Vie privée :

Votre meilleur ennemi est dans la poche droite

par Jean-Luc MANISE
Toutes nos analyses sont disponibles sur le site **www.cesep.be**
Votre avis : secouezvouslesidees@cesep.be

Des TV qui vous regardent (LG) ou qui vous enregistrent (Samsung), des systèmes d'exploitation qui contrôlent vos achats (Microsoft), des capteurs intelligents qui savent combien vous êtes dans la chambre (Nest), c'est le tout venant. Au hit-parade de l'espionnage en temps réel, il y a... votre smartphone !

Souvenez-vous, c'était il y a 3 ans. Un programmeur britannique, Jason Huntly, découvre que sa TV l'espionne. Son modèle, une Smart TV de marque LG, mémorise les programmes visionnés, et en transmet la liste à l'entreprise sud-coréenne. L'appareil transmet également la liste des fichiers présents sur une clé USB qu'il a inséré dans la TV.

Huntly trouve comment désactiver la fonction de collecte ; pourtant, les infos continuent à être transmises. Il traite le sujet sur son blog. Devant le tollé que cela suscite, LG revoit sa copie et intègre dans son appli la possibilité de désactiver pour de bon la collecte de données.

Votre TV vous regarde...

L'année passée, c'est Samsung qui prend le relais. Lu dans sa clause de confidentialité Smart TV, section commande vocale qui fait elle aussi l'objet de « transferts » : « Veuillez noter que si vos propos contiennent des informations sensibles, personnelles ou autres, ces informations seront parmi les données saisies et transmises à un tiers par l'utilisation de la reconnaissance vocale ».

Combien de personnes sont dans la pièce ?

La collecte de données intéressent tous les «majors » du Net. De Google qui a racheté le fabricant de capteurs Nest à Microsoft qui a lancé l'année passée un Windows 10 fort curieux. Arne Empen, journaliste pour Arte Future : « Depuis le rachat de la société Nest Labs pour 3 milliards d'euros, Google peut désormais recueillir des données sur nos habitudes, nos modes de fonctionnement, ce que nous consommons, même sans caméra. Grâce aux capteurs intégrés dans les détecteurs de fumée et les thermostats, on peut savoir combien de fois le réfrigérateur a été ouvert, combien de personnes se trouvent dans telle pièce et à quelle heure, au dire même du co-fondateur et ex-patron de Nest ».

Windows 10, régie publicitaire en ligne

Lors de l'installation de Windows 10, Microsoft vous attribue un identifiant publicitaire, afin « d'améliorer la pertinence des publicités ». Windows n'est plus un système d'exploitation, c'est une régie publicitaire en ligne ! Afin d'assurer un maximum d'efficacité dans cette noble tâche, Microsoft récupère également via son navigateur Edge l'historique de votre navigation, vos favoris, et vos saisies dans la barre d'adresse. Si vous utilisez un compte utilisateur Microsoft, vos mots de passe pour l'accès à des applications en ligne ou installées sur votre ordinateur ainsi que vos codes Wi-Fi seront stockés sur serveurs Microsoft, et synchronisés.

Vos coups de fils, vos achats et bien plus...

L'assistant vocal Cortana n'est pas en reste. Lu cette fois dans les conditions d'utilisation de Windows 10 : « Pour permettre à Cortana de fournir des expériences personnalisées et des suggestions pertinentes, Microsoft recueille et utilise différents types de données, comme la localisation de votre appareil, les données de votre calendrier, les applis que vous utilisez, les données de vos e-mails et de vos SMS, les personnes que vous appelez, vos contacts et les personnes avec lesquelles vous interagissez sur votre appareil. Cortana en apprend également à votre sujet en recueillant des données sur votre manière d'utiliser votre appareil et d'autres services Microsoft, comme votre musique, vos réglages d'alarme, si l'écran verrouillé est activé, ce que vous regardez et achetez, votre historique de navigation et de recherche Bing, et bien plus ».

Quand c'est gratuit, c'est vous le produit

Mais la palme du flicage en temps réel revient assurément à... votre smartphone. L'utilisateur lambda télécharge en règle générale une petite trentaine d'applications, gratuites la plupart du temps. Qu'il s'agisse d'un matériel

Apple ou d'un écran Android, elles vont signaler aux annonceurs leur position géographique à 40 reprises, tout au long de la journée. Si vous téléchargez une application liée à un réseau social, elle vous cadrera minute par minute et transmettra non seulement les coordonnées de l'endroit où vous vous trouvez mais aussi votre numéro de téléphone, le numéro de votre carte SIM et votre numéro de série. N'y voyez pas malice : il s'agit simplement de connaître et idéalement d'anticiper votre comportement pour le monétiser.

