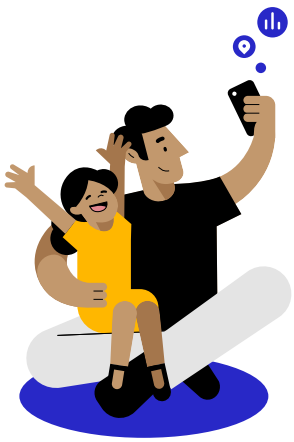


Un día en la vida de tus datos

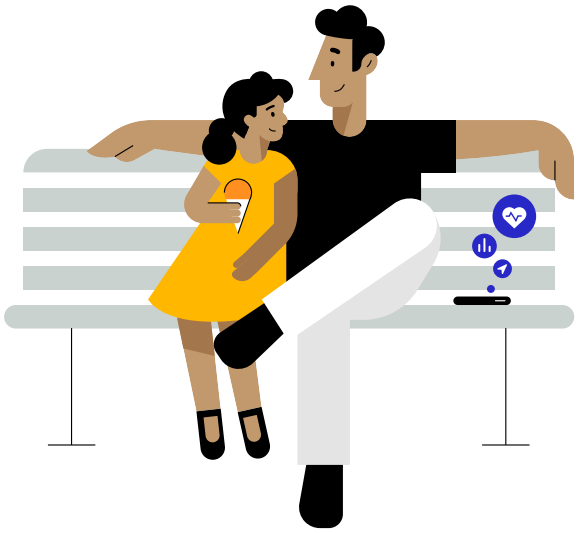
Un día de parque para un padre y su hija

Abril de 2021

«Creo que las personas son inteligentes y que hay algunas que están dispuestas a compartir más datos que otras. Pregúntales. Pregúntales todo el rato hasta que te digan que no quieren más preguntas. Infórmales de qué es lo que vas a hacer exactamente con sus datos».

Steve Jobs

Conferencia de All Things Digital (2010)



Durante la última década, un sector grande y opaco ha estado acumulando cada vez más datos personales.[1,2] Un complejo ecosistema de páginas web, apps, redes sociales, intermediarios de datos y empresas de tecnología publicitaria rastrean a los usuarios tanto dentro como fuera de internet para recopilar sus datos. Unos datos que se juntan, se comparten, se agrupan y se subastan en tiempo real para alimentar un gigante que mueve 227.000 millones de dólares al año.[1] Esto ocurre todos los días y forma parte de nuestras vidas cotidianas, muchas veces sin que lo sepamos y sin nuestro permiso.[3,4] Veamos todo lo que este sector es capaz de conocer sobre un padre y su hija que van a pasar un agradable día en el parque.

¿Lo sabías?

Los rastreadores están integrados en las apps que usas a diario, a una media de seis por app.[3] La mayoría de las apps más conocidas para iOS y Android tienen estos rastreadores.[5,6,7]

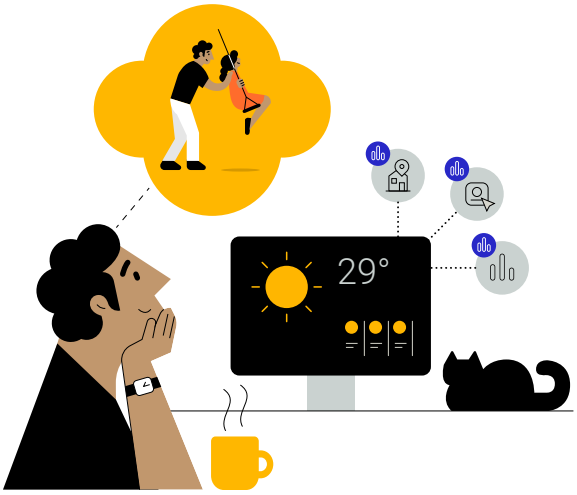
Los rastreadores suelen estar incluidos en el código de empresas externas que ayuda a los desarrolladores a crear las apps. Al incluir rastreadores, los desarrolladores también permiten que estas empresas externas tengan acceso a los datos que el usuario ha compartido y los vinculen con otras apps y con otro tipo de información que se haya recopilado sobre esa persona.

