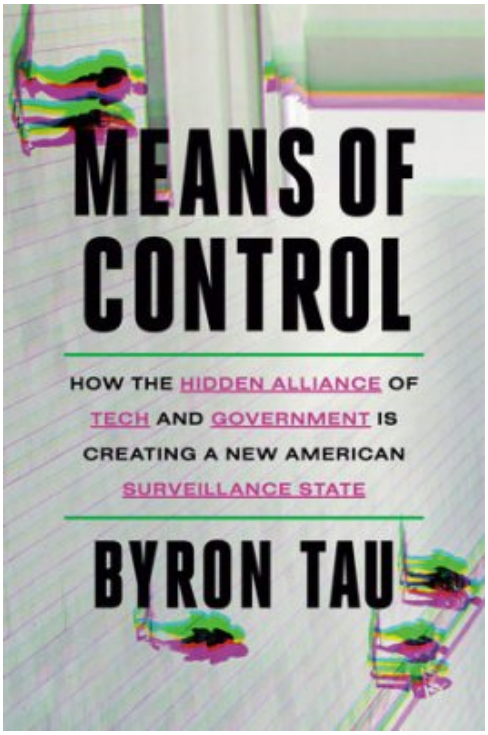
https://www.elcorreo.eu.org/Le-Pentagone-surveille-vos-rendez-vous

Le Pentagone surveille vos rendez-vous

- Cybersocieté -

Date de mise en ligne : dimanche 17 mars 2024

L'écosystème des technologies publicitaires est la plus grande entreprise de collecte d'informations jamais conçue par l'homme. Et ce n'est pas le gouvernement qui l'a créé. Comment les agences de renseignement américaines ont trouvé le moyen de tirer le meilleur parti de ce fabuleux outil.



Dans son numéro du 27 février, le mensuel américain **Wired** (en ligne), qui s'attache depuis son lancement en 1993 à mesurer l'impact de la technologie sur tous les aspects de la vie, publie en avant-première un nouvel essai de **Byron Tau**, journaliste américain au Wall Street Journal. Son titre inquiétant est : « ***Means of Control : How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State*** » (Moyens de contrôle : comment l'alliance cachée de la technologie et du gouvernement crée un nouvel État étasunien de surveillance) .

Dans la version abrégée de cet aperçu du livre de Tau - qui suit -, outre le fait de noter comment le Pentagone a appris à utiliser la publicité personnalisée pour trouver ses cibles, il raconte, à travers des faits et des personnages, comment les agences de renseignement américaines ont trouvé le moyen de tirer le meilleur parti de l'écosystème de la techno publicitaire. A coté de la cuisine géopolitique vraiment intéressante, il s'agit vraiment d'un thème clé pour nous. En effet, il s'agit d'un premier aperçu de l'impact que tout cela aura sur le territoire numérique de la politique argentine. Ce sont les mouvements des plaques tectoniques qui composent cette morphologie édaphique plus que singulière.

L'histoire racontée par Tau commence en 2019 et concerne la plus grande entreprise de collecte d'informations jamais conçue par l'homme. Cette année-là, **Mike Yeagley**, consultant pour le gouvernement et technologue, a commencé à donner des interviews à Washington, DC.Il a lancé un avertissement brutal à tous ceux qui, au sein de l'establishment de la sécurité nationale, étaient prêts à l'écouter : le gouvernement américain avait un problème avec ***Grindr***.

Grindr, une application populaire de rencontres et de rendez vous, s'appuie sur les capacités GPS des smartphones

modernes pour mettre en relation des partenaires potentiels dans la même ville, le même quartier ou même le même immeuble. L'application peut indiquer en temps réel la distance qui sépare un partenaire potentiel, au mètre près. En dix ans d'existence, *Grindr* a accumulé des millions d'utilisateurs et est devenu un élément central de la culture gay dans le monde entier.

Mais pour Yeagley, explique Tau, Grindr était autre chose : l'une des dizaines de milliers d'applications de téléphonie mobile conçues sans précaution et laissant échapper d'énormes quantités de données vers le monde opaque des annonceurs en ligne. Yeagley savait que ces données étaient facilement accessibles à toute personne disposant d'un peu de savoir-faire technique.Yeagley, 40 ans, dont la vie professionnelle s'est déroulée presque sans exception au service du gouvernement, s'est donc efforcé d'expliquer en quoi ces données constituaient un risque sérieux pour la sécurité nationale.

Yeagley démontrait comment les données de géolocalisation des utilisateurs de *Grindr* étaient accessibles par un point d'entrée caché mais omniprésent : les échanges publicitaires qui affichent les petites annonces numériques en haut de *Grindr*, et sur presque toutes les autres applications mobiles et sites web financés par la publicité. Cela a été rendu possible par la manière dont l'espace publicitaire est vendu en ligne, par le biais d'enchères quasi instantanées dans le cadre d'un processus appelé « enchères en temps réel ». Ces enchères comportaient un fort potentiel de surveillance.

Géorepérage

À partir des données de *Grindr*, Yeagley a commencé à tracer des **géorepérages**, c'est-à-dire à créer des frontières virtuelles dans des ensembles de données géographiques, autour de bâtiments appartenant à des agences gouvernementales chargées de la sécurité nationale. Cela a permis à Yeagley de voir quels téléphones se trouvaient dans certains bâtiments à certaines heures et où ils allaient ensuite. Il recherchait des téléphones appartenant à des utilisateurs de Grindr qui passaient la journée dans des bâtiments administratifs. Si l'appareil passait la plupart de ses journées de travail dans ces bureaux, il était très probable que son propriétaire travaillait pour l'une de ces agences.

Il a ensuite commencé à observer les mouvements de ces téléphones grâce aux données de *Grindr*. Lorsqu'ils n'étaient pas au bureau, où allaient-ils ? Un petit nombre d'entre eux avaient séjourné sur des aires d'autoroute dans la région de Washington en même temps et à proximité d'autres utilisateurs de *Grindr*, parfois pendant la journée de travail et parfois pendant les déplacements entre des édifices gouvernementaux. Pour les autres utilisateurs de *Grindr*, il pouvait déduire où ils vivaient, voir où ils voyageaient et même deviner avec qui ils sortaient.

Tau écrit avec une prose inquiète que Yeagley a découvert que toutes ces informations étaient disponibles à la vente pour peu d'argent. Et il ne s'agissait pas seulement de *Grindr*, mais de toute application ayant accès à la localisation précise d'un utilisateur : autres applications de rencontres, applications météorologiques, jeux, etc. Yeagley a choisi *Grindr* parce qu'elle générait un ensemble de données particulièrement riche et que sa base d'utilisateurs pouvait être exceptionnellement vulnérable. En 2016, une société chinoise avait obtenu une participation majoritaire dans *Grindr*, ce qui a fait craindre à Yeagley et à d'autres personnes à Washington qu'un ennemi géopolitique puisse utiliser les données à mauvais escient.

De l’archi espionnage

Mais l'objectif de Yeagley n'était pas seulement d'affirmer, dans les conférences qu'il a données, que les données publicitaires représentaient une menace pour la sécurité des États-Unis et la vie privée de ses citoyens. Il s'agissait de montrer que ces sources représentaient également une énorme opportunité entre de bonnes mains.

Selon M. Tau, lorsque l'on s'adresse à un groupe d'agences de renseignement, il n'y a pas de meilleur moyen d'attirer leur attention que de leur montrer un outil capable de révéler quand leurs agents s'arrêtent sur « les aires de repos sur la route ».

Mike Yeagley a vu à la fois les promesses et les pièges des données publicitaires parce qu'il a joué un rôle clé dans l'introduction des données publicitaires au sein du gouvernement. Le cycle de conférences qu'il a organisé en 2019 avait pour but de sensibiliser le personnel diversifié et souvent isolé des services de renseignement américains. Mais à ce moment-là, certains secteurs du monde du renseignement connaissaient déjà très bien son travail et l'utilisaient activement.

Yeagley avait passé des années à travailler comme « explorateur » technologique : il recherchait des capacités ou des ensembles de données qui existaient dans le secteur privé et aidait à les introduire au sein du gouvernement. Il avait contribué à la mise au point d'une technique que certains de ses utilisateurs appelaient en plaisantant « ADINT », un jeu de mots avec l'argot de la communauté du renseignement pour désigner différentes sources de renseignement, telles que SIGINT (renseignement d'origine électromagnétique), qui est devenu synonyme de l'essor du décryptage et des écoutes téléphoniques au 20e siècle. Il y a également eu l'OSINT (Renseignement d'origine sources ouvertes) de l'ère Internet, dont l'ADINT était une forme. Le plus souvent, cependant, l'ADINT était connu dans les cercles gouvernementaux sous le nom de données des technologies publicitaires.

Le fait que les agences de renseignement puissent simplement acheter certaines des données dont elles ont besoin directement auprès d'entités commerciales a été une révélation, notamment en raison des fuites d'**Edward Snowden**. Un autre consultant en technologie travaillant sur des projets pour le gouvernement des Etats-Unis l'a expliqué à Tau de la manière suivante : « *L'écosystème des technologies publicitaires est la plus grande entreprise de collecte d'informations jamais conçue par l'homme. Et ce n'est pas le gouvernement qui l'a créé* ».

Fonctionnement

Apple ou *Google* ont fourni à tous les propriétaires d'un *iPhone* ou d'un téléphone *Android* un identifiant publicitaire de manière « caché et anonyme ». Ce numéro est utilisé pour suivre nos déplacements dans le monde réel, notre comportement de navigation sur internet, les applications que nous installons sur notre téléphone et bien d'autres choses encore. Les plus grandes entreprises des États-Unis ont investi des milliards de dollars dans ce système.Face à un répertoire de données commerciales aussi riche et détaillé, les gouvernements du monde entier ont de plus en plus ouvert leur portefeuille pour acheter ces informations à tout le monde, plutôt que de les pirater ou de les obtenir par le biais d'ordonnances judiciaires secrètes, rapporte Tau.

Pour illustrer ce fonctionnement, Tau invite une femme imaginaire nommée Marcela. Elle possède un téléphone Google Pixel sur lequel est installée l'application type « La Météo/*Weather Channel* ». Alors qu'elle sort de chez elle pour aller courir, elle voit un ciel nuageux. Marcela ouvre alors l'appli pour vérifier si les prévisions annoncent de la pluie.

En cliquant sur l'icône bleue d'une chaîne météo, Marcela est entraînée dans une frénésie d'activités numériques visant à lui montrer une publicité personnalisée. Tout commence avec une entité appelée « **ad exchange** », qui est essentiellement un marché massif où des milliards d'appareils mobiles et d'ordinateurs informent un serveur

centralisé chaque fois qu'ils disposent d'un espace publicitaire ouvert.

En moins d'un clin d'œil, l'application *Weather Channel* partage une multitude de données avec cet ad exchange, notamment l'adresse IP du téléphone de Marcela, la version d'Android qu'elle utilise, son opérateur, ainsi qu'une série de données techniques sur la configuration du téléphone, jusqu'à la résolution de l'écran.Plus important encore, l'application partage les coordonnées GPS précises du téléphone de Marcela et le numéro d'identification pseudo-anonymisé que Google lui a attribué, appelé **AAID** (sur les appareils Apple, il s'agit de l'**IDFA**).

Pour le profane, un identifiant publicitaire est une série d'éléments de charabia, quelque chose comme « bdca712j-fb3c-33ad-2324-0794d394m912 ». Pour les annonceurs, c'est une mine d'or. Ils savent que « bdca712j-fb3c-33ad-2324-0794d394m912 » possède un appareil *Google Pixel* avec l'application *Nike Run Club*. Ils savent que « bdca712j-fb3c-33ad-2324-0794d394m912 » fréquente *Runnersworld.com*. Et ils savent que « bdca712j-fb3c-33ad-2324-0794d394m912 » désire ardemment une nouvelle paire de chaussures de course *Vaporfly* . Ils le savent parce que *Nike*, *Runnersworld.com* et *Google* sont connectés au même écosystème publicitaire, dont l'objectif est de comprendre ce qui intéresse les consommateurs. Avec les listes électorales, ils se feraient un vrai pic-nic.

Les annonceurs utilisent ces informations pour concevoir et diffuser leurs publicités. En s’appuyant sur les énormes quantités de données qu'ils peuvent extraire, ils peuvent créer une « audience », essentiellement une énorme liste d'identifiants publicitaires de clients dont on sait ou dont on soupçonne qu'ils se trouvent sur le marché qui les intéresse. Ensuite, dans le cadre d'une vente aux enchères instantanée, automatisée et en temps réel, les annonceurs indiquent à un marché publicitaire numérique le montant qu'ils sont prêts à payer pour atteindre ces consommateurs chaque fois qu'ils chargent une application ou une page web. Tout un modèle commercial a été construit sur cette base : l'extraction de données à partir de réseaux d'enchères en temps réel, leur conditionnement et leur revente pour aider les entreprises à comprendre le comportement des consommateurs.

Il existe des limites et des garanties pour toutes ces données. Techniquement, un utilisateur peut réinitialiser le numéro d'identification publicitaire qui lui a été attribué, mais peu de gens le font ou savent même qu'ils en ont un. Par ailleurs, les utilisateurs ont un certain contrôle sur ce qu'ils partagent par le biais des paramètres de leur application. Si les consommateurs n'autorisent pas l'application qu'ils utilisent à accéder au GPS, Ad Exchange ne peut pas obtenir la position GPS du téléphone, par exemple (ou du moins il n'est pas censé le faire).Toutes les applications ne respectent pas les règles, et parfois elles ne sont pas correctement contrôlées une fois qu'elles sont dans les boutiques d'applications).

La donnée la plus précieuse

La géolocalisation est la donnée commerciale la plus précieuse qui émerge de ces appareils. Comprendre les mouvements des téléphones est aujourd'hui une industrie de plusieurs milliards de dollars, selon Tau. Elle peut être utilisée pour diffuser des publicités ciblées en fonction de l'emplacement, par exemple pour une chaîne de restaurants qui souhaite cibler les personnes se trouvant à proximité. Elle peut être utilisée pour mesurer le comportement des consommateurs et l'efficacité de la publicité - combien de personnes ont vu une publicité et se sont ensuite rendues dans un magasin ? Les analyses peuvent également être utilisées pour la planification et les décisions d'investissement : quel est le meilleur emplacement pour un nouveau point de vente ? Le trafic piétonnier sera-t-il suffisant pour assurer la pérennité d'un tel commerce ? Le nombre de personnes visitant un détaillant particulier est-il en hausse ou en baisse ce mois-ci ?

Mais ce type de données a une autre utilité. Parce que ce que nous faisons dans le monde avec nos appareils ne

peut pas être « vraiment anonyme », explique Tau. Le fait que les publicitaires connaissent Marcela sous le nom de « bdca712j-fb3c-33ad-2324-0794d394m912 » lorsqu'ils l'observent se déplacer dans le monde en ligne et hors ligne n'offre pratiquement aucune protection de sa vie privée. Dans l'ensemble, ses habitudes et ses routines lui sont propres. Nos déplacements dans le monde réel sont très spécifiques et personnels. L'endroit où un téléphone passe la plupart de ses nuits est un bon indicateur de l'endroit où vit son propriétaire. Les publicitaires le savent. Les gouvernements le savent aussi.

Vous êtes localisé

« Si vous avez déjà autorisé une application météo à savoir où vous vous trouvez, il est très probable qu'un enregistrement de vos mouvements précis a été stocké dans une base de données à laquelle des dizaines de milliers d'inconnus ont accès », explique M. Tau. Cela inclut les agences de renseignement. Selon M. Tau, le Ministère de la Sécurité Intérieure (DHS) s'est montré particulièrement enthousiaste à l'idée d'acheter ce type de données ad-tech. Trois de ses composantes (*US Customs and Border Protection*, *US Immigration and Customs Enforcement* et *US Secret Service*) ont acheté plus de 200 licences à des fournisseurs commerciaux de technologies publicitaires depuis 2019.

Ils ont utilisé ces données pour trouver des tunnels frontaliers et suivre l'accès des immigrants non autorisés, ainsi que pour résoudre des crimes nationaux. En 2023, un auditeur général du gouvernement a réprimandé le DHS pour son utilisation de la technologie publicitaire, affirmant que le département n'avait pas mis en place des garanties adéquates en matière de protection de la vie privée et recommandant que les données cessent d'être utilisées jusqu'à ce que des politiques soient élaborées. Le DHS a indiqué à l'auditeur général qu'il continuerait à utiliser les données. D'autres agences gouvernementales de renseignement ont également accès à ces données et les vendent à des organismes de sécurité nationale et de sécurité publique dans le monde entier.

Pour souligner qu'il ne s'agit pas d'une préoccupation abstraite, Tau rappelle qu'en 2021, un petit blog catholique conservateur appelé ***The Pillar*** a rapporté que **Jeffrey Burrill**, le secrétaire général de la Conférence des Evêques Catholiques des États-Unis, était un utilisateur régulier de *Grindr*. La publication indique que M. Burrill « a visité des bars gays et des résidences privées tout en utilisant une application de rencontre géolocalisée ». Elle décrit sa source comme étant « des enregistrements de données de signaux d'applications disponibles dans le commerce et obtenus par *The Pillar* ».

Selon Byron Tau, « nous avons tous la vague impression que nos opérateurs de téléphonie mobile possèdent ces données sur nous. Mais les autorités ont généralement besoin d'une décision de justice pour les obtenir. Et il faut des preuves d'un délit pour obtenir un tel mandat. Il s'agit là d'un autre type de cauchemar en matière de protection de la vie privée. Reste que la politique argentine (ou une autre] a tendance à s'endormir sur le territoire numérique sans remarquer ce que la Droite dure fait à travers ces cauchemars de la vie privée. Apparemment, elle, elle est bien réveillée.

Cristina Robles* pour **¿Y ahora qué ?**

¿Y ahora qué ?. Buenos Aires, le 16 mars 2024.

Traduit de l'espagnol pour *El Correo de la Diáspora* par : Estelle et Carlos Debiasi.

El Correo de la Diaspora. Paris, le 17 mars 2024.

Post-scriptum :
Pour *Supprimer* ou *Réinitialiser* votre identifiant publicitaire (ID) sur IOS ou ANDROID

ANDROID :*Paramètres* > *Google* > *Annonces* Et cliquer sur l'option **« Réinitialiser »** ou **« Supprimer »** l'identifiant publicitaire.

Pour **IOS** : Voir **ce lien**