

Une journée dans la vie de vos données

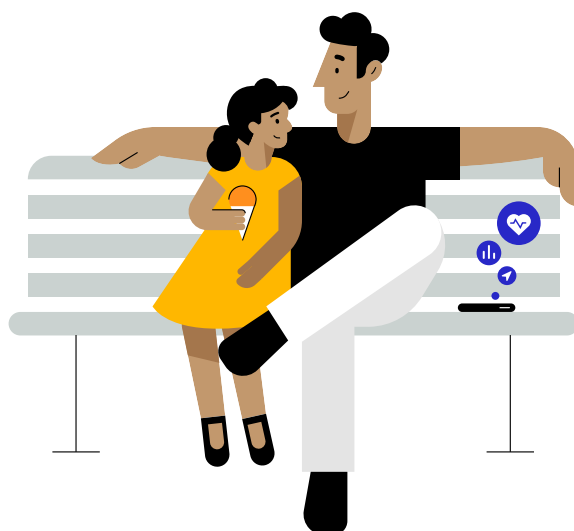
Une sortie au parc entre père et fille

Avril 2021

« Je crois que les gens sont intelligents et que certaines personnes sont prêtes à partager davantage de données que d'autres. Il faut leur poser la question. Encore et encore. Jusqu'à ce qu'elles vous demandent d'arrêter si elles en ont assez. Dites-leur précisément ce que vous comptez faire avec leurs données. »

Steve Jobs

Conférence All Things Digital, 2010



Au cours de la dernière décennie, une industrie vaste et peu transparente a amassé des quantités croissantes de données personnelles^{1,2}. Un écosystème complexe de sites web, d'apps, de médias sociaux, de courtiers en données et d'entreprises de technologie publicitaire traquent l'activité en ligne et hors ligne des utilisateurs et utilisatrices afin de recueillir leurs renseignements personnels. Ces données sont regroupées, partagées, agrégées et vendues dans des enchères en temps réel pour alimenter une industrie dont la valeur annuelle est estimée à 227 milliards de dollars¹. Et ce manège se répète tous les jours pendant que les gens vaquent à leur quotidien, souvent à leur insu, sans qu'ils aient autorisé quoi que ce soit^{3,4}. Voyons ensemble ce que cette industrie est capable d'apprendre sur un père et sa fille lors d'une agréable sortie au parc.

Le saviez-vous?

Des traqueurs sont intégrés dans les apps que vous utilisez tous les jours : une app compte en moyenne six traqueurs³.

La plupart des apps Android et iOS couramment utilisées sont dotées de traqueurs intégrés^{5,6,7}.

Des traqueurs sont souvent intégrés dans le code tiers pour faciliter le développement des apps. Grâce à eux, les développeurs permettent aussi à des entités tierces d'amasser et de lier les données que vous leur avez transmises par le biais de différentes apps avec d'autres données recueillies sur vous.

Les courtiers en données sont des entreprises qui collectent, dans le but de vendre, de céder sous licence ou de distribuer d'une autre manière à des tiers, les renseignements personnels de certaines personnes avec lesquelles ils n'entretiennent pas de relation directe³.



Des centaines de courtiers en données recueillent des renseignements en ligne et hors ligne⁸.

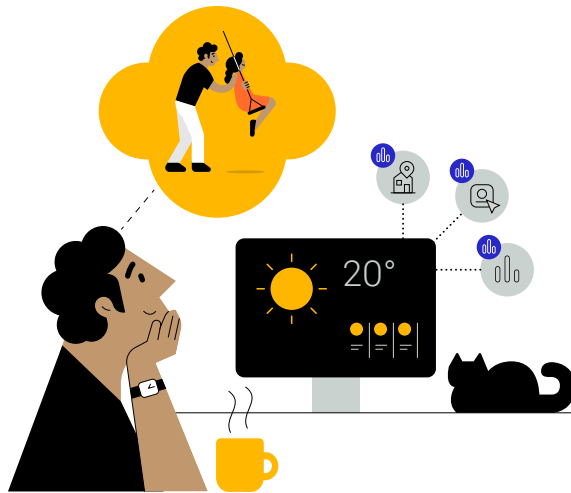
Un seul courtier arrive à collecter des données sur 700 millions de personnes dans le monde et à créer des profils de consommation qui intègrent jusqu'à 5 000 caractéristiques⁹.