Los intermediarios de datos pueden recopilar, vender, licenciar o ceder a terceros la información privada de personas con las que no tienen ninguna relación directa.[3]

Cientos de intermediarios de datos recaban información dentro y fuera de internet.[8]
Un solo intermediario puede recopilar datos sobre 700 millones de consumidores en todo el mundo, lo que permite crear perfiles de consumo con hasta 5.000 características distintas.[9]

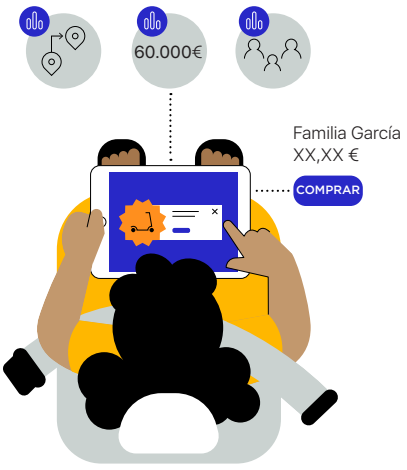
Según un estudio, aproximadamente el 20 % de las apps para niños permite a los desarrolladores recoger y compartir información personal identificable sin que se pueda comprobar que un adulto ha dado su consentimiento.[10]

Cada hora, se muestran miles de millones de anuncios digitales a los usuarios de internet.[11,12,13]
En los pocos milisegundos que tarda en cargar un anuncio, tiene lugar una subasta en la que los anunciantes pujan por el espacio del anuncio y, para ello, suelen basarse en los datos personales que el rastreador ha conseguido sobre ese usuario.[14,15]



Juan quiere pasar un día en el parque con su hija

Juan y su hija Emma, de siete años, van a pasar el día juntos. Por la mañana, Juan busca en el ordenador información sobre el tiempo, lee las noticias y consulta en una app de mapas de su smartphone el estado del tráfico hasta el parque que está cerca del colegio de su hija. Por el camino, cuatro apps de su teléfono recopilan y rastrean en segundo plano los datos de su ubicación.[16,17,18] Después de extraer los datos del dispositivo, los desarrolladores de apps los venden a un centro externo de intermediarios de datos nada transparente y del que Juan no ha oído hablar nunca.[16,17] Aunque se supone que los datos que han recopilado sobre su ubicación son anónimos, el rastreo de usuarios permite a los intermediarios vincular el historial de ubicaciones de Juan de estas apps con la información que hayan recabado a partir de su uso de otras apps.[16,19] Esto significa que los datos que tienen de las diferentes apps y otras fuentes pueden acabar en manos de cualquier empresa u organización y utilizarse para crear un perfil completo sobre Juan que incluya todos sus movimientos a lo largo del día.[3,16]



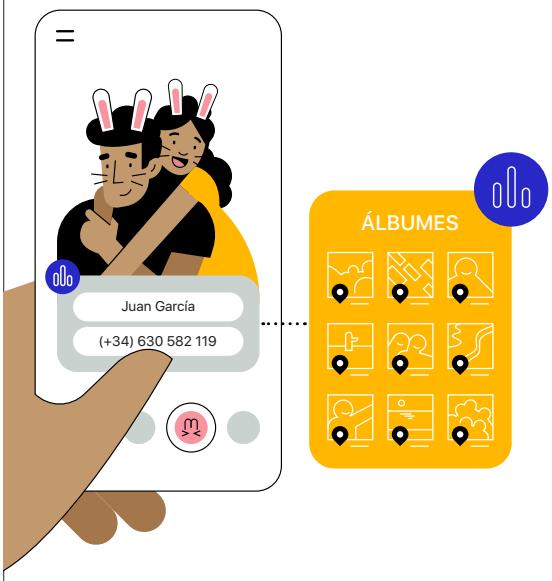
Emma juega a un juego de camino al parque

Mientras van al parque, Juan deja a su hija jugar con la tablet. Al abrir la app, le aparece un anuncio de un patinete, y no es por casualidad. En la décima de segundo que ha tardado la app en cargarse, se ha subastado el espacio del anuncio.[14] Las empresas de publicidad que trabajan para el fabricante de patinetes han sabido, gracias a los intermediarios, que ese anuncio estaba disponible.[15] Con los datos personales que habían recopilado de Juan y Emma, han pujado por el anuncio.[15] Los anunciantes de la empresa de patinetes siguen recogiendo información sobre el comportamiento de Juan y Emma después de ver el anuncio y ven si han hecho clic en él o si han comprado el patinete.[3] Y seguirán mostrando ese anuncio de todas las formas que puedan, siguiéndoles por las distintas apps y sitios web que visiten en todos los dispositivos de Juan.[3,20,21]

Hay apps que piden tener acceso a más datos de los que son necesarios para ofrecer su servicio. Por ejemplo, cuando una app de teclado solicita tener acceso a la ubicación exacta.[5]

El intercambio de información puede ir a redes de publicidad, editores de anuncios, proveedores de atribución y medición, intermediarios de datos, otras empresas privadas e incluso organizaciones gubernamentales.[3,15,40,41,42] Las empresas de redes sociales y de tecnología publicitaria tienen que pagar o han pagado multas millonarias por usar datos personales con fines distintos de los que especificaron a los usuarios en el momento de recopilarlos.[22,23,24,25]