« Cher abonné, vous êtes enregistré comme participant à un trouble massif de l'ordre public ».

Votre smartphone vous surveille minute par minute

En collaboration avec l'Inria, la CNIL, l'équivalent français de la Commission Belge Vie Privée, a développé un outil capable de détecter les accès à des données personnelles (localisation, photos, carnet d'adresse, ...). Il a été installé sur des smartphones que ses agents ont utilisé à la place de leur téléphone personnel pendant 3 mois : 189 apps iOS (iPod) et 121 applications Android ont été scannées. Dans les 2 environnements, entre 50 et 60 % des applications testées ont accédé à des identifiants du téléphone. Qu'est-ce que cela veut dire ? Que vos us et coutumes sont stockés ici et là dans des bases de données et que ces infos peuvent être utilisées pour créer des profils. Les plus gourmands en matière de flicage comportemental (traduisez flitrage collaboratif en langage marketing 2.0) sont les réseaux sociaux. Claude Castelluccia et Vincent Roca, chercheurs auteur de l'étude chez Inria Privatics : « La localisation est la donnée reine dans l'environnement des smartphones. Elle joue un rôle clé pour les services les plus utiles (car contextualisés) mais peut aussi constituer une intrusion importante dans les habitudes et comportements de la personne. Entre un quart et un tiers des applications y accèdent. Mais ce qui retient l'attention, c'est la fréquence d'accès. Ainsi, une application de service de réseau social a pu accéder plus de 1 million de fois à la géolocalisation et une deuxième application plus de 700.000 fois. Cela représente en moyenne près d'un accès par minute sur une période de 3 mois... ».

Déduire vos comportements

Si l'on peut comprendre que Facebook soit intéressé par ces infos de localisation au moment où l'un des utilisateurs de son réseau souhaite partager un contenu localisé, l'accès quasi permanent à cette information pose de facto question en matière de vie privée car ces bases de données de géolocalisation vont pouvoir être utilisées pour déduire voire anticiper vos comportements : lieux de sortie, achats, vacances, fréquentation d'établissements sportifs, de soins de santé, de lieux de culte, participation à des événements.

Des manifestants repérés par leur smartphone

Nous sommes le 22 janvier 2014. Tandis que les manifestations pro-européenne ont fait 4 morts et plus de 400 blessés à Kiev, les personnes présentes dans les environs des affrontements ont reçu ce message : « Cher abonné, vous êtes enregistré comme participant à un trouble massif de l'ordre public ». Selon le New York Times de l'époque, le gouvernement ukrainien a utilisé la fonction de géolocalisation des mobiles détectés sur les lieux des affrontement pour repérer les participants...

Cours toujours

Tous les amoureux branchés du bitume connaissent Runkeeper. La synthèse vocale de l'appli rythme la course des 45 millions d'utilisateurs : vitesse moyenne, vitesse par kilomètre, performance globale. Cerise sur le gâteau : vos performances peuvent être partagées automatiquement sur les réseaux sociaux Bingo ! Mais bingo pour qui ? En mai dernier, le Conseil des consommateurs norvégiens a déposé plainte auprès de l'équivalent norvégien de la Commission belge de défense de la vie privée. Il reproche à FitnessKeeper, l'éditeur de Runkeeper, de géolicaliser ses utilisateurs même s'ils sont au repos (intéressant pour les boîtes de pubs géo-ciblées de savoir s'ils se rafraîchissent après l'effort et où, histoire de leur suggérer quelque consommation bien sportive) . Dans son rapport, le Conseil indique que, lors de son test (48 heures), l'appli a transmis dix fois les données à une boîte de pub, toujours en mode repos. La CNC soupçonne encore FitnessKeeper de conserver les infos de façon indéterminée, histoire d'être relax dans ses contacts avec des annonceurs potentiels. On peut trouver cela bête. Reste que c'est en contradiction avec la législation européenne qui estime, c'est le moins, que le coureur soit prévenu et d'accord.

Espionné par défaut

A chaque fois, les éditeurs ont fait machine arrière et leurs applications peuvent être paramétrées pour devenir moins intrusives. Le hic est que, par défaut, c'est un espion que l'on place avec gourmandise dans sa poche ou son sac. Cours, Forest, cours !

Sources & Infos

Les smartphones et leurs apps sous le microscope de la CNIL et d'Inria. N° 8 Novembre 2014
Les objets connectés : des espions parmi nous. 29 octobre 2015, Arte Future
Complaint concerning the mobile phone app Runkeeper -10 mai 2016, ForbrukerRadet