Une étude a démontré que près de 20 % des apps développées spécialement pour les enfants collectent et partagent des données à caractère personnel sans qu'un consentement parental vérifiable ait été accordé¹⁰.



Tous les jours, vingt-quatre heures sur vingt-quatre, des milliards de publicités numériques s'affichent sous les yeux des internautes^{11,12,13}. Pendant les quelques millisecondes que prend la publicité pour se charger, se déroule une vente aux enchères en temps réel où les annonceurs tentent de mettre la main sur l'espace publicitaire, la plupart du temps en se fiant aux données personnelles recueillies^{14,15}.

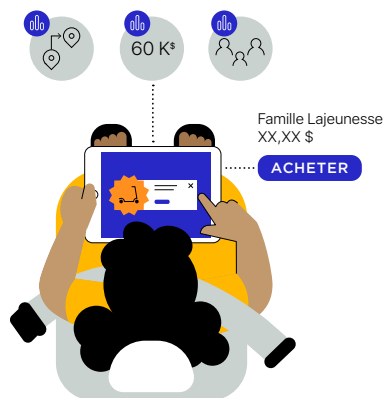


Jean planifie sa sortie au parc avec sa fille

Jean et Emma, sa fille de 7 ans, passent la journée ensemble. Le matin, Jean utilise son ordinateur pour consulter la météo et lire les nouvelles, puis se sert d'une app sur son téléphone pour vérifier l'état de la circulation avant de se rendre au parc situé à côté de l'école de sa fille. En chemin, pas moins de quatre apps installées sur le téléphone de Jean suivent son trajet et collectent périodiquement les données de localisation en arrière-plan^{16,17,18}. Une fois les données extraites de l'appareil, les développeurs de ces apps les vendent à une multitude de mystérieux courtiers en données dont Jean n'a jamais entendu parler^{16,17}. Même si les données de localisation amassées sont censées être confidentielles, les traqueurs intégrés à ces apps permettent aux courtiers en données de relier l'historique de localisation de Jean avec les données recueillies par les autres apps qu'il a utilisées^{16,19}. Les renseignements collectés par les apps auprès de différentes sources sont ainsi mis à la disposition de toutes les entreprises ou organisations qui souhaitent les acheter, et qui peuvent les utiliser pour établir le profil complet de Jean, y compris ses moindres déplacements quotidiens^{3,16}.

Emma joue à un jeu pendant le trajet

Sur le chemin du parc, Jean permet à sa fille de jouer à un jeu sur sa tablette. Quand elle ouvre l'app, elle voit une publicité annonçant une trottinette – et ce n'est pas un hasard. À l'instant même où l'app s'exécute, l'espace publicitaire est mis aux enchères¹⁴. Par le biais d'intermédiaires, les entreprises de publicité qui travaillent pour le fabricant de trottinettes savent qu'un espace publicitaire est disponible¹⁵. Ensuite, en se servant des données collectées auprès de Jean et d'Emma, les entreprises misent pour mettre la main sur cet espace¹⁵. Les partenaires publicitaires du fabricant de trottinettes continuent de recueillir de l'information sur le comportement de Jean et d'Emma après qu'ils aient vu la publicité pour déterminer s'ils ont cliqué dessus ou s'ils ont acheté la trottinette³. Ces partenaires vont continuer d'exposer Jean et Emma à la trottinette par tous les moyens, en suivant leur activité sur les différentes apps et pages web qu'ils utilisent sur l'ensemble des appareils de la famille^{3,20,21}.





Certaines apps demandent l'accès à plus de données qu'il ne leur en faut pour fournir leurs services – comme une app de clavier qui demande l'accès à la position exacte de la personne⁵.

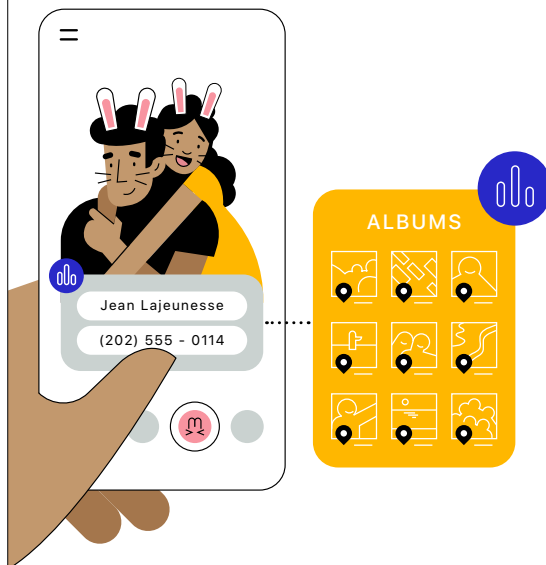


L'information peut être transmise à des réseaux de publicité, des éditeurs de publicité, des services de mesure et d'attribution, des courtiers en données, d'autres entreprises privées et même des organisations gouvernementales^{3,15,40,41,42}.