Los intermediarios usan los datos que recogen para asignar atributos a los usuarios y agruparlos en segmentos de mercado hiperdetallados, como «personas que quieren perder peso pero van a pastelerías».[26] Sin embargo, estos perfiles suelen ser incorrectos. De hecho, más del 40 % de los atributos son inexactos según un estudio.[27,28]

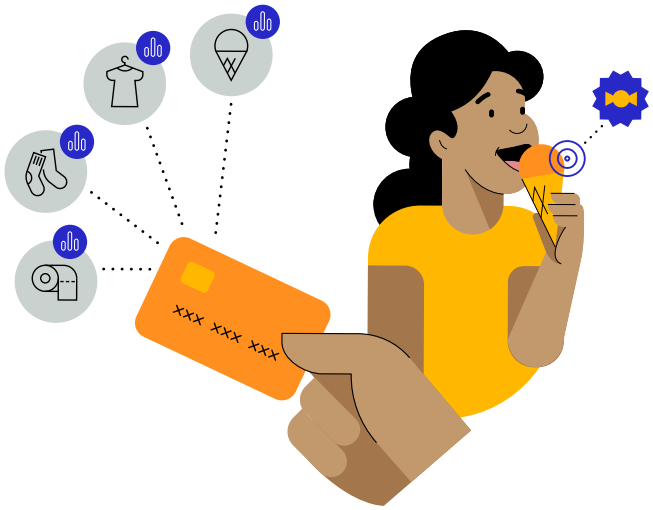


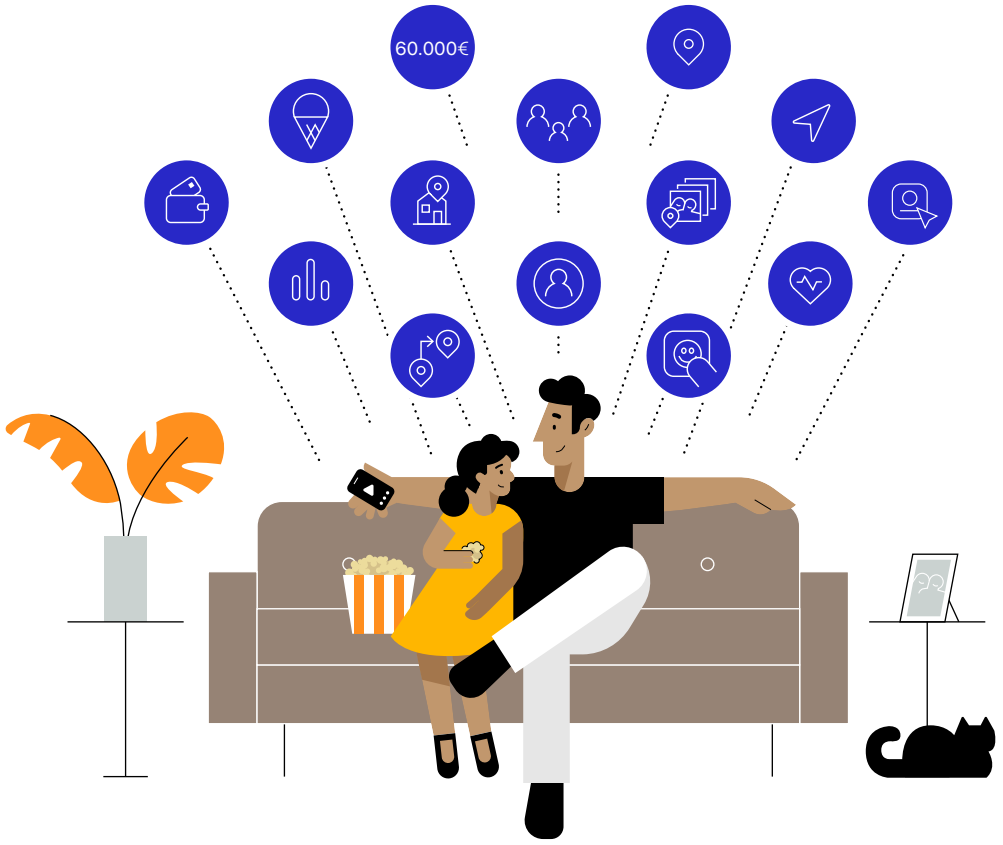
Juan y Emma se hacen un selfie en el parque

