Fitbit Gare aux programmes en entreprise

Il est 6 heures du matin quand le bracelet « Fitbit Blaze » d'Anna se met à vibrer pour la réveiller en douceur. L'assureur de son employeur – une grande entreprise américaine – a équipé chaque membre de la société d'une montre *Fitbit Blaze*. Cette technologie permet, grâce aux capteurs corporels dont elle est dotée, de mesurer – entre autres – l'activité physique, le nombre de pas, la fréquence cardiaque, les heures de sommeil de celui qui la porte. Anna n'a pas osé la refuser. Son patron était convaincant : en acceptant *« librement »* de la porter et de partager les données captées avec lui, *« l'intérêt est réciproque »*. Les employés en profitent pour améliorer leur activité physique et augmenter leur bien-être et font, par la même occasion, bénéficier l'entreprise d'une assurance santé beaucoup moins coûteuse. *« Que du bonus ! »*

En se levant, Anna consulte son « journal de bord » sur l'application mobile Fitbit reliée à la montre connectée. Le constat est vite fait : son petit écart au restaurant lui aura valu 550 calories de plus que recommandé. Elle ne prendra donc pas de petit-déjeuner.

Une notification apparaît. L'application lui rappelle de faire du sport, elle enfile donc ses baskets pour aller courir. Mais rapidement, sa fréquence cardiaque s'accélère jusqu'à atteindre un seuil inquiétant. *« Bizarre… »*, s'étonne-t-elle. Elle ne se sent pourtant pas fatiguée. Elle ralentit tout de même le pas, de peur que son cœur ne s'emballe.

A peine arrivée au bureau, son employeur la félicite pour sa séance de sport matinale qui la mettra *« sans aucun doute dans les meilleures conditions de travail pour le reste de la journée »*. Au détour du couloir, il lui conseille tout de même de garder un œil sur sa santé, et d'aller passer quelques tests cardiaques *« pour être sûr »*. Un collègue pousse la porte du bureau et ne tarde pas à complimenter Anna pour le nombre de pas qu'elle a déjà parcourus depuis son réveil.

Au moment de rentrer chez elle, le patron d'Anna, ayant remarqué son manque de concentration durant l'après-midi, l'interpelle brièvement pour lui suggérer d'aller dormir plus tôt qu'hier, *« ainsi, elle sera en meilleure forme demain… »*

Cette histoire est inventée. Pourtant elle jette un coup de projecteur sur une réalité déjà bien ancrée outre-Atlantique. Il n'est pas rare que des entreprises américaines demandent à leurs employés de porter des traqueurs d'activité afin d'évaluer la productivité de leur personnel. Selon le *Chicago Tribune*, *« au cours de (l'année 2016), 31 % des 510 entreprises américaines comprenant 1.000 employés ou plus, interrogées par l'entreprise de consultance Willis Towers Watson, ont eu recours à cette pratique. Tandis que 23 % d'entre elles envisagent d'adopter le projet au cours des deux prochaines années. »*

Fitbit@Work

Selon le cabinet IDC, avec 23 % des parts du marché mondial des traqueurs d'activité et montres de fitness au dernier quadrimestre 2016, Fitbit se place en tête, suivie par Xiaomi, Garmin et Apple. Pour atteindre les entreprises, la société californienne a développé la plate-forme Fitbit@work. Les données personnelles, d'activité physique et de santé des employés sont ainsi partagées avec leur employeur et l'assureur de la compagnie.

Mais toutes ces données sensibles qu'un employé abandonne à son entreprise ne pourraient-elles pas se retourner contre lui ? Selon Antoine Delforge, chercheur au Centre de recherche information droit et société (Crids, UNamur), une société qui propose ce type de programme doit, dès le départ, être totalement explicite et transparente envers ses employés. *« Ceux-ci doivent être avertis non seulement de la finalité du projet et de la nature exacte des données qu'ils partagent, mais aussi connaître l'identité des personnes et des organisations qui auront accès à leurs données individuelles et agrégées. »* Ces conditions sont valables pour l'inscription à Fitbit@work. Pour éviter à l'entreprise de se mettre en porte-à-faux face aux lois américaines sur la protection des données et de bien-être au travail, elles sont d'ailleurs minutieusement décrites sur son site.

Vers une assurance santé individualisée ?

Une autre obligation inscrite sur cette page internet attire l'attention du chercheur : l'adhésion au programme doit se faire sur base volontaire. *« Mais le caractère volontaire de la participation à la plate-forme peut poser certaines questions,* ajoute Antoine Delforge. *On pourrait imaginer que des membres du personnel se sentent obligés d'y prendre part à cause de la relation de subordination qui existe entre eux et leurs employeurs. »* Et ce n'est pas tout : le refus d'un employé pourrait aussi être interprété comme un indice de « mauvais risque » par l'employeur ou l'assureur… et mener à des discriminations.

Pour les mutuelles et autres assurances santé, les données agrégées et récupérées dans les entreprises qu'elles « parrainent » en bracelets connectés représentent un précieux butin. En analysant toutes les données utilisateurs rendues anonymes, les assureurs élaborent des algorithmes qui permettent ensuite de catégoriser statistiquement les clients « les plus risqués ». De cette manière, elles peuvent adapter leurs primes à chaque client.

