de plus en plus importante dans les années à venir. Mais l'avantage incomparable qu'elles apportent à un appareil toujours allumé et connecté présente également des risques pour notre vie privée. Et vu les données sensibles que les utilisateurs stockent désormais dans leurs téléphones (textes, coordonnées, localisations, photos, vidéos…), les responsabilités qui incombent aux fabricants, opérateurs, développeurs d'applications et régies publicitaires mobiles sont de plus en plus importantes pour respecter la vie privée des utilisateurs, afin de gagner et conserver la confiance, plus que jamais importante et nécessaire, de ces derniers.

Heureusement, il existe des recommandations répondant aux besoins et attentes

des utilisateurs. Ce *guide des bonnes pratiques* s'inspire fortement de documents tels que le projet de loi FEP de Droits à la confidentialité pour les utilisateurs de réseaux sociaux ainsi que du livre blanc de la Maison Blanche La confidentialité des données des consommateurs dans un monde connecté pour établir une référence et indiquer aux acteurs de l'industrie mobile ce qu'ils doivent faire afin de mieux respecter la vie privée de l'utilisateur.

Constructeurs ou régies publicitaires ont leur part de responsabilité mais on s'intéressera ici avant tout aux développeurs qui ont les possibilité de devancer ces problèmes.

Une déclaration des droits de l'utilisateur de mobile

Les développeurs doivent créer des applications qui respectent les droits suivants :

- **Contrôle individuel** : Les utilisateurs ont le droit d'exercer un contrôle sur les données collectées par les applications et savoir comment elles sont utilisées. Bien qu'il existe un contrôle d'accès au niveau du système d'exploitation des smartphones (iOS, Android…), les développeurs devraient s'appliquer à donner également ce pouvoir aux utilisateurs même lorsque cela n'est pas requis techniquement ou juridiquement par la plateforme. Le droit à un contrôle individuel inclut également la possibilité de revenir sur son consentement et d'effacer ces données des serveurs d'applications. Les fiches techniques de la Maison Blanche le disent explicitement : « les compagnies doivent fournir les moyens d'annuler un accord avec la même facilité qu'on a eu à l'obtenir en installant l'application. Si des consommateurs donnent leur consentement en appuyant sur une simple touche, ils devraient être capables de l'annuler de la même façon. »

- **La collecte de données ciblées** : En plus des guides des meilleures pratiques pour les fournisseurs d'accès, les développeurs d'applications doivent se montrer particulièrement prudents lorsqu'il s'agit d'appareils mobiles. Le partage non désiré et à son insu des contacts du carnet d'adresses ou des albums photos ont déjà fait l'objet de vives protestation des utilisateurs. Un autre domaine particulièrement sensible concerne les données et les archives de localisation, ainsi que les contenus et les

métadonnées relatives aux appels téléphoniques et aux messages texto. Les développeurs d'applications mobiles ne devraient recueillir que le minimum nécessaire pour fournir le service tout en préservant l'anonymat des renseignements personnels.

- **Transparence** : Les utilisateurs ont besoin de connaître les données auxquelles une application accède, combien de temps ces données sont conservées et avec qui elles seront partagées. Les usagers devraient être en mesure d'accéder de manière claire aux politiques de confidentialité et de sécurité, et ce, avant et après l'installation. La transparence est particulièrement critique là où l'utilisateur n'interagit pas directement avec l'application (comme par exemple avec Carrier IQ).

- **Respect du contexte** : Les applications qui collectent des données ne devraient les utiliser ou les partager qu'en respectant le contexte dans lequel elles ont été fournies. Par exemple si une application possède une fonction « trouver des amis » qui nécessite l'accès à vos contacts, elle ne doit pas donner ces informations à des tiers ou les utiliser pour envoyer des e-mails à ces contacts. Quand l'application souhaites faire une une utilisation externe de ces données, elle doit impérativement obtenir l'accord explicite de l'utilisateur.

- **Sécurité** : Les développeurs sont responsables de la sécurité des données qu'ils collectent et conservent. Elle devraient être chiffrées aussi pour le stockage que lorsqu'elles transitent du téléphone au serveur de l'application.

- **Responsabilité** : En fin de compte, tous les acteurs de l'industrie mobile sont responsables du comportement des matériels et des logiciels qu'ils créent et déploient. Les utilisateurs ont le droit d'attendre un comportement responsable de leur part et de leur demande de rendre des comptes.

Bonnes pratiques techniques

Que devraient faire les développeurs pour respecter les points ci-dessus ? Voici quelques pratiques à suivre pour préserver la vie privée des utilisateurs.

- **Anonymisation et dissimulation** : Les informations devraient être si

possible hachées, dissimulées ou au moins anonymisées.

- **Sécuriser les transmission de données** : Les connexions TLS devraient être utilisées par défaut pour transférer toute information personnelle et doivent l'être impérativement pour toute information sensible.
- **Stockage sécurisé des données** : Les développeurs doivent conserver les informations uniquement durant le temps nécessaire au fonctionnement de leurs services, et ces informations doivent être correctement chiffrées.
- **Sécurité interne** : Les entreprises doivent protéger les utilisateurs non seulement des attaques venues de l'extérieur mais aussi du risque de voir des employés abuser de leur possibilité d'accès aux données sensibles.
- **Test d'intrusion** : Souvenez-vous de la loi Schneier qui stipule que « n'importe qui, du plus parfait amateur au meilleur cryptographe, peut créer un algorithme que lui-même ne peut pas casser ». Les systèmes de sécurité devraient être testés de manière indépendante et vérifiés avant qu'ils ne soient compromis.
- **Do Not Track** : Il faut encourager l'implémentation et la diffusion des systèmes de type Do Not Track (Ne me suivez pas à mon insu et laissez-moi régler mes préférences de confidentialité). Actuellement cela se limite aux navigateurs Web, et seul le projet Mozilla Boot2Gecko (encore en développement) le prend directement en charge à partir du système d'exploitation.

Ces recommandations constituent une base de référence, et l'ensemble des acteurs (des développeurs d'applications aux fournisseurs d'accès et de services en passant par les régies publicitaires et bien d'autres) devraient tout faire pour les atteindre voire les dépasser. L'écosystème d'applications mobiles s'est développé et a mûri. Les utilisateurs sont en droit d'attendre désormais des politiques et des pratiques sérieuses et responsables. Il est temps de répondre à ces attentes.

Notes

[1] Crédit photo : Phil Campbell (Creative Commons By)

[2] La question, une fois de plus, se pose différemment si ces apps sont sous licence libre car la transparence est alors de mise.

[3] La non vigilance des utilisateurs de smartphones n'implique pas forcément la même imprudence pour leur ordinateur personnel. Il n'est ainsi par rare de rencontrer des *libristes* faisant très attention à ce qu'il y a dans leur PC mais installant à peu près n'importe quoi sur leur téléphone sous Android.