DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

LE SPORT CONNECTÉ EST RISQUÉ POUR LA VIE PRIVÉE

Publié le 10 janvier 2023

par Christian Du Brulle

Cyclisme, course à pied, randonnée… Si vos performances physiques s'améliorent avec le temps et la pratique, en matière de protection de la vie privée par contre, vos applications sportives ont encore bien des progrès à faire. Certaines de leurs fonctionnalités ne fourniraient qu'un faux sentiment de sécurité à leurs utilisateurs. Notamment en ce qui concerne leur géolocalisation. Cette conclusion, ce sont trois chercheurs de l'Université catholique de Louvain (KULeuven) qui la formulent.

« Les applications de sport et de fitness gagnent en popularité d'année en année », notent-ils. « L'application Strava comptait l'an dernier plus de 100 millions d'utilisateurs dans 195 pays. Runtastic, d'Adidas, totalisait même 182 millions d'utilisateurs enregistrés. »

Réseaux sociaux

Ce ne sont là que deux exemples de la popularité des réseaux sociaux qui se sont développés autour des activités sportives. Chaque jour, des millions de séances dans le monde sont partagées avec des amis et d'autres utilisateurs de l'application ou avec une communauté virtuelle de supporters.

« Le problème, c'est qu'on partage sur ces réseaux des données très personnelles, et parfois, sans le savoir, la localisation exacte de son domicile ou de son lieu de travail. Des lieux qui peuvent coïncider avec le point de départ ou d'arrivée des activités sportives », pointent les chercheurs.

Les applications permettent généralement de masquer ces emplacements. Mais l'équipe du groupe imec-DistriNet de la KULeuven a découvert que, dans de nombreux cas, cette option donnait un

faux sentiment de sécurité à l'utilisateur.

Identification de zones militaires confidentielles

A titre d'exemple, les chercheurs rappellent que dans un passé pas si lointain, des militaires avaient révélé à leur insu l'emplacement de sites confidentiels en partageant leurs circuits sportifs. Autre exemple de l'usage détourné de ce genre d'informations: le vol d'équipements sportifs, comme des vélos de valeur, au domicile de sportifs.

« Même les nouveaux moyens de protéger ses données de localisation ne sont pas infaillibles », indiquent les ingénieurs qui ont passé ces applications au crible. « Sans oublier que les activités que vous partagez en disent également long sur vous. Très souvent, vous pouvez y découvrir des schémas : des lieux et des heures fixes pour l'exercice, des itinéraires fixes… »

Pour éviter de divulguer purement et simplement ces données, les réseaux sociaux fonctionnent souvent avec des zones de confidentialité aux extrémités (départ/arrivée) des parcours partagés. Ces zones permettent de masquer des zones autour de lieux sensibles.

L'utilisateur décide du périmètre de cette zone où les informations de géolocalisation sont moins précises. Cela fonctionne souvent par cercles concentriques dont on choisit la dimension. Mais même cette approche créerait un faux sentiment de sécurité, montre l'équipe de la KULeuven.

Les données croisées sont révélatrices

« L'aperçu de votre activité ainsi protégée contient encore tellement de données sur, par exemple, la distance parcourue et l'itinéraire emprunté que, combiné à un plan de ville, il révèle encore votre point de départ ou d'arrivée », estime le chercheur Karel Dhondt.

Pour le prouver, les membres de l'équipe ont croisé des données personnelles des utilisateurs avec leur zone d'activité anonymisée. Au total, 1,4 million de séances « Strava » ont été analysées. « Nous avons été en mesure de découvrir jusqu'à 85 % des lieux théoriquement cachés, uniquement sur la base des données supplémentaires révélées publiquement », explique Victor Le Pochat, du groupe imec-DistriNet.

Pour tenter d'améliorer cette confidentialité, l'équipe a non seulement transmis ses résultats aux plateformes concernées, mais elle a également proposé diverses pistes d'amélioration.

Les applications pourraient à l'avenir mieux masquer les informations relatives à la distance parcourue dans la zone cachée, voire les omettre complètement. Cette dernière intervention aurait toutefois un impact important sur les utilisateurs, car l'activité ne serait plus entièrement enregistrée. Une alternative serait, pour les applications en question, de permettre de varier davantage la forme et la taille des zones cachées, et non se limiter à des cercles.

« En tant qu'utilisateur, vous pouvez également mieux protéger votre vie privée sur les applications sportives », explique encore l'équipe de la KULeuven. « La mise en place d'une zone de confidentialité est de toute façon une bonne idée, mais faites en sorte que la zone autour des endroits que vous voulez garder cachés soit suffisamment grande. Souvent, le minimum est de 200 mètres, mais vous pouvez augmenter la zone à plus d'un kilomètre. Plus c'est gros, mieux c'est », souligne le chercheur Karel Dhondt. « Et varier davantage vos points de départ et d'arrivée est également une stratégie efficace ». Des conseils à mettre en œuvre dès la prochaine sortie.