Más tarde, en el parque, Juan y Emma se hacen un selfie. Juegan con una app de filtros y se ponen orejas de conejo en la foto. Pero la app de filtros puede acceder a todas las fotos del dispositivo y a los metadatos adjuntos, no solo al selfie del parque.[29,30] Juan publica la foto en una app de redes sociales. La app vincula la actividad online de Juan en ese momento con un montón de datos recopilados por otras apps, como su información demográfica y sus hábitos de compra, a través de una dirección de correo electrónico, un número de teléfono o un identificador de publicidad.[3]

Una parada de camino a casa para comprar un helado

De vuelta a casa, Juan y Emma paran a comerse un helado. Juan paga el helado con la tarjeta de crédito, y ya hay más información que se añade al completo perfil de datos sobre sus preferencias: la ubicación de la tienda y cuánto se ha gastado.[31,32,33] Una de las apps que rastrea la localización de Juan sabe que su hija y él también se han parado en una juguetería.[3] La información sobre los establecimientos en los que compra la familia pasa a los intermediarios de datos, que la combinan con lo que ya saben (que Juan tiene una hija pequeña) para bombardear el dispositivo del padre con anuncios personalizados de todo tipo de dulces y de la tienda de juguetes que visitaron.[17]





Al final del día, un buen número de empresas de todo el mundo con las que Juan nunca ha tenido ningún contacto han actualizado sus perfiles con información sobre él y su hija. Estas empresas saben dónde está la casa de la familia, el parque al que van, las páginas web de noticias que leen, los productos que han buscado, los anuncios que han visto, sus hábitos de consumo y las tiendas a las que han ido.[3,34] Estos datos se han recogido y rastreado a través de las distintas apps que Juan y su hija han usado durante el día, y también a través de otras fuentes. Juan no tenía ni idea de la cantidad de datos que se iban recopilando a lo largo del día, no siempre lo podía controlar y no dio su permiso conscientemente para que ocurriera.[3,4] Al buscar una película infantil en una app de su televisor inteligente antes de irse a dormir, el ciclo de rastreo, intercambio de datos, subastas y retargeting (volver a mostrar el mismo anuncio) continúa.[35,36]

Puedes encontrar más información sobre las prestaciones de privacidad de Apple y el trabajo que está haciendo para proteger la privacidad de los usuarios en apple.com/es/privacy.

También tienes más detalles sobre cómo Safari protege la privacidad en el libro blanco de Safari.

Si quieres saber cómo protege Apple tus datos de localización, consulta el libro blanco de los servicios de localización.

Principios de privacidad de Apple

Apple cree que la privacidad es un derecho humano fundamental. Cuando diseñamos nuestros productos y servicios, nos guiamos por nuestros cuatro principios de privacidad fundamentales:

Minimización de datos

Recopilamos la cantidad mínima de datos necesaria para ofrecerte lo que necesitas con respecto a un servicio determinado.

Procesamiento en el dispositivo

En la medida de lo posible, procesamos los datos en el dispositivo en lugar de enviarlos a servidores de Apple. De esta forma, protegemos la privacidad del usuario y minimizamos la recopilación de datos.

Transparencia y control para los usuarios

Nos aseguramos de que los usuarios sepan qué datos se comparten y cómo se usan. También les damos control sobre ellos.

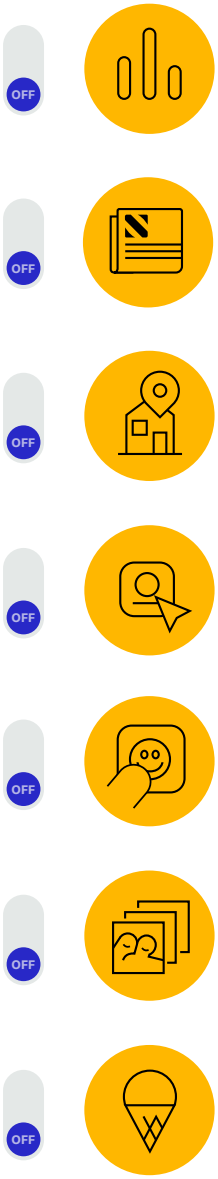
Seguridad

El hardware y el software trabajan juntos para garantizar la seguridad de los datos.

El objetivo de Apple con estos cuatro principios siempre ha sido permitir a los usuarios compartir los datos que quieran y hacerlo de una forma segura, entendiendo y controlando todo el proceso. Esta es la razón por la que, durante las dos últimas décadas, Apple ha seguido innovando para garantizar la privacidad de los usuarios en todos nuestros productos y servicios. Por ejemplo, empleamos tecnologías de inteligencia integradas y otras prestaciones para limitar todo lo posible la cantidad de datos que recopilamos en nuestras apps, navegadores y servicios online, y no creamos un perfil de usuario completo a partir de todas nuestras apps y servicios.

Las prestaciones de privacