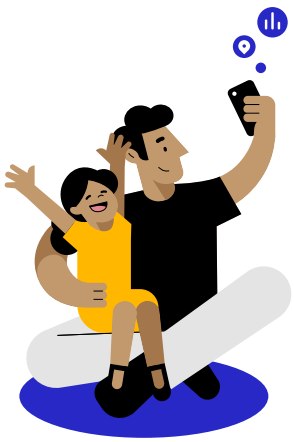


Une journée avec vos données

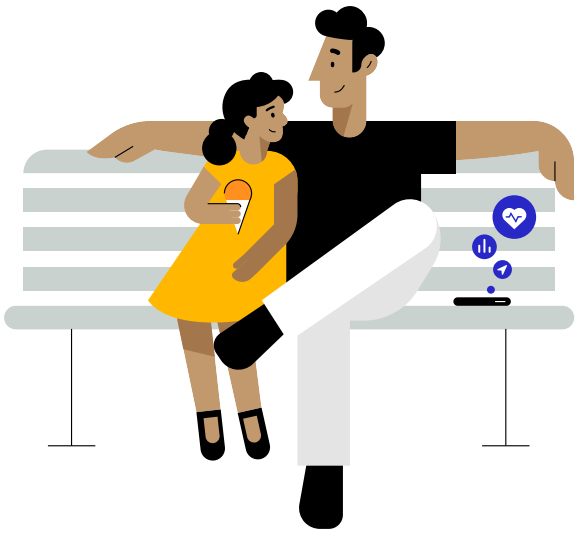
Une journée au parc entre père et fille

Avril 2021

« Je crois que les gens sont intelligents et que certaines personnes sont prêtes à partager plus de données que d’autres. Posez-leur la question. Posez-leur la question à chaque fois. Demandez-leur de vous dire d’arrêter de poser la question si ça devient lassant. Dites-leur précisément ce que vous comptez faire de leurs données. »

Steve Jobs

Conférence All Things Digital, 2010



Depuis une décennie, un secteur d'activité opaque et tentaculaire amasse des volumes croissants de données personnelles[1,2]. Un écosystème complexe de sites web, apps, réseaux sociaux, courtiers en données (« data brokers ») et sociétés d'adtech suivent les internautes en ligne et hors ligne, récoltant au passage leurs données personnelles. Rassemblées, partagées, agrégées et utilisées dans des enchères en temps réel, ces données alimentent un secteur d'activité dégageant un chiffre d'affaires annuel de 227 milliards de dollars[1]. Cela se passe chaque jour, alors que les personnes concernées vaquent à leurs occupations quotidiennes. Et cela se passe sans leur autorisation, sans même qu'elles en aient conscience[3,4]. Voyons ce que ce secteur peut apprendre sur un père et sa fille qui profitent d'une agréable journée au parc.

Le saviez-vous ?

Des traqueurs sont intégrés aux apps que vous utilisez chaque jour : en moyenne, une app intègre six traqueurs[3]. La majorité des apps Android et iOS les plus appréciées en contiennent[5,6,7].

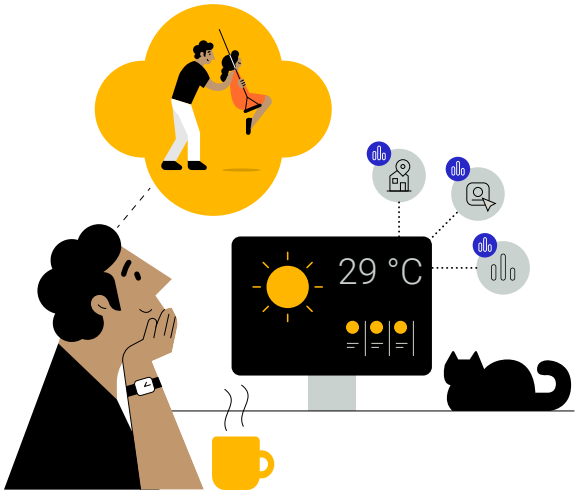
Les traqueurs sont souvent intégrés dans le code tiers qui sert à créer les apps. Grâce à eux, les sociétés de développement permettent aussi à des entreprises tierces de collecter et de relier les données que vous leur avez communiquées par le biais de différentes apps avec d'autres données vous concernant ayant été recueillies par ailleurs.

Les courtiers en données collectent et commercialisent, diffusent sous licence ou divulguent d'autres façons à des tiers les informations personnelles d'individus avec lesquels ils n'ont pas de relation directe[3].

Des centaines de courtiers en données recueillent des données en ligne et hors ligne[8]. Un même courtier collecte des données sur 700 millions de consommateurs et consommatrices à l'échelle mondiale, créant des profils intégrant jusqu'à 5 000 caractéristiques[9].

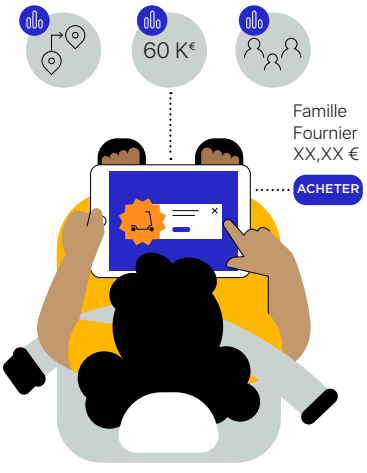
Une étude a montré que dans près de 20 % des apps destinées aux enfants, les sociétés de développement collectaient et partageaient des données permettant d'identifier les personnes sans qu'ait été accordé un consentement parental vérifiable[10].

Chaque heure de chaque journée, des milliards d'annonces publicitaires numériques sont présentées aux internautes[11,12,13]. Durant les quelques millisecondes nécessaires à une annonce pour se charger, a lieu une enchère en temps réel, au cours de laquelle des annonceurs enchérissent sur l'espace publicitaire en question, en s'appuyant souvent sur des données personnelles recueillies sur les individus[14,15].



Pierre prévoit de passer une journée au parc avec sa fille

Pierre et sa fille Emma, âgée de sept ans, passent la journée ensemble. Le matin, Pierre allume son ordinateur pour regarder la météo et lire la presse, puis il vérifie sur l'app de plans de son smartphone l'état de la circulation afin de se rendre au parc situé près de l'école de sa fille. En chemin, quatre apps installées sur son téléphone vont collecter et suivre régulièrement ses données de géolocalisation en arrière-plan[16,17,18]. Une fois les données extraites de l'appareil, les sociétés de développement les vendront à toute une série de courtiers en données tiers assez obscurs dont Pierre n'a jamais entendu parler[16,17]. Bien que les données de géolocalisation soient censées être anonymes, le suivi d'utilisation permet aux courtiers en données d'associer l'historique de géolocalisation de Pierre issu de ces apps à des informations collectées à partir de son utilisation d'autres apps[16,19]. Ce qui signifie que les informations suivies sur différentes apps et auprès de diverses sources peuvent être achetées par n'importe quelle entreprise ou organisation et qu'elles peuvent servir à créer un profil complet sur Pierre, incluant ses déplacements précis au quotidien[3,16].



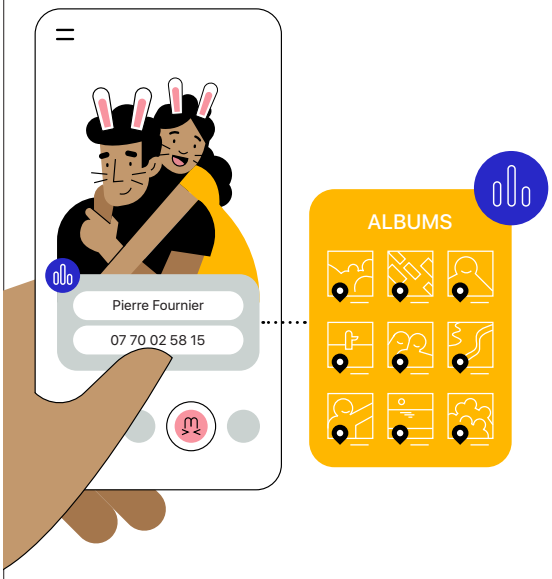
Emma joue à un jeu sur le chemin du parc

Sur le chemin du parc, Pierre laisse sa fille jouer à un jeu sur sa tablette. En ouvrant l'app, elle voit une pub pour une trottinette… Et c'est loin d'être un hasard. À la seconde où l'app s'est chargée, une enchère a eu lieu pour occuper l'espace publicitaire[14]. Grâce à des intermédiaires, les agences de publicité travaillant pour le compte du fabricant de trottinettes ont su que cet espace était disponible[15]. À l'aide des données personnelles collectées à propos de Pierre et d'Emma, elles ont placé une enchère sur cet espace[15]. Les partenaires publicitaires du fabricant de trottinettes continuent à recueillir des informations sur le comportement de Pierre et d'Emma une fois que le père et sa fille ont vu l'annonce, afin de déterminer si l'un et l'autre ont cliqué dessus ou acheté la trottinette en question[3]. Et ces partenaires continueront à présenter la publicité de cette trottinette par tous les moyens possibles à Pierre et Emma, en les suivant sur différentes apps et différents sites web sur tous les appareils de Pierre[3,20,21].

Certaines apps demandent l'accès à plus de données que ne le nécessite le service qu'elles rendent : par exemple, une app de clavier demandant à accéder à la localisation précise de la personne[5].

Les informations échangées peuvent être communiquées à des régies publicitaires, des éditeurs, des fournisseurs d'attributions et de mesures, des courtiers en données, d'autres entreprises privées et même des organismes publics[3,15,40,41,42]. En utilisant des données personnelles à des fins autres que celles indiquées à l'utilisateur ou utilisatrice au moment de la collecte des données en question[22,23,24,25], les réseaux sociaux et les sociétés d'adtech s'exposent à des amendes de plusieurs millions de dollars et ont d'ailleurs déjà été condamnés à payer de telles sommes.

Les courtiers en données utilisent les données qu'ils recueillent pour attribuer des caractéristiques (« attributs ») à des utilisateurs et utilisatrices, puis répartir ces personnes dans des segments de marché hyper-détaillés, tels que « personnes cherchant à perdre du poids mais aimant les pâtisseries »[26]. Néanmoins, ces profils sont souvent erronés : une étude a montré que plus de 40 % de ces attributs étaient inexacts[27,28].

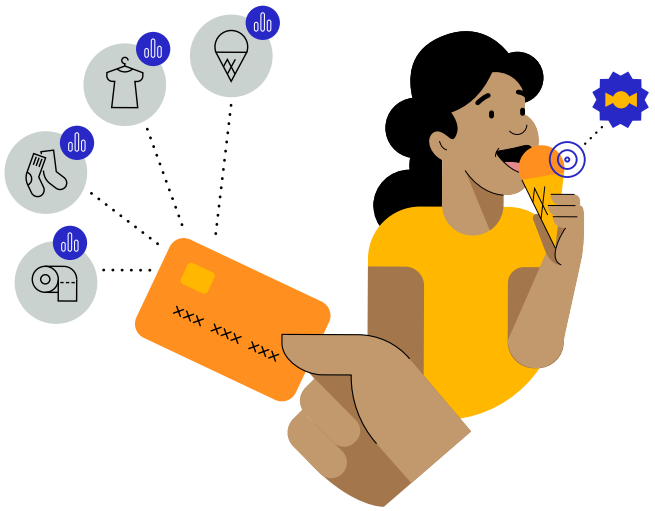


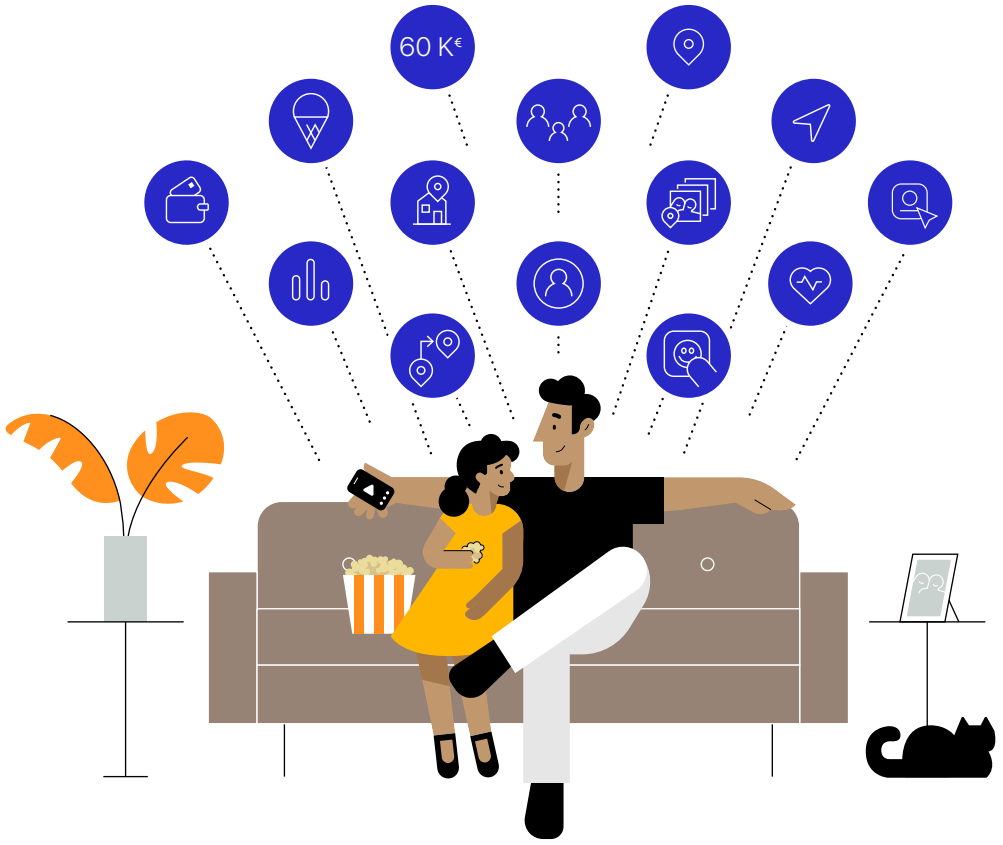
Pierre et Emma font un selfie au parc

Plus tard, au parc, Pierre et Emma font un selfie. Le père et sa fille s'amusent avec une app de filtres et se mettent des oreilles de lapin sur la photo. Cette app de filtres accède alors à toutes les photos que comporte l'appareil ainsi qu'aux métadonnées associées, plutôt que de se limiter au seul selfie réalisé dans le parc[29,30]. Pierre publie ensuite la photo sur une app de réseau social. L'app relie l'activité en ligne actuelle de Pierre à une véritable mine de données, comme ses données démographiques et ses habitudes d'achats, collectées par d'autres apps à l'aide d'une adresse e-mail, d'un numéro de téléphone ou d'un identifiant publicitaire[3].

Un détour chez le glacier avant de rentrer

En rentrant à la maison, Pierre et Emma s'offrent une glace. Pierre paie les glaces avec sa carte de crédit, et d'autres informations viennent enrichir le profil déjà très complet de ses préférences : l'adresse du glacier et le montant dépensé[31,32,33]. L'une des apps qui suivent Pierre est capable de détecter que Pierre et Emma sont également passés par un magasin de jouets[3]. Les informations sur les endroits où la famille a fait des achats au cours de la journée sont transmises à des courtiers en données, qui les associent à ce qu'ils savent déjà de Pierre (il est père d'une petite fille) pour diffuser massivement sur ses appareils des publicités ciblées pour des sucreries et pour le magasin de jouets dans lequel il s'est rendu avec sa fille[17].





Au bout du compte (et de la journée), un certain nombre d'entreprises du monde entier avec lesquelles Pierre n'a jamais eu la moindre interaction ont pu actualiser leurs profils grâce à des informations sur lui et sa fille. Ces entreprises connaissent l'adresse de la famille, le parc où elle s'est rendue, les sites d'informations qu'elle a consultés, les produits qu'elle a recherchés, les publicités qu'elle a regardées, la façon dont elle fait des achats et les magasins dans lesquels elle s'est rendue[3,34]. Ces données ont été collectées et suivies sur diverses apps que Pierre et sa fille ont utilisées tout au long de la journée, et auprès d'autres sources. Pierre n'avait pas la moindre idée du volume de données recueillies tout au long de la journée, il n'avait pas en permanence le contrôle de ces données, et il n'a pas expressément autorisé leur collecte[3,4]. Alors que le père et sa fille recherchent un film pour enfants à regarder sur une app de leur téléviseur connecté pour bien finir la journée, le cycle de suivi, d'échange de données, de mise aux enchères et de reciblage se poursuit sans relâche[35,36].

Principes d'Apple en matière de confidentialité

Apple considère que le respect de la vie privée est un droit humain fondamental. En matière de confidentialité, quatre principes essentiels guident la conception de nos produits et services :

Collecte minimale de données

Nous ne recueillons que le strict volume de données nécessaire au fonctionnement d'un service donné.

Traitement sur l'appareil

Chaque fois que c'est possible, les données sont traitées sur l'appareil au lieu d'être envoyées aux serveurs Apple, afin de protéger la vie privée des utilisateurs et utilisatrices et de réduire au maximum la collecte de données.

Pour en savoir plus sur les fonctionnalités de confidentialité introduites par Apple et sur les efforts que déploie la société pour protéger la vie privée des utilisateurs et utilisatrices, consultez apple.com/fr/privacy.

Transparence et contrôle pour les utilisateurs et utilisatrices

Nous veillons à ce que les personnes qui utilisent nos produits sachent quelles données sont partagées et quel usage en est fait, et à ce qu'elles puissent exercer leur contrôle en la matière.

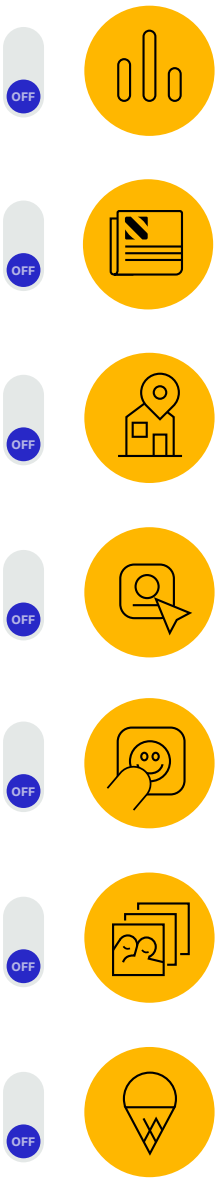
Pour en savoir plus sur la façon dont Safari protège votre vie privée, lisez le Livre blanc sur Safari.

Sécurité

Le matériel et les logiciels fonctionnent en parfaite synergie pour préserver la sécurité des données.

Pour en savoir plus sur la façon dont Apple protège vos données de localisation, lisez le Livre blanc sur le service de localisation.

À travers ces quatre principes, l'objectif d'Apple a toujours été de permettre aux utilisateurs et utilisatrices de partager leurs données à leur convenance, d'une façon sûre, claire et contrôlable. C'est la raison pour laquelle, au cours des deux dernières décennies, Apple n'a cessé d'innover pour préserver la confidentialité dans tous ses produits et services. Par exemple, nous employons l'intelligence embarquée et d'autres fonctionnalités pour limiter au maximum les données que nous recueillons dans nos apps, navigateurs et services en ligne. Et aucune de nos apps, ni aucun de nos services ne crée de profil complet de l'utilisateur ou utilisatrice.



Les fonctionnalités de confidentialité d'Apple donnent à Pierre plus de transparence et de contrôle sur ses données

Le récit de la journée de Pierre et Emma illustre bien les problèmes de confidentialité auxquels est confronté Apple et les solutions que la société met en place pour y faire face.

Pierre prévoit de passer une journée au parc avec sa fille

Si Pierre avait utilisé le navigateur Safari pour consulter la météo sur son ordinateur, la prévention intelligente du suivi aurait évité par défaut le suivi de son activité.

Si Pierre avait utilisé Apple News pour lire les nouvelles du jour, Apple lui aurait proposé des contenus en fonction de ses centres d'intérêt, sans savoir qui il est ni découvrir ce qu'il avait lu.

Si Pierre avait utilisé Apple Plans pour vérifier l'état de la circulation, ses données de localisation auraient été associées à un identifiant aléatoire régulièrement réinitialisé et non associé à Pierre. Ainsi, personne – hormis Pierre lui-même – n'aurait pu savoir où il se trouvait.

Sur un iPhone, il aurait été régulièrement rappelé à Pierre que telle ou telle app accédait en arrière-plan à sa localisation. Avant de partager sa position avec une app, Pierre aurait pu choisir de ne communiquer que sa localisation approximative ou de ne partager sa position exacte qu'une seule fois.

Emma joue à un jeu sur le chemin du parc

Sur un iPad, la fonctionnalité bientôt disponible de transparence du suivi par les apps donnerait à Pierre le choix de permettre ou non au jeu de suivre l'activité d'Emma sur des apps et des sites web détenus par d'autres entreprises.

Les régies publicitaires utilisant l'API SKAdNetwork d'Apple seraient capables de mesurer l'efficacité générale de leurs annonces publicitaires sans accéder à des informations permettant de remonter à l'appareil de Pierre.

Pierre et Emma font un selfie au parc

Sur un iPhone, Pierre aurait eu le choix de permettre à l'app de filtres d'accéder uniquement au selfie, et non à l'ensemble de sa photothèque.

Un détour chez le glacier avant de rentrer

Si Pierre avait payé les glaces à l'aide de l'Apple Card, sa banque n'aurait pas utilisé les données de sa transaction à des fins de marketing. S'il avait utilisé Apple Pay, Apple aurait exploité l'intelligence embarquée pour lui permettre de consulter l'historique de ses transactions sur son iPhone. Et ce, sans qu'Apple n'obtienne d'informations sur l'endroit où il avait fait des achats, sur ce qu'il avait acheté ou sur la somme qu'il avait dépensée.

Au final, les produits et fonctionnalités de confidentialité Apple peuvent donner à Pierre plus de transparence et de contrôle tout au long de la journée sur la quantité de données personnelles partagées et sur l'usage qui en est fait.

Transparence du suivi par les apps et nouvelle section Informations sur la confidentialité de l'App Store

Apple va plus loin dans la protection de la vie privée des utilisateurs et utilisatrices au sein de l'écosystème d'apps. Alors qu'un ensemble complexe et croissant d'entités accèdent aux données personnelles, les suivent et les monétisent, Apple introduit deux nouvelles fonctionnalités visant à offrir plus de transparence, de visibilité et d'options afin que chaque personne puisse choisir en toute connaissance de cause et exercer un contrôle renforcé sur la confidentialité de ses propres données.

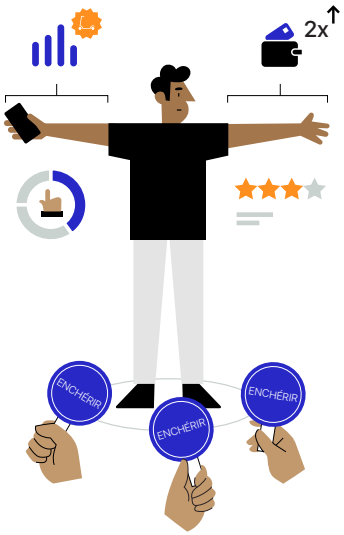
D'ici peu, grâce à notre prochaine version bêta, la transparence du suivi par les apps exigera que ces dernières obtiennent l'autorisation de l'utilisateur ou utilisatrice avant d'en suivre les données sur des apps ou des sites web détenus par d'autres entreprises. Dans Réglages, les utilisateurs et utilisatrices pourront voir quelles apps ont demandé l'autorisation de suivre leurs données, ce qui leur permettra de faire des changements à leur convenance. Cette fonctionnalité sera largement déployée au début du printemps avec les prochaines versions d'iOS 14, d'iPadOS 14 et de tvOS 14, et a déjà recueilli le soutien de personnes défendant activement le droit à la vie privée dans le monde entier. En concevant cette fonctionnalité, Apple cherchait à offrir plus de transparence et de contrôle tout en continuant à permettre la publicité comme moyen adapté et viable de soutenir les apps et les contenus web. L'introduction de fonctionnalités précédentes, comme la prévention intelligente du suivi dans Safari, a montré que la protection de la vie privée pouvait être renforcée sans entraver l'efficacité de la publicité. La transparence du suivi par les apps permet de faire des choix en toute connaissance de cause sur les apps que l'on utilise et sur les autorisations que l'on accorde ou non à ces apps. Grâce à cette fonctionnalité, les utilisateurs et utilisatrices peuvent désormais décider d'autoriser ou non les apps à les suivre. Les sociétés de développement des apps qui leur semblent fiables ou pour lesquelles une autorisation de suivi a été accordée peuvent donc continuer à effectuer ce suivi.

Outre l'autorisation obligatoire de l'utilisateur ou utilisatrice pour le traçage, Apple a également apporté des changements récents aux pages de produits de l'App Store afin d'améliorer la transparence. Ainsi, la nouvelle section Confidentialité des apps de l'App Store permet de mieux comprendre les pratiques de chaque app en matière de respect de la confidentialité. Chaque page de produit dédiée à une app doit fournir un résumé clair des pratiques de la société de développement en matière de respect de la confidentialité. Les pages de détails contiennent des informations sur les types de données que collecte l'app, comme les photos, la localisation ou encore les coordonnées personnelles. Ces pages fournissent également des détails complémentaires sur l'usage qui est fait de chaque type d'information par la société de développement, en précisant si ces informations sont utilisées pour le suivi et si elles sont associées à l'utilisateur ou utilisatrice. Toutes les sociétés développant des apps, y compris Apple, doivent rendre compte de leurs pratiques en matière de respect de la vie privée.

L'ajout, sur les pages de produits de l'App Store, de réglages de suivi par les apps et d'informations sur la transparence et le respect de la vie privée permet aux utilisateurs et utilisatrices de découvrir plus facilement l'usage qui est fait de leurs données personnelles et leur offre plus de contrôle sur ces données en jetant un éclairage inédit sur des pratiques auparavant opaques et dissimulées.

Apple continuera à mettre au point des technologies innovantes en matière de respect de la confidentialité et à chercher de nouveaux moyens de sécuriser vos données personnelles.

Une journée avec une annonce publicitaire



Enchères publicitaires

Si Emma a vu une publicité pour une trottinette sur l'écran de Pierre, ce n'était pas par hasard. Les annonceurs enchérissent pour placer leur publicité sur l'appareil[37]. Voici une explication simple de ce qui s'est passé en une fraction de seconde pour que cette annonce publicitaire en particulier s'affiche à l'écran :

1.
L'entreprise ayant développé l'app qu'utilise Emma engage une société d'adtech qui met aux enchères en temps réel son espace publicitaire[14].

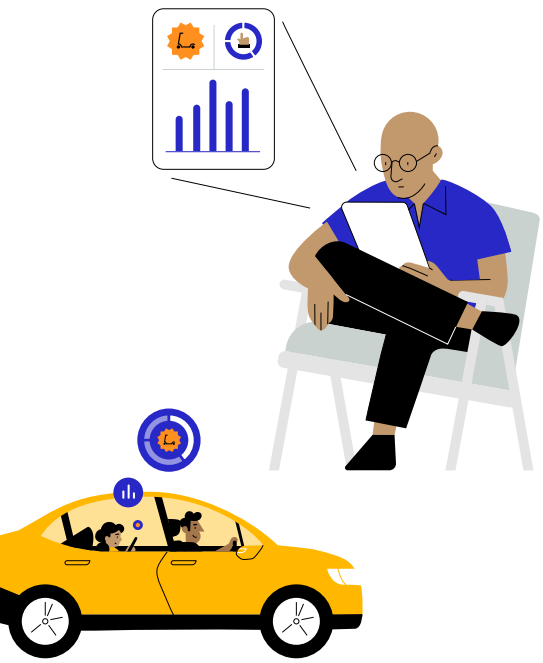
2.
Dès qu'Emma ouvre l'app, la régie publicitaire collecte des données, issues à la fois de son utilisation de l'appareil de Pierre (par exemple, quelle app elle est train d'utiliser, où elle se trouve et l'identifiant publicitaire de Pierre) et d'entités tierces, en s'appuyant sur l'identifiant publicitaire de Pierre ou sur d'autres informations qui permettent le suivi[3].

3.
La régie publicitaire partage certaines de ces informations, en particulier l'identifiant publicitaire, avec de potentiels annonceurs. Avant d'enchérir, les annonceurs essaient généralement d'en savoir autant que possible sur la personne, à partir de ses propres données ainsi que de données personnelles recueillies et agrégées grâce à des techniques de suivi et de profilage[3,15].

4.
Plus les caractéristiques de Pierre et d'Emma – issues de leurs données – correspondent au public visé par les annonceurs, plus les enchères montent pour l'obtention de cet espace publicitaire[15,38].

5
L'annonce ayant remporté l'enchère – en l'occurrence celle pour une trottinette – s'affiche sur l'écran de l'appareil qu'Emma est en train d'utiliser[14].

Comme le processus d'enchères publicitaires se déroule en une fraction de seconde, les deux parties prenant part à la vente recueillent, échangent et utilisent des données personnelles pour enchérir sur l'espace disponible et présenter des annonces publicitaires[14,15].



Attribution

Une fois l'annonce présentée à Emma, les sociétés chargées de la publicité de l'entreprise de trottinettes souhaitent en mesurer l'effet sur son comportement. On appelle ce processus « attribution ».

Pour ce faire, l'annonceur essaie de suivre le comportement d'Emma sur l'appareil qu'elle utilise, de recueillir des informations sur son activité sur le Web et dans les apps, et même sur les endroits qu'elle fréquente hors ligne.

- **Si l'annonce publicitaire concerne un produit,** l'annonceur pourra essayer de vérifier si la personne s'est rendue par la suite sur son site web ou dans son magasin physique pour acheter le produit en question[3].
- **Si l'annonce publicitaire concerne une app, l'annonceur pourra essayer de vérifier si la personne l'a installée ou non.** On appelle ce processus « attribution mobile »[39].

Les annonceurs utilisent également l'attribution pour « optimiser » leurs campagnes publicitaires en ciblant les groupes auprès desquels celles-ci seront le plus efficaces[3].

Mais ces façons de procéder peuvent être évitées. Les annonceurs peuvent mesurer l'impact de leurs campagnes publicitaires auprès de certains groupes sans pour autant suivre les utilisateurs et utilisatrices. Apple travaille au développement d'outils capables de s'en charger tout en préservant la confidentialité :

SKAdNetwork permet aux annonceurs de savoir combien de fois une app a été installée après que la publicité correspondante a été vue, afin de mesurer l'impact de la campagne publicitaire. Mais ces informations sont conçues pour ne pas communiquer la moindre donnée sur l'utilisateur ou utilisatrice ou sur l'appareil, afin que les annonceurs ne puissent pas effectuer de suivi.

La fonctionnalité **Private Click Measurement**, destinée aux apps sous iOS et iPadOS 14.5, permet aux annonceurs de mesurer l'impact des annonces publicitaires qui conduisent des internautes vers un site web, tout en réduisant au maximum la collecte de données grâce au traitement sur l'appareil. Lorsqu'une personne clique sur une annonce pour un produit au sein d'une app, le navigateur web, en utilisant la fonctionnalité Private Click Measurement, est capable d'informer l'annonceur qu'une personne a cliqué sur son annonce et que ce clic a conduit à un certain résultat sur son site web, comme une visite ou un achat, sans lui révéler l'identité de cette personne.

Questions et réponses

Pourrai-je encore utiliser toutes les fonctionnalités de l'app si je sélectionne « Demander à l'app de ne pas suivre mes activités » ?

Oui. Les sociétés développant des apps ne peuvent pas vous obliger à autoriser le suivi pour vous permettre d'utiliser toutes les fonctionnalités de leurs apps.

Que sont les identifiants et comment sont-ils utilisés ?

Les identifiants tels que l'IDFA (identifiant publicitaire) et l'adresse e-mail contribuent à identifier un appareil précis sur un réseau. Ils permettent également aux annonceurs de créer un profil détaillé de votre activité sur plusieurs apps ou sites web lorsqu'ils voient votre identifiant d'appareil et l'associent à l'usage que vous en faites.

Qu'est-ce que l'IDFA (identifiant publicitaire) ?

L'IDFA (identifiant publicitaire) est un identifiant contrôlable par l'utilisateur ou utilisatrice, attribué par iOS à chaque appareil. Parce que cet identifiant est basé sur le logiciel et non associé au matériel lui-même, l'IDFA peut être bloqué pour une app en particulier grâce à l'option de transparence du suivi par les apps, ce qui permet de contrôler le suivi basé sur l'IDFA.

Ai-je la garantie, de la part d'Apple, qu'une app ne me suivra pas si je sélectionne « Demander à l'app de ne pas suivre mes activités » ?

Si vous sélectionnez « Demander à l'app de ne pas suivre mes activités », la société ayant développé l'app ne pourra pas accéder à l'IDFA (identifiant publicitaire), qui est souvent utilisé pour le suivi. Elle devra également respecter votre choix au-delà de l'identifiant publicitaire. Ce respect est exigé par les règles qu'a acceptées la société de développement en proposant son app à la diffusion sur l'App Store. Si nous apprenons qu'une telle société suit les personnes qui demandent à ne pas l'être, nous exigerons qu'elle actualise ses pratiques afin de respecter votre choix. À défaut, son app risque d'être exclue de l'App Store.

Si j'utilise un de mes comptes de réseaux sociaux pour me connecter à une app, l'entreprise propriétaire du réseau social en question peut-elle suivre ce que je fais sur cette app ?

Cela dépend de l'autorisation de suivi que vous avez accordée ou non. Si vous sélectionnez « Demander à l'app de ne pas suivre mes activités », l'app ne doit pas vous suivre sur les apps ou les sites web d'autres sociétés à des fins publicitaires, ni partager les informations vous concernant avec un courtier en données. Cela signifie qu'elle ne doit pas communiquer vos données à l'entreprise propriétaire du réseau social si ces données doivent être utilisées à des fins publicitaires.

Que fait Apple pour s'assurer de l'exactitude des informations sur le respect de la vie privée figurant sur les pages de produits de l'App Store ?

Comme pour les tranches d'âge sur l'App Store, les sociétés de développement doivent rendre compte des pratiques qu'elles mettent en œuvre pour le respect de la confidentialité. Si nous apprenons qu'une société de développement a fourni des informations inexactes, nous la contactons et veillons à ce qu'elle respecte ses engagements.

Qu'est-ce qu'un courtier en données, ou « data broker » ?

D'une manière générale, un courtier en données est une entreprise dont l'activité consiste à collecter et vendre, diffuser sous licence ou divulguer par d'autres moyens à des tiers les données personnelles d'utilisateurs et utilisatrices spécifiques avec qui l'entreprise n'a pas de relation directe. Dans certains pays, l'activité des courtiers en données est encadrée par la loi.

Sources

1. Gröne, Florian, Pierre Péladeau, et al., « Tomorrow's data heroes », *Strategy+Business*, 19 février 2019.

2. Reinsel, David, John Gantz, et al., « The Digitization of the World: From Edge to Core », *IDC*, novembre 2018.

3. Competition & Markets Authority, « Online platforms and digital advertising », 1 juillet 2020.

4. Hitlin, Paul, and Lee Rainie, « Facebook Algorithms and Personal Data », *Pew Research Center*, 16 janvier 2019.

5. AppCensus, « 1,000 Mobile Apps in Australia: A Report for the ACCC », 24 septembre 2020.

6. Binns, Reuben, Ulrik Lyngs, et al., « Third Party Tracking in the Mobile Ecosystem », *Proceedings of the 10th ACM Conference on Web Science*, 2018, pp. 23-31.