Mais avec l'avènement de programmes partageant des données personnellement identifiables aux assurances, comme Fitbit@work, un autre scénario se dessine à l'horizon… celui d'une singularisation des risques. Dans un tel scénario, s'ils veulent bénéficier d'un barème plus avantageux, les individus devraient alors démontrer à leur mutuelle qu'ils mènent un mode de vie sain. Les appareils connectés renverraient directement – chiffres et graphiques à l'appui – la preuve d'une activité physique ou d'heures de sommeil suffisantes. *« On observe déjà ce fonctionnement chez les assureurs automobiles*, explique Antoine Delforge. *Ils stockent des données très précises sur le passé du conducteur et adaptent leurs primes en fonction des informations détenues. »* Autant savoir. ■

MARGOT DEVILLE

géolocalisation Souriez, vous êtes pisté !

Tinder, Waze ou Park Indigo, voilà plusieurs applications qui connaissent un véritable succès sur smartphone. Toutes les trois fonctionnent grâce au principe de la géolocalisation : par antennes GSM ou routeurs wifi, une personne ou un objet est localisé grâce à ses relais de proximité.

Mais cette technique a aussi ses côtés sombres. Si l'utilisateur tire profit des applications, il n'est pas rare que les applications tirent elles aussi profit de ses utilisateurs. Publicités ciblées, enregistrement des données personnelles ou encore localisation perpétuelle : les apps de géolocalisation sont de véritables traqueurs pour des utilisateurs constamment suivis mais rarement mis au courant de ces pratiques de pistage.

L'IPhone, smartphone commercialisé par Apple, est une mine d'or en ce qui concerne les informations de géolocalisation. Pourquoi ? Tout simplement parce que l'entreprise à la pomme enregistre l'ensemble des lieux où nous allons et stocke toutes ces informations dans un dossier présent dans l'appareil. Avec Apple, pas besoin d'applications de géolocalisation pour être géolocalisé, l'IPhone vous localise sans qu'aucune app ne soit lancée.

Une porte dérobée

Les applications de géolocalisation peuvent aussi être la porte dérobée par laquelle une localisation clandestine de l'utilisateur est offerte aux regards malveillants. Pour le démontrer, nous avons réalisé une expérience avec un informaticien spécialisé dans ces apps. A l'aide d'un simple ordinateur et de Wireshark (un logiciel gratuit et libre d'accès, cfr. page 26), il nous a été possible de localiser une personne et d'avoir accès à certaines de ses données personnelles.

Pendant quelques jours, cette personne a utilisé quotidiennement plusieurs applications fonctionnant via un logiciel de géolocalisation (Tinder, Foursquare, Swarm…) A Bruxelles, à Louvain-la-Neuve puis à Gand, cet utilisateur s'est promené dans plusieurs endroits différents du pays. Ensuite, grâce à un ordinateur et à une simple connexion du smartphone à une borne wifi, notre informaticien complice a pu « entrer » dans le téléphone de l'utilisateur. Après seulement quelques minutes, il a ensuite pu consulter de nombreuses informations confidentielles de l'utilisateur liées aux applications de géolocalisation : ses photos de profil sur les différentes apps, les photos de profil de ses « amis ». Plus intéressant, l'informaticien a su localiser l'utilisateur qui avait employé Foursquare. Cette application permet à son utilisateur de se localiser dans un lieu (un restaurant, un bar…) via un « check-in ». Après s'être localisé, il donne son avis sur l'établissement et gagne des points en fonction des endroits visités. Dans le cas qui nous intéresse, l'informaticien a réussi à connaître le lieu, mais aussi l'heure et la date à laquelle l'utilisateur était présent dans l'un de ces bars. Via le logiciel, l'informaticien a donc su localiser de manière précise l'utilisateur de cette application, sans que celui-ci ne soit au courant de cet usage détourné. ■

FRANÇOIS GARITTE

Les apps de géolocalisation sont de véritables traqueurs pour des utilisateurs constamment suivis.

© D.R.

LinkedIn Comm

A l'inscription, LinkedIn sollicite nom, prénom, e-mail, code postal ainsi que le job pour lequel le membre travaille ou souhaiterait travailler. Rien d'anormal pour un réseau social professionnel. LinkedIn souhaite ensuite accéder à la messagerie de l'internaute pour *« lui proposer des connexions et l'aider à créer son réseau »*. Mais même s'il refuse de donner son adresse mail, le nouveau membre se verra suggérer une quinzaine d'individus qu'il pourrait connaître. Le réseau se serait-il introduit de force dans sa boîte mail ?

Edouard Cuvelier, chercheur en sécurité informatique à l'UCL, n'en est pas convaincu. *« LinkedIn n'a pas besoin d'avoir accès au mail de quelqu'un pour trouver ses connaissances. Il peut tout simplement accéder à ses informations via d'autres utilisateurs qui, eux, ne se protègent pas correctement. Avec les carnets d'adresses, il sait retracer les liens qui unissent différentes personnes. Finalement, il a besoin d'un seul individu qui lui ouvre les portes pour pou-*