Vos objets intelligents vous espionnent en continu !

Big Brother n'est pas autour de vous, il est installé dans votre poche

Les applications pour téléphones mobiles sont un concentré de violations de votre vie privée. Dans cette jungle administrée par les seuls intérêts privés de Apple et Google, hors de tout contrôle éthique, l'absence totale de législation protectrice laisse le champ entièrement libre à des de tous poils pour collecter tout sur vos habitudes de vie. Une manne de données collectées sans aucun mal qu'ils espèrent vendre (c'est l'objectif des simples magouilleurs à petits moyens) et dont ils rêvent de pouvoir tirer des indications hautement instructives (c'est le rêve des malhonnêtes à gros moyens).

La passivité de l'Europe en général et de la France en particulier est absolument consternante.

La donnée de base, c'est la géolocalisation GPS. Ensuite, un petit message programmé entièrement automatique permet d'envoyer toutes les quelques secondes vos coordonnées GPS avec l'identifiant de votre terminal à un serveur

C'est exactement ce que fait un petit bout de code installé sur instruction des autorités chinoises par défaut sur tous les terminaux vendables en Chine, ce qui permet aux services de police d'avoir les trajets d'activation de tous les terminaux des 1,5 milliard de Chinois.
Cerise sur le gâteau, ce code fonctionne aussi sur les terminaux vendus ailleurs dans le monde, comme le démontre la terrifiante bévue du fabricant NOKIA pourtant finlandais et ce qui n'est qu'une banale violation de la part d'une société chinoise larbinement à la botte du pouvoir chinois sans le moindre scrupule, OnePlus.

Pour Nokia, il n'est pas publié comment c'est réalisé ; c'est un utilisateur norvégien, apparemment un geek, qui s'est rendu compte des messages envoyés à chaque allumage du mobile
https://www.androidcentral.com/how-does-company-nokia-or-oneplus-mistakenly-collect-user-data-and-ship-it-server-china

the Nokia 7 Plus — the best phone from the new HMD-owned Nokia by far — was found to be sending private data from a Norwegian user's phone to a remote server in China. It seems that every time the phone was turned on, unencrypted data containing Henrik Austad's location, the SIM card number, and the phone's serial number went flying through the tubes to a Chinese server. HMD Global says this was an "error in the packing process of software" and that it has been fixed.

Cette version minimaliste ne tient elle-même pas la route ; personne n'éteint son téléphone mobile, et les autorités chinoises ne peuvent évidemment pas se satisfaire de la seule indication de la boutique où un résident achète et active son terminal…
En réalité un examen plus attentif par une société spécialisée norvégienne montre que ces données sont bien, évidemment, envoyées en continu
https://www.frandroid.com/marques/nokia/577593_le-nokia-7-plus-a-transmis-des-donnees-personnelles-en-chine-la-finlande-ouvre-une-enquete

Il a été établi que les données sont envoyées à l'opérateur d'Etat chinois China Mobile
L'autorité finlandaise type CNIL vient, quatre mois après la révélation des faits, seulement d'ouvrir une enquête ; la CNIL en France évidemment ne fait rien : l'incompétence de cette instance qui sert de simple paravent aux pratiques illicites de tous genres n'est plus à illustrer

Pour OnePlus, c'est une application ''constructeur'' appelée ClipBoard , intégrée au système d'exploitation, c'est-à-dire impossible à supprimer, qui fait le job
https://www.frandroid.com/marques/oneplus/485380_accuse-de-transferer-des-donnees-en-chine-oneplus-se-defend-de-nouveau

Pour les téléphones de la marque Wiko, ce sont deux applications fournies par le fabricant, appelées ApsaleTracker et ApeStsMonths, qui procèdent à la collecte des données, et les envoient semble-t-il une fois par mois, ce qui est plus habile et beaucoup plus difficile à détecter, à la maison-mère du dit fabricant, Tinno Mobile Technologies. **Ces applications outre récupérer des données d'identification et de localisation peuvent aussi lire vos SMS, et même écrire des messages de ce type**.
https://www.frandroid.com/marques/wiko/471870_wiko-sts-collecte-donnees-personnelles

Il y a un an, c'est Facebook qui avait été pris la main dans le sac ; leur application mobile récupérait toutes les données des contacts et en plus toutes les données d'appels voix et de SMS (quel numéro, avec l'horodatage). Une pratique qui relève du délit de droit commun au même titre que l'ouverture de votre courrier. Là encore on doit constater l'incroyable passivité des mêmes autorités européennes et françaises, qui semblent n'avoir même pas convoqué Facebook pour des explications et exiger une destruction de ces données. L'Assurance-retraite par exemple a pris la mesure du sujet et a désactivé son interface de communication avec les usagers via Facebook et l'a fait savoir par un communiqué de presse du 4 avril 2018
https://www.lassuranceretraite.fr/portail-info/accueil voir la rubrique Liste des communiqués de presse