Des entreprises technologiques et de réseaux sociaux se sont exposées à un moment ou à un autre à des amendes de plusieurs millions de dollars pour avoir utilisé des données personnelles à des fins autres que celles spécifiées à l'utilisateur au moment de la collecte^{22,23,24,25}.



Les courtiers en données utilisent l'information recueillie pour donner des attributs aux utilisateurs et utilisatrices, et les classer en segments de marché extrêmement détaillés – par exemple, les personnes qui « essaient de perdre du poids, mais qui adorent les pâtisseries »²⁶. Toutefois, ces profils sont souvent erronés : une étude a prouvé que plus de 40 % des attributs s'avèrent inexacts^{27,28}.

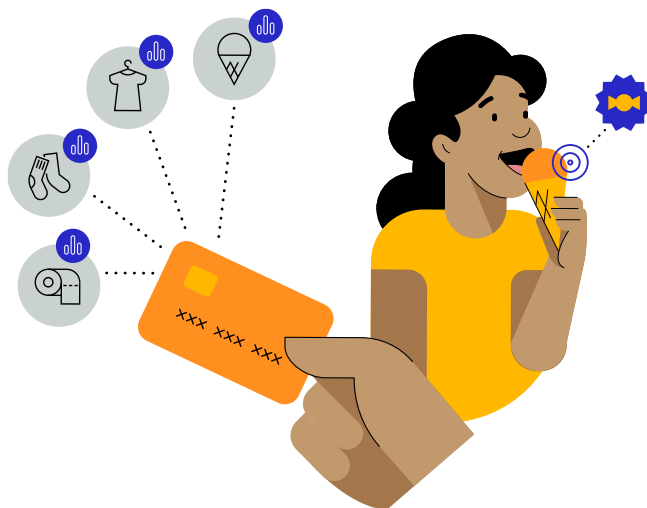


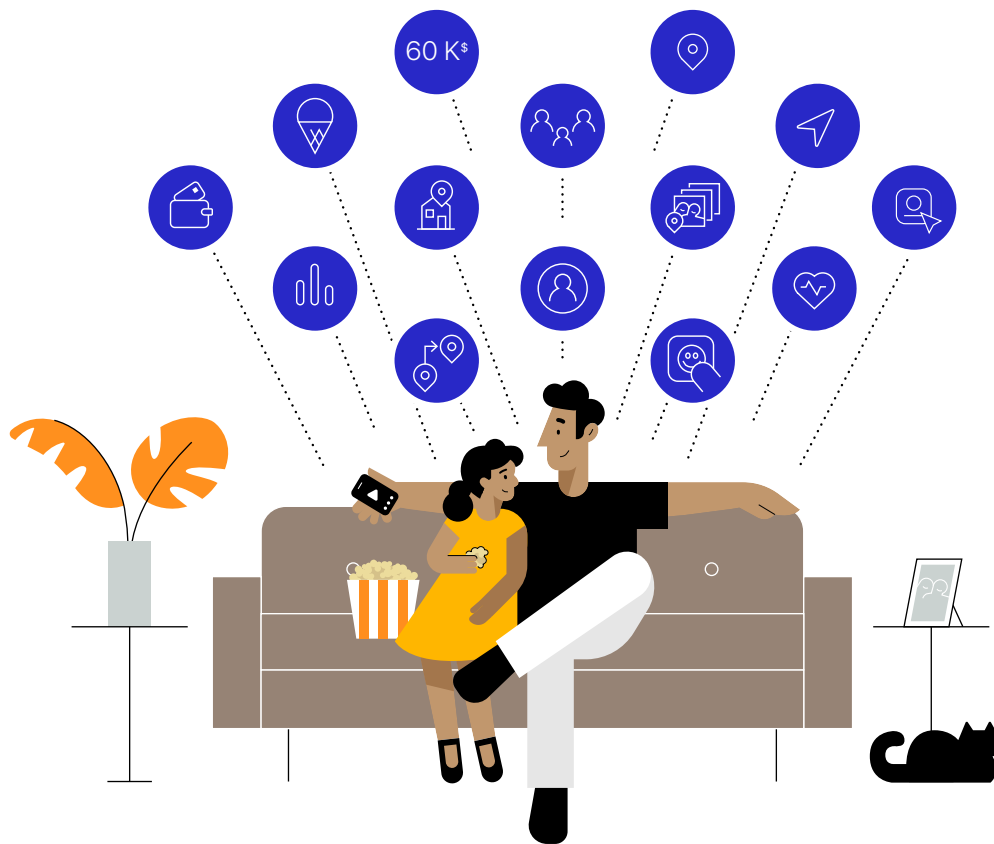
Jean et Emma prennent un selfie au parc

Plus tard, alors qu'ils sont au parc, Jean et Emma prennent un selfie. Ils s'amuse avec une app de photo, puis utilisent un filtre pour s'ajouter des oreilles de lapin. Mais, en plus d'avoir accès au selfie du parc, l'app de filtres est capable d'accéder à toutes les photos de l'appareil ainsi qu'à leurs métadonnées^{29,30}. Jean publie la photo avec l'app d'un média social. L'app relie l'activité en ligne de Jean à une mine de renseignements collectés par d'autres apps, comme ses données démographiques et ses habitudes d'achat, en utilisant une adresse courriel, un numéro de téléphone ou un identifiant publicitaire³.

Un arrêt à la crèmerie avant de rentrer

En rentrant à la maison, Jean et Emma s'arrêtent pour manger une crème glacée. En payant avec sa carte de crédit, Jean ajoute de précieuses informations à son profil de consommation déjà bien garni : l'adresse du commerce et le montant qu'il a dépensé^{31,32,33}. L'une des apps qui suivent les déplacements de Jean a pu déterminer qu'Emma et lui se sont aussi arrêtés dans un magasin de jouets³. Les endroits où les membres de la famille ont fait des achats pendant la journée sont communiqués aux courtiers en données. Ces derniers profitent de cette information et du fait qu'ils savent que Jean a une jeune enfant pour bombarder ses appareils mobiles de publicités ciblées montrant des friandises et le magasin de jouets qu'ils ont visité¹⁷.