7. MightySignal, « Most Used SDKs in Top 200 Free iOS Apps », mightysignal.com/top-ios-sdks.

8. State of California Department of Justice, « Data Broker Registry », oag.ca.gov/data-brokers.

9. Acxiom Corporation, 2018 Form 10-K, déposé le 25 mai 2018, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.

10. Reyes, Irwin, Primal Wijesekera, et al., « 'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale », *Proceedings on Privacy Enhancing Technologies*, Vol. 2018, No. 3, 2018, pp. 63-83.

11. Edwards, Jim, « Here's The Staggering Number of Ads Facebook Serves On Its Exchange Every Day », *Business Insider*, 9 novembre 2012.

12. Kim, Larry, « How Many Ads Does Google Serve In A Day? », *Business 2 Community*, 2 novembre 2012.

13. Deighton, John, and Leora Kornfeld, « The Socioeconomic Impact of Internet Tracking », *Interactive Advertising Bureau*, février 2020.

14. Hwang, Tim, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*, FSG Originals, 13 octobre 2020.

15. Australian Competition and Consumer Commission, « Digital advertising services inquiry - Interim report », décembre 2020.

16. Thompson, Stuart A., and Charlie Warzel, « Twelve Million Phones, One Dataset, Zero Privacy », *The New York Times*, 19 décembre 2019.

17. Nanos, Janelle, « Every step you take: How companies use geolocation data to target you – and everyone around – in ways you're not even aware of », *The Boston Globe*, 21 juillet 2018.

18. Vitaldevara, Krish, « Safer and More Transparent Access to User Location », *Android Developers Blog*, 19 février 2020.

19. Schechner, Sam, and Mark Secada, « You Give Apps Sensitive Personal Information. Then They Tell Facebook », *The Wall Street Journal*, 22 février 2019.

20. Facebook for Business, « Measuring Conversions on Facebook, Across Devices and in Mobile Apps », 14 août 2014.

21. Bender, Brad, « New digital innovations to close the loop for advertisers », *Google Ads & Commerce Blog*, 26 septembre 2016.

22. Federal Trade Commission, « FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook », 24 juillet 2019.

23. Chin, Kimberly, « Twitter Could Pay FTC Fine Over Alleged Privacy Violations », *The Wall Street Journal*, 3 août 2020.

24. Satariano, Adam, « Google Is Fined $57 Million Under Europe's Data Privacy Law », *The New York Times*, 21 janvier 2019.

25. Schiffer, Zoe, « Period tracking app settles charges it lied to users about privacy », *The Verge*, 13 janvier 2021.

26. Thompson, Stuart A., « These Ads Think They Know You », *The New York Times*, 30 avril 2019.

27. Venkatadri, Giridhari, Piotr Sapiezynski, et al., « Auditing Offline Data Brokers via Facebook's Advertising Platform », *The World Wide Web Conference*, 2019, pp. 1920-1930.

28. Leetaru, Kalev, « The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong », *Forbes*, 5 avril 2018.

29. Grothaus, Michael, « The top 7 iOS 14 privacy features: What you need to know », *Fast Company*, 16 septembre 2020.

30. Germain, Thomas, « How a Photo's Hidden 'Exif' Data Exposes Your Personal Information », *Consumer Reports*, 6 décembre 2019.

31. Helm, Burt, « Credit card companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism », *Fast Company*, 12 mai 2020.

32. Ramirez, Edith, Julie Brill, et al., « Data Brokers: A Call for Transparency and Accountability », *Federal Trade Commission*, mai 2014.

33. Oracle, « 12 Must-Ask Questions to Separate Fact from Fiction », www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf.

34. Hern, Alex, « 'Anonymous' browsing data can be easily exposed, researchers reveal », *The Guardian*, 1 août 2017.

35. Fowler, Geoffrey A., « You watch TV. Your TV watches back », *The Washington Post*, 18 septembre 2019.

36. X-Mode, « Data Licensing », xmode.io/data-licensing/.

37. Si l'âge de la personne associée à l'identifiant Apple enregistré sur un appareil est inférieur à 18 ans, l'accès à l'IDFA est désactivé par défaut et ne peut être accordé à aucune société de développement.

38. Aide Google Ads, « À propos des stratégies d'enchères intelligentes », support.google.com/google-ads/answer/7065882?hl=fr.

39. Litfin, Marne, « What is Mobile ad attribution? An introduction to app tracking », *Adjust*, 4 février 2019.

40. Cox, Joseph, « The IRS Is Being Investigated for Using Location Data Without a Warrant », *Vice*, 6 octobre 2020.

41. Cox, Joseph, « How the U.S. Military Buys Location Data from Ordinary Apps », *Vice*, 16 novembre 2020.

42. Cox, Joseph, « CBP Bought 'Global' Location Data from Weather and Game Apps » *Vice*, 6 octobre 2020.