

Enquête. Le passé suspect de Monsieur Pokémon Go



(http://www.courrierinternational.com/sites/ci_master/files/styles/image_original_1280/public/assets/images/pokemon_theintercept_01.jpg?itok=PcZg7lnY)

Avant de lancer l'application la plus téléchargée au monde, John Hanke a fait carrière chez Google. Spécialiste de la cartographie, il s'est retrouvé au cœur de l'affaire Wi-Spy, “le plus grand scandale d'atteinte à la vie privée de l'ère Internet”, détaille The Intercept.

Sorti le mois dernier [le 7 juillet aux Etats-Unis], le jeu de réalité augmentée *Pokémon Go* aurait battu en seulement deux semaines les records de popularité de Twitter, Facebook et Netflix chez les utilisateurs de téléphones Android. Côté Apple, le jeu a été plus téléchargé lors de sa première semaine que n'importe quelle autre application dans l'histoire de l'Apple Store.

Le succès phénoménal de ce jeu n'a pourtant d'égal que l'avidité avec laquelle il aspire les données personnelles de ses utilisateurs. Contrairement à Twitter, Facebook ou Netflix, *Pokémon Go* exige d'avoir un accès ininterrompu à votre caméra et à votre localisation, soit “une véritable mine de données sensibles et personnelles (<https://epic.org/privacy/ftc/FTC-letter-Pokemon-GO-07-22-2016.pdf>)”, écrit une association de lutte pour le respect de la vie privée dans une lettre aux régulateurs fédéraux américains.

L'information est d'autant plus inquiétante que *Pokémon Go* est la propriété d'un homme qui a été au cœur d'une des plus graves controverses depuis les débuts d'Internet. Un homme qui, grâce aux voitures Google chargées de cartographier chaque recoin de ville pour le service Google Street View, a secrètement enregistré des masses d'informations privées : activité de réseaux Internet privés, mots de passe, e-mails, dossiers médicaux, situations financières, fichiers audio et vidéo.

Pionnier de la géolocalisation

Avant de prendre la tête de Niantic Labs [la société qui a développé le jeu *Pokémon Go*], John Hanke a dirigé le département "Geo" de Google et s'est retrouvé chargé de presque tous les projets liés à la localisation. C'était précisément à l'époque où le célèbre moteur de recherche commençait à faire bien plus que cataloguer des pages web et s'apprêtait à répertorier le moindre pâté de maisons construit sur la planète.

Fondateur de Keyhole, une société d'imagerie satellitaire extrêmement populaire et qui a bénéficié du soutien financier de la CIA, Hanke est entré chez Google en 2004 après le rachat de sa société, rebaptisée Google Earth en 2005. Deux ans plus tard, Hanke était globalement responsable de tout ce qui avait trait à la cartographie chez Google. Un portrait de *Wired* (http://archive.wired.com/techbiz/it/magazine/15-07/ff_maps?currentPage=all), publié en 2007 ("*Google Maps is changing the way we see the world*"), le présentait comme un véritable pionnier. Dans cet article illustré d'une photo de l'intéressé en digne successeur du dieu Atlas, un énorme globe reposant sur ses épaules, on pouvait lire :



Sous la direction de John Hanke, Google Earth et Google Maps mettent les outils de cartographie à disposition du monde entier."

Google était alors en pleine effervescence. Supplantant ses rivaux de MapQuest, Google Maps était devenu incontournable et la firme de Mountain View avait de grandes ambitions pour monétiser ces informations cartographiques. Mais avant de pouvoir revendre la Terre à ses occupants, Google devait la numériser : une armada de voitures équipées de capteurs et estampillées Google Street View se mirent à sillonner toutes les villes, autoroutes et pistes de la planète pour photographier le moindre bâtiment, arbre ou poteau s'offrant à leur objectif. Google ajouta ensuite ces photos à ses cartes via une API (interface de programmation applicative), qui est aujourd'hui le socle sur lequel *Pokémon Go* – et bien d'autres applications – a bâti son succès.

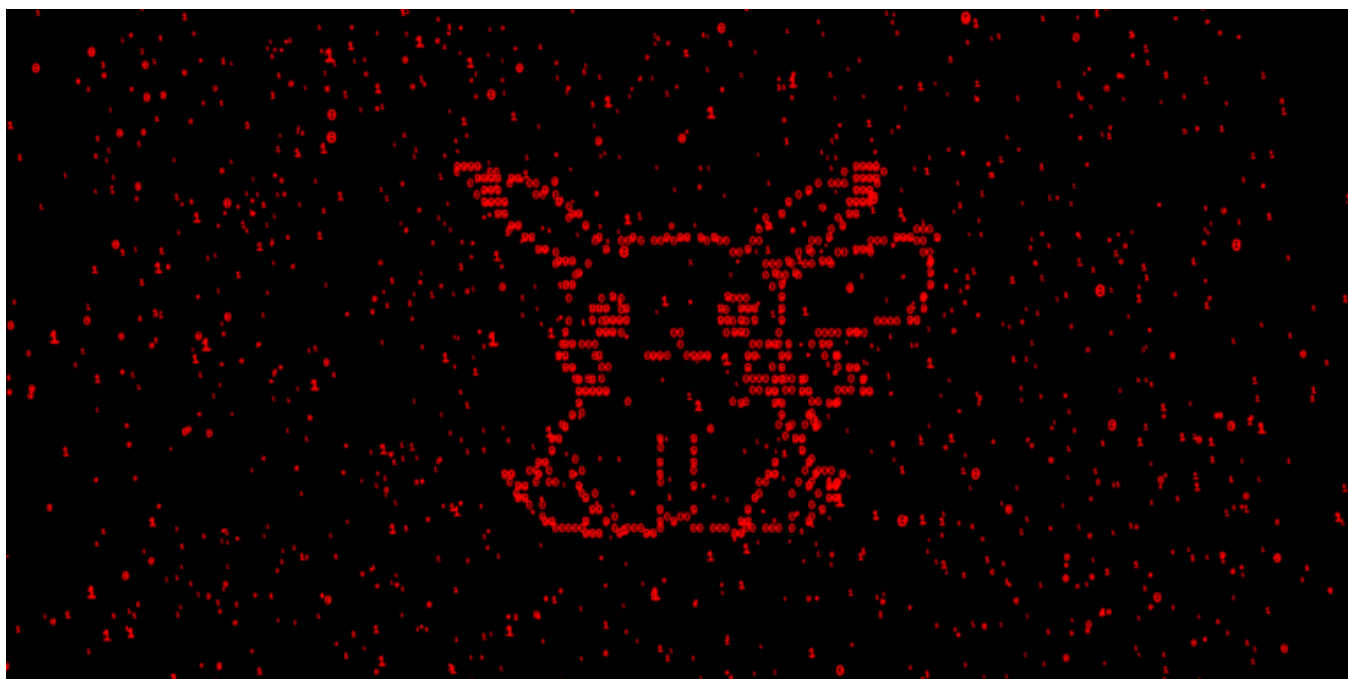


Illustration d'Erik Carter pour *The Intercept*.

C'est en avril 2010 qu'une autorité allemande de protection des données révèle que ces voitures ont récupéré illégalement des données de réseaux WiFi privés. Les investigations d'autres instances de contrôle et de la presse finissent par faire éclater la vérité : sur leur passage, les voitures de Google Street View ont collecté un grand nombre de données sur des réseaux non protégés. Le commissaire allemand pour la protection des données, Peter Schaar, se déclare "horrié" et "stupéfait". Aux Etats-Unis, cette collecte illégale d'informations s'est étalée sur plus de deux ans. L'affaire Wi-Spy entraîne plusieurs conséquences :

- la collecte de données sur des réseaux WiFi est déclarée illégale au Royaume-Uni, en France, au Canada, en Corée du Sud et en Nouvelle-Zélande ;
- un directeur de la FCC (Commission fédérale des communications) déclare que l'activité de Google "est une infraction manifeste au respect de la vie privée" et la société est condamnée à payer 25 000 dollars d'amende [22 000 euros] ;
- une enquête est ouverte (<https://epic.org/privacy/streetview/DOJ-Google-Street-View-Investigation-Letter-05272011.pdf>) par le ministère de la Justice américain ;
- un recours collectif (*class action*) est lancé contre Google, dans le cadre duquel une cour fédérale de grande instance et une cour d'appel rejettent les arguments de Google et précisent que les données illégalement collectées sont protégées par la loi du Wiretap Act (la Cour suprême rejette la demande d'appel déposée par Google) ;
- les autorités espagnoles portent plainte contre Google ;
- les autorités de régulation interviennent en Italie et en Hongrie ;
- le gouvernement allemand ouvre une enquête.

Par l'intermédiaire de son porte-parole, Hanke dément toute implication dans le scandale et rejette la faute sur le département Mobile de Google. C'est pourtant bien une entité de son

service qui est au cœur de l'enquête ouverte par les autorités américaines et c'est bien de son département que dépendaient les voitures de Google Street View mises en cause. Les antécédents de John Hanke devraient aujourd'hui alerter les joueurs de *Pokémon Go* (et leurs parents).

Alors que l'affaire devient publique, Google tente de se soustraire à ses responsabilités, balayant toutes les craintes, repoussant les demandes des enquêteurs, bref, manifestant toute l'arrogance qui lui est régulièrement reprochée. Au début du scandale, Google récuse toute accusation et affirme sur un blog que ses voitures n'ont collecté aucune donnée de réseau WiFi mais uniquement *"des informations permettant d'identifier les réseaux et leur système opératoire"*, autrement dit des choses comme le nom de votre réseau que tout le monde peut voir.

Sauf que deux semaines plus tard, alors que la pression des diverses autorités américaines et étrangères s'accroît, Google passe des dénégations à la désignation d'un bouc émissaire. L'entreprise reconnaît avoir copié des données de trafic mais de manière *"fragmentaire"* et *"par accident"*. Ses dirigeants tentent de rejeter l'entière responsabilité de la faute sur un ingénieur *"un peu trop entreprenant qui travaillait sur un projet expérimental"*.

Et pourtant, deux mois plus tard, un des vice-présidents du département de Hanke reconnaît dans un billet de blog (<https://googlepolicyeurope.blogspot.fr/2010/07/street-view-driving-update.html>) :



De graves erreurs ont été commises dans la collecte de données WiFi que nous nous sommes efforcés de corriger rapidement. [...] Les capteurs WiFi ont été retirés des voitures."

Pour l'entreprise, cet incident reste néanmoins une simple erreur. Trois mois plus tard, tout en répétant qu'il s'agissait d'une *"erreur"*, un autre message sur un blog de Google (<https://googleblog.blogspot.fr/2010/10/creating-stronger-privacy-controls.html>) reconnaissait que l'entreprise avait récupéré des e-mails, des adresses URL et des mots de passe.

Ce n'est que face aux demandes de plus en plus véhémentes de la FCC (Commission fédérale des communications) – exaspérée par les *"entraves et retards délibérés"* du géant du web – que Google finit par révéler la vérité. Vérité résumée dans un rapport sévère de la FCC publié en 2012 (<https://epic.org/privacy/google/FCC%20Google%20SV%20Enforcement%20UNREDACTED.pdf>). Loin d'avoir agi seul, l'entrepreneur "ingénieur X" avait ouvertement discuté de son code avec d'autres ingénieurs de Google, y compris certains de ses supérieurs.

En réalité, il avait même mis en garde ses collègues et envoyé un document de travail aux responsables du projet Street View, qui l'ont fait circuler auprès de toutes leurs équipes. *"Ce document de travail, note la FCC, formulait plusieurs 'inquiétudes concernant la vie privée' et suggérait un passage en revue devant un conseil, ce qui n'a jamais été fait."* Le document indiquait clairement qu'il jugeait *"problématique que l'on enregistre des données d'utilisateurs avec*

suffisamment d'autres informations pour savoir précisément où se trouvent les gens et ce qu'ils font". Difficile de faire plus clair.

D'après le rapport de la FCC, pendant l'élaboration du projet, "à au moins deux reprises", "l'ingénieur X a informé ses collègues que les voitures de Street View collectaient des données réseaux" et qu'elles partageaient même certaines informations personnelles. En 2008, dans un échange de mails, un "haut responsable du projet Street View" qualifiait "d'intéressante" l'analyse de quelque 300 millions de paquets de données WiFi contenant près de 32 000 adresses web. "Est-ce que vous êtes en train de me dire que ces URL ont été extraites des paquets de données WiFi que nous avons récoltés avec les voitures ?" demanda le supérieur à l'ingénieur X. Ce dernier confirma : "Les données ont été collectées en plein jour pendant que l'essentiel du trafic web est effectué depuis des lieux de travail (c'est-à-dire sur des réseaux sécurisés). Mais je ne pense pas que les chiffres soient suffisants pour constituer un bon échantillon."

Masses d'informations non protégées

Les documents transmis aux régulateurs européens et analysés par la FCC révèlent que Google a collecté toutes sortes de données, y compris des informations liées à des sites de rencontre et des préférences sexuelles. Au final, ce sont peut-être les données de centaines de milliers d'internautes qui ont ainsi pu être secrètement récupérées par des voitures Google dont la mission officielle était de localiser des réseaux WiFi. Les voitures de Google n'ont pas seulement récupéré des noms de routeurs WiFi, elles ont aspiré des masses d'informations non protégées envoyées depuis ou sur ces routeurs au moment de leur passage, notamment des sites favoris, des recherches web et des e-mails.

Il va de soi que même des données fragmentaires peuvent en dire long sur les centres d'intérêt d'une personne et que la plupart des gens préfèrent que ces informations restent confidentielles. Tout cela s'est produit alors que John Hanke dirigeait le département Geo de Google, qui abrite Google Street View et Google Maps. Si l'entreprise a fini par prendre des mesures pour mieux respecter la vie privée des gens, le fait est que personne n'a levé un sourcil quand des ingénieurs parlaient ouvertement de collecter des données réseaux de particuliers.

Cela tient peut-être à la culture de Google. Dans un entretien au <http://www.thetimes.co.uk/tto/technology/article1859450.ece>) Times (<http://www.thetimes.co.uk/tto/technology/article1859450.ece>), en 2009, Hanke déclarait :

“

En tant qu'entreprise, on ne fait peut-être pas toujours l'unanimité, mais je pense que personne ne peut vivre sa vie – en tant qu'individu ou en tant qu'entreprise – sans jamais vouloir piétiner quelques plates-bandes. Nous devons louver entre les bénéfices d'un potentiel service et le respect de la loi et des mœurs sociales.”

Peu après la publication du rapport de la FCC, le **New York Times** désigna un certain Marius

Milner comme le fameux "ingénieur X". Spécialiste des systèmes de sécurité et figure bien connue de la communauté des hackers, Milner a refusé de détailler son rôle dans ce fiasco sur la collecte de données et s'était contenté à l'époque de déclarer que l'idée défendue par Google qu'il avait agi seul invitait à *"beaucoup de réflexion"*. Quatre ans après le départ de John Hanke – qu'il affirme n'avoir *"jamais rencontré"* –, l'ingénieur "trop entreprenant" confirme qu'il travaille toujours pour Google.

Il se trouve que Milner a aussi des liens avec le projet *Pokémon Go* puisqu'il est l'un des cinq coauteurs – avec Hanke – d'un brevet détenu par la société Niantic Lab (<https://www.google.com/patents/US8968099>)s, *"un système et une méthode permettant de transporter des objets virtuels dans un jeu de réalité parallèle"*.



John Hanke, fondateur de Niantic Labs, à Tokyo, le 15 juillet 2016. Photo Toru Hanai /REUTERS

D'après Milner, le brevet serait né d'une idée *"discutée entre amis, dont l'un des coauteurs du brevet"*. Il affirme n'en avoir jamais parlé directement à Hanke. Il est intéressant de noter que Google a déposé sa demande de brevet en 2012, soit deux ans après avoir fait porter le chapeau à Milner dans l'affaire des voitures de Google Street View. L'office des brevets et des marques américain l'a attribué en 2015 à Niantic, une petite entreprise de réalité augmentée alors peu connue.

Hanke avait lancé Niantic comme un projet parallèle à l'époque où il travaillait pour Google, en 2010. Un an plus tard, Niantic devient une filiale de Google pour pouvoir collaborer avec un plus grand choix de partenaires. Google et Nintendo financent la start-up à hauteur de 20 millions de dollars – même si la part exacte de Google n'est pas connue.

En quittant le giron de Google, Niantic emporte le brevet dans ses valises. Brevet qui présente explicitement comment un jeu comme *Pokémon Go* peut être utilisé pour collecter des données sur les joueurs à leur insu. *“L’objectif du jeu peut être directement lié à une activité de collecte de données : par exemple lorsque le jeu implique que l’utilisateur récupère des informations dans le monde réel et les transmette pour compléter un objectif.”*

Le brevet cite également, à titre d’exemple, un article universitaire de Sebastian Matyas paru dans l’ (<http://citeseerx.ist.psu.edu/viewdoc/citations;jsessionid=ACBB4BDDDB904AB18A1F4B48E8D660E02?doi=10.1.1.84.7142>) *International Journal of Virtual Reality* (<http://citeseerx.ist.psu.edu/viewdoc/citations;jsessionid=ACBB4BDDDB904AB18A1F4B48E8D660E02?doi=10.1.1.84.7142>) :

“

Tout l’enjeu est d’inciter l’utilisateur à fournir des données en permanence, y compris une fois passé l’effet de la nouveauté. Le processus de collecte des données doit être divertissant pour maintenir le niveau d’engagement des participants à long terme. Nous sommes convaincus que les aspects ludiques et divertissants jouent un rôle essentiel dans ce genre de services de collecte de données.”

Le rapport de la FCC suggère une explication quant au fait que Hanke plaide non coupable : les avertissements de Milner – écrits et oraux – auraient tout simplement été ignorés. *“Les responsables du projet Street View et leurs collaborateurs ont déclaré ne pas avoir lu les documents [de Milner].”* Même s’ils ont été envoyés à toute l’équipe.

La confusion vient peut-être du fait qu’à l’époque Milner travaillait pour YouTube [qui a été racheté par Google en 2006], ne relevant pas des départements Mobile ou Geo de Google – et qu’il aurait créé son projet de collecte de données WiFi en parallèle de son travail [Google permet à ses salariés de consacrer 20 % de leur temps à des projets personnels]. Tout en indiquant que le département Mobile était à l’origine de l’opération de localisation des réseaux WiFi, Google affirme que ce service ne contrôlait pas le travail de Milner et que ses responsables n’avaient *“pas l’intention de recueillir des données utiles”*.

Le programme de Milner a pourtant été déployé sur les voitures de Street View, sous la direction de Hanke, afin de permettre aux conducteurs et aux piétons de se situer sur la version mobile de Google Maps (qui faisait partie du service de Hanke) et sur le système d’exploitation mobile d’Android (relevant d’un autre département). Sur son blog officiel, Google explique (<https://googleblog.blogspot.fr/2010/05/wifi-data-collection-update.html>) que deux services – Google Maps et le département Mobile – ont reçu des données récupérées par le programme de Milner (qui ne relevait d’aucun de ces deux services).

La seule chose qui apparaît clairement, c’est que tout le monde cherche à rejeter la faute sur son voisin. Vu l’ampleur du succès de *Pokémon Go* aujourd’hui et le nombre de données

personnelles auquel le jeu a accès, on retiendra surtout qu'un service a pu être utilisé – à l'insu de ses responsables ou non – pour permettre à un ingénieur de collecter des quantités de données sensibles tandis que sa hiérarchie fermait les yeux sur tous les avertissements qu'il avait formulés à l'écrit et à l'oral. L'Electric Privacy Information Center (Epic) fait déjà monter la pression sur Niantic et son PDG.

“Réfléchissez avant de jouer à ‘Pokémon Go’”

Dans un courrier adressé le mois dernier à la FTC (Commission fédérale du commerce), l'Epic déclarait :



Ces antécédents laissent penser que Niantic continuera à enfreindre les lois sur la sécurité et la vie privée des consommateurs. Compte tenu de la popularité de Niantic et du nombre de données sensibles collectées, la FTC doit redoubler de vigilance. [...] Les activités passées de Google Street View ne donnent guère de raison de croire aux discours rassurants sur les pratiques de Niantic.”

Jointe par téléphone, une responsable de l'Epic, Claire Gartland, explique que le scandale de Google Street View devrait inciter tous les joueurs de *Pokémon Go* à “réfléchir à deux fois avant de leur faire confiance”. Elle ajoute qu'il est “crucial que la FTC veille à ce que Niantic se montre de plus en plus scrupuleux sur le sujet vu les quantités de données que la société récupère”.

Les conditions d'utilisation de *Pokémon Go* indiquent clairement que “l'application est un jeu basé sur les coordonnées géographiques. Nous recueillons et stockons des informations sur votre localisation (ou celle de votre enfant autorisé) lorsque vous (ou votre enfant autorisé) utilisez notre application et suivez des actions de jeu qui utilisent les services de localisation mis à disposition par le système d'exploitation mobile de votre appareil (ou celui de votre enfant autorisé), qui fait usage de la triangulation du signal, du WiFi et/ou du GPS. Vous comprenez et acceptez qu'en utilisant notre application, vous (ou votre enfant autorisé) nous transmettez la localisation de votre appareil (ou de votre enfant autorisé) et que certaines de ces informations de localisation, notamment votre (ou celui de votre enfant autorisé) nom d'utilisateur, peuvent être partagées via l'application.”

Niantic se réserve le droit de partager certaines informations “ne permettant pas l'identification” à des tiers à des fins de “recherche et d'analyse, de profilage démographique et à d'autres fins similaires”. Cela fait beaucoup de données sensibles et il est d'autant plus inquiétant de les confier à un responsable dont la réputation en matière de confidentialité est loin d'être sans tache. Les joueurs se sont déjà fait une frayeur lors de la première semaine lorsqu'ils ont découvert que le jeu accédait à bien plus de données de leur compte Google que nécessaire. Réponse de l'entreprise : “Nous avons récemment découvert que la création de comptes pour *Pokémon Go* sur iOS demandait par erreur une autorisation d'accès complet au compte Google de l'utilisateur. [...] Google a vérifié qu'aucune autre information n'avait été reçue ou été rendue

accessible à Pokémon Go ou Niantic". Ne manque que la mention d'un ingénieur un peu trop "entreprenant".

Sam Biddle