À la fin de la journée, des entreprises des quatre coins du monde avec lesquelles Jean n'a jamais eu d'interactions ont actualisé leurs profils avec des données sur lui et sa fille. Ces entreprises savent maintenant beaucoup de choses sur Jean et Emma : l'endroit où ils habitent, le parc qu'ils ont visité, les nouvelles qu'ils ont lues en ligne, les pages de produits qu'ils ont consultées, les publicités qu'ils ont regardées, les magasins où ils sont allés et leurs habitudes d'achat^{3,34}. Ces données ont été recueillies et suivies à travers plusieurs des apps utilisées par Jean et sa fille au cours de la journée, ainsi qu'à partir d'autres sources. Jean ignorait qu'autant de renseignements avaient été recueillis au fil de la journée; il n'avait pas toujours eu le contrôle de ce qu'il partageait, et n'avait pas sciemment autorisé la collecte des données^{3,4}. De retour à la maison, alors que Jean et sa fille cherchent un film d'animation sur une app de leur télé intelligente pour terminer la soirée en beauté, le cycle de suivi, échange de données, mise aux enchères et ciblage se répète sans relâche^{35,36}.

Les principes d'Apple en matière de respect de la vie privée

Pour Apple, la vie privée est un droit fondamental. La conception de nos produits et services est guidée par quatre principes essentiels en matière de confidentialité :

Pour en savoir plus sur les fonctionnalités de confidentialité mises de l'avant par Apple et sur les efforts déployés pour protéger la vie privée des utilisatrices et utilisateurs, consultez apple.com/ca/fr/privacy.

Pour en savoir plus sur la façon dont Safari protège votre vie privée, consultez le [document sur Safari](#) (en anglais).

Pour en savoir plus sur la façon dont Apple protège vos données de localisation, consultez le [document sur le service de localisation](#) (en anglais).



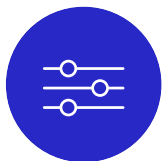
Réduction des données recueillies

Nous collectons uniquement la quantité minimale de données nécessaire pour vous fournir le service dont vous avez besoin.



Traitement sur l'appareil

Autant que possible, les données sont traitées sur l'appareil plutôt que d'être envoyées aux serveurs d'Apple afin de protéger la vie privée et de limiter la collecte de données.



Transparence et contrôle lors de l'utilisation

Apple veille à ce que les utilisateurs et utilisatrices puissent avoir le plein contrôle de leurs données et savoir quels renseignements sont partagés et à quelles fins.



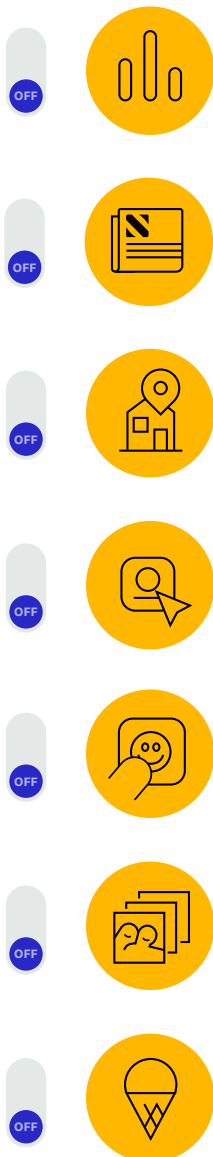
Sécurité

Le matériel et les logiciels font équipe pour assurer la sécurité de vos données.

À travers ces quatre principes, l'objectif d'Apple est depuis toujours le même : **donner aux personnes le contrôle de leurs données et la liberté de les partager comme ils l'entendent, de manière sûre et en toute connaissance de cause.** C'est pourquoi depuis vingt ans Apple innove sans arrêt pour concevoir des produits et services qui protègent la vie privée de ceux et celles qui les utilisent. Par exemple, nous faisons appel à l'intelligence embarquée et à d'autres fonctionnalités pour limiter la collecte de données dans nos apps, navigateurs et services en ligne, et jamais nous ne créons de profils exhaustifs sur les personnes qui utilisent nos apps et services.

Les fonctionnalités de confidentialité d'Apple offrent à Jean plus de transparence et un meilleur contrôle de ses données

L'histoire de la journée de Jean et d'Emma illustre bien les problèmes de confidentialité et les solutions qu'Apple s'efforce de mettre en place pour y remédier.



Jean planifie sa sortie au parc avec sa fille

Si Jean avait utilisé Safari pour consulter la météo sur son ordinateur, **la prévention intelligente du suivi aurait bloqué par défaut le suivi** de son activité.

Si Jean avait ouvert Apple News pour lire les nouvelles du matin, **Apple lui aurait proposé des contenus basés sur ses préférences, sans utiliser d'information sur lui ou sur ce qu'il lit.**

Si Jean avait utilisé l'app Plans d'Apple pour vérifier l'état de la circulation, **ses données de localisation auraient été liées à un identifiant aléatoire régulièrement réinitialisé plutôt qu'à Jean lui-même.** Au bout du compte, personne d'autre que Jean n'aurait su où il se trouvait.

Sur iPhone, Jean aurait reçu des **rappels périodiques pour lui dire qu'une app accédait à sa localisation en arrière-plan.** Avant de partager sa position avec une app, Jean aurait pu choisir de donner seulement son emplacement approximatif, ou de partager sa position exacte une seule fois.

Emma joue à un jeu pendant le trajet

Sur iPad, la fonctionnalité bientôt offerte de **transparence du suivi par les apps** aurait permis à Jean **de décider** s'il voulait ou non autoriser le jeu à suivre l'activité d'Emma sur d'autres apps et sites web.

Les réseaux publicitaires qui utilisent l'API SKAdNetwork d'Apple auraient pu mesurer l'efficacité de leurs publicités sans accéder à des renseignements permettant d'identifier Jean.

Jean et Emma prennent un selfie au parc

Sur iPhone, Jean aurait **eu le choix de permettre à l'app de filtrer d'accéder uniquement au selfie en question** plutôt qu'à l'ensemble de sa photothèque.

Un arrêt à la crèmerie avant de rentrer

Si Jean avait payé les crèmes glacées à l'aide d'Apple Card, **sa banque n'aurait pas utilisé ses données de transaction à des fins de marketing.** Et s'il avait utilisé Apple Pay, Apple aurait employé l'intelligence embarquée pour permettre à Jean de voir l'historique de ses transactions sur son iPhone, sans qu'Apple obtienne d'information sur l'endroit où il a magasiné, sur ce qu'il a acheté ou sur l'argent qu'il a dépensé.

Au bout du compte, les produits Apple et les fonctions de confidentialité auraient offert à Jean plus de transparence et de contrôle tout au long de la journée en ce qui concerne la quantité de données partagées et leur utilisation.

La transparence du suivi par les apps et la nouvelle rubrique sur la confidentialité dans l'App Store

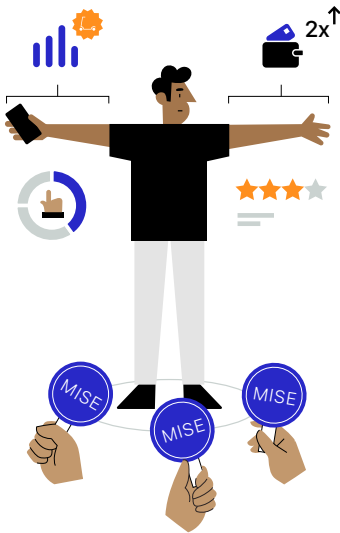
[Apple fait un pas de plus pour protéger la vie privée des utilisateurs et utilisatrices à l'échelle de son vaste écosystème d'apps.](#) Alors qu'un ensemble complexe et croissant d'entités accède aux données personnelles pour les suivre et les monnayer, Apple lance deux nouvelles fonctionnalités qui donneront aux utilisatrices et utilisateurs plus de transparence, de visibilité et d'options, leur permettant ainsi de faire des choix éclairés et d'exercer un contrôle accru sur la confidentialité de leurs données.

[Bientôt, à la suite de la prochaine mise à jour bêta d'Apple, la transparence du suivi par les apps obligera les développeurs à obtenir une autorisation avant de suivre les données personnelles dans les apps et sur les sites web d'entreprises tierces.](#) Dans Réglages, il sera possible de voir quelles apps ont demandé à suivre les données personnelles et de modifier les autorisations accordées. Cette exigence, qui prendra effet au début du printemps avec le lancement d'une nouvelle version d'iOS 14, d'iPadOS 14 et de tvOS 14, a déjà reçu le soutien d'organismes voués à la protection des renseignements personnels des quatre coins du monde. En concevant cette fonctionnalité, Apple a voulu offrir aux personnes qui utilisent ses appareils un plus haut niveau de transparence et de contrôle, tout en permettant à la publicité d'exister comme moyen approprié et viable de soutenir les apps et les contenus web. L'arrivée de fonctionnalités précédentes, comme la prévention intelligente du suivi dans Safari, a prouvé que la publicité pouvait demeurer un outil efficace, même en renforçant les mesures de protection de la vie privée. La transparence du suivi par les apps permet de faire des choix plus éclairés concernant les apps qu'on installe et les autorisations qu'on leur accorde. Grâce à cette fonctionnalité, il est désormais possible de décider si l'on souhaite ou non permettre le suivi par une app. Si on juge qu'une app est fiable et qu'on lui accorde cette permission, l'entreprise de développement peut continuer à faire le suivi.

[En plus de l'autorisation de suivi obligatoire, Apple a récemment apporté des modifications aux pages de produits de l'App Store afin d'améliorer la transparence.](#) Avec la nouvelle rubrique Confidentialité de l'app, l'App Store permet de mieux comprendre les pratiques de confidentialité des applications. La page de produit de chaque app doit comprendre un résumé clair des pratiques employées par le développeur en matière de respect de la vie privée. Les pages des détails contiennent de l'information sur les types de données qui sont recueillies par les apps, comme les photos, la localisation et les coordonnées personnelles. Elles fournissent aussi des détails supplémentaires sur la manière dont chaque type de donnée est utilisée par le développeur, y compris si elle l'est à des fins de suivi et si elle est liée à l'utilisateur ou l'utilisatrice. Tous les développeurs d'apps, Apple y compris, ont l'obligation de déclarer eux-mêmes leurs pratiques de confidentialité.

[Les nouveaux paramètres de suivi par les apps, ainsi que l'information sur la transparence et la confidentialité récemment ajoutée aux pages de produits de l'App Store, permettent aux utilisateurs et utilisatrices](#) de savoir plus facilement à quelles fins leurs données personnelles sont utilisées et d'exercer un meilleur contrôle sur leur vie privée, en mettant en lumière des pratiques qui étaient jusqu'ici opaques et dissimulées. Apple continuera à concevoir des technologies novatrices pour protéger la vie privée et à développer de nouvelles méthodes pour sécuriser vos données personnelles.

Une journée dans la vie d'une publicité



Enchères publicitaires

Quand Emma a vu apparaître une publicité de trottinette sur l'appareil de son père, ce n'était pas un hasard. Les annonceurs participent à des ventes aux enchères pour pouvoir afficher des publicités sur des appareils³⁷. Voici une explication simplifiée de ce qui s'est passé, en une fraction de seconde, pour que cette publicité apparaisse à l'écran à ce moment précis.

1. Le développeur de l'app qu'utilise Emma a confié à une entreprise de technologie publicitaire la mise aux enchères en temps réel de ses espaces publicitaires¹⁴.
2. Quand Emma a ouvert l'app, le réseau publicitaire a recueilli des données sur l'appareil de Jean (comme les apps en cours d'utilisation, la localisation et l'identifiant publicitaire de l'appareil) et auprès d'entités tierces, en se basant sur l'identifiant publicitaire de Jean et sur d'autres données permettant de faire le suivi³.
3. Le réseau publicitaire partage certaines de ces données, en particulier l'identifiant publicitaire, avec des annonceurs potentiels. Avant de miser, les annonceurs essaient généralement d'en savoir le plus possible sur la personne, sur la base de leurs propres données, mais aussi des données personnelles recueillies et agrégées au moyen de dispositifs de suivi et de profilage^{3,15}.
4. Plus les caractéristiques de Jean et d'Emma – obtenues à partir de leurs données – correspondent au public cible des annonceurs, plus les annonceurs sont nombreux à tenter d'acquérir l'espace^{15,38}.
5. Ici, c'est la publicité de la trottinette qui a remporté l'enchère, et c'est pourquoi elle s'est affichée sur l'appareil qu'Emma utilisait¹⁴.

Parce que l'enchère publicitaire se déroule en une fraction de seconde, la partie qui achète et celle qui vend recueillent, échangent et utilisent toutes deux des données personnelles pour faire des offres et afficher des publicités^{14,15}.



Attribution publicitaire

Après lui avoir présenté l'annonce, les entreprises de publicité qui travaillent pour le fabricant de trottinettes vont vouloir évaluer les effets de la pub sur le comportement d'Emma. On appelle ce processus « attribution ».

Pour ce faire, l'annonceur va tenter de suivre l'activité d'Emma sur l'appareil qu'elle utilise pour collecter de l'information sur son activité sur le web et dans les apps, et même sur ses déplacements hors ligne.

- **Si la publicité concerne un produit**, l'annonceur peut essayer de savoir si la personne a par la suite visité son site web ou son magasin physique pour acheter le produit³.
- **Si la publicité concerne une app**, l'annonceur tentera de savoir si la personne l'a installée ou non. On appelle ce processus « attribution mobile »³⁹.

Les annonceurs ont aussi recours à l'attribution pour « optimiser » leur campagne publicitaire afin de rejoindre les groupes auprès desquels elles seront le plus efficaces³.

Mais ce n'est pas la seule façon de faire. Les annonceurs peuvent mesurer l'efficacité de leurs campagnes publicitaires auprès des membres de leurs groupes cibles sans suivre leur activité. Apple a mis au point des outils de mesure qui respectent la vie privée :

SKAdNetwork permet aux annonceurs de savoir combien de personnes ont installé une app après en avoir vu la publicité, et d'ainsi mesurer l'efficacité de leur campagne publicitaire. Mais comme l'outil est conçu de manière à ne partager aucune donnée sur la personne ou son appareil, les annonceurs ne peuvent pas faire de suivi.

Private Click Measurement, une fonctionnalité pour les apps sous iOS et iPadOS 14.5, permet aux annonceurs de mesurer l'efficacité des publicités qui dirigent les internautes vers un site web, tout en limitant la collecte de données grâce au traitement de l'information sur l'appareil. Quand une personne clique sur l'annonce d'un produit dans une app – ou le navigateur web –, Private Click Measurement peut informer l'annonceur qu'un clic a été effectué sur sa publicité et qu'il a entraîné une certaine activité sur son site web, comme une visite ou un achat, mais sans lui donner aucune autre information sur la provenance de ce clic.

Foire aux questions

Vais-je pouvoir continuer d'utiliser toutes les fonctionnalités de l'app si je sélectionne « Demander à l'app de ne pas faire de suivi »?

Oui. Les développeurs doivent vous donner accès à toutes les fonctionnalités de l'app même si vous n'autorisez pas le suivi.

Que sont les identifiants et comment sont-ils utilisés?

Un identifiant tel que l'identifiant publicitaire IDFA utilisé avec une adresse courriel permet d'identifier un appareil donné sur un réseau. Chaque fois qu'ils détectent l'identifiant de votre appareil en y associant l'utilisation que vous en faites, les identifiants donnent aussi aux annonceurs la possibilité de créer un profil détaillé de votre activité sur une variété d'apps et de sites web.

Qu'est-ce qu'un identifiant publicitaire IDFA (Identifier For Advertisers)?

L'IDFA est un identifiant contrôlable par l'utilisateur qu'iOS assigne à chaque appareil. Comme l'IDFA est associé au logiciel plutôt qu'à l'appareil physique lui-même, l'utilisateur ou l'utilisatrice peut le bloquer pour une app en particulier lorsque la fonction de transparence du suivi l'invite à le faire – et même tenir les rênes de l'ensemble du suivi basé sur l'IDFA.

Est-ce qu'Apple peut me garantir que l'app ne suivra pas mon activité si je sélectionne « Demander à l'app de ne pas faire de suivi »?

Si vous sélectionnez « Demander à l'app de ne pas faire de suivi », le développeur ne sera pas en mesure d'accéder à l'identifiant publicitaire (IDFA), lequel est souvent utilisé pour faire le suivi. Le développeur a également l'obligation de respecter votre choix au-delà de l'identifiant publicitaire. Cette obligation est liée aux politiques que le développeur accepte en soumettant son app à l'App Store pour sa distribution. Si nous découvrons qu'un développeur suit des personnes qui ont demandé de ne pas l'être, nous exigerons qu'il modifie ses pratiques pour respecter leur choix, à défaut de quoi son app pourrait être retirée de l'App Store.

Si j'utilise un de mes comptes de réseaux sociaux pour me connecter à une app, l'entreprise de ce réseau social peut-elle suivre mon activité sur l'app en question?

Cela dépend si vous lui avez donné l'autorisation de vous suivre ou non. Si vous avez choisi « Demander à l'app de ne pas faire de suivi », l'app ne doit pas faire le suivi de votre activité sur d'autres apps ou sites web à des fins publicitaires ni partager vos renseignements personnels avec des courtiers en données. En résumé, l'app ne doit pas fournir vos renseignements à l'entreprise de réseau social si l'objectif est de les utiliser à des fins publicitaires.

Comment Apple s'assure-t-elle que l'information sur la confidentialité présentée sur les pages de produits de l'App Store est exacte?

Un peu comme pour les catégories d'âge sur l'App Store, les développeurs sont responsables d'établir et de communiquer leurs propres pratiques en matière de confidentialité. Si nous découvrons qu'un développeur pourrait avoir fourni des renseignements inexacts, nous collaborerons avec lui dans le but de corriger la situation.

Qu'est-ce qu'un courtier en données?

De manière générale, les courtiers en données sont des entreprises qui recueillent les renseignements personnels de certaines personnes avec lesquelles ils n'entretiennent pas de relation directe, pour les vendre, les céder sous licence ou les distribuer par d'autres moyens à des tiers. L'activité des courtiers en données est définie par la loi dans certains pays.

Sources

1. GRÖNE, Florian, Pierre PÉLADEAU et coll., « Tomorrow's data heroes », *Strategy+Business*, 19 février 2019.
2. REINSEL, David, John Gantz et coll., « The Digitization of the World: From Edge to Core », *IDC*, novembre 2018.
3. Competition and Markets Authority, « Online platforms and digital advertising market study », 1^{er} juillet 2020.
4. HITLIN, Paul et 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 coll., « Third Party Tracking in the Mobile Ecosystem », *Actes de la 10^e conférence de l'ACM sur les sciences du web*, 2018, p. 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, Rapport 10-K 2018, déposé le 25 mai 2018, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.
10. REYES, Irwin, Primal Wijesekera et coll., « "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale », *Actes du symposium sur les technologies d'amélioration de la confidentialité*, vol. 2018, no 3, 2018, p. 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 et 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. et 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 et 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 coll., « Auditing Offline Data Brokers via Facebook's Advertising Platform », *The World Wide Web Conference*, 2019, p. 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 coll., « 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^{er} 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 donné à aucun développeur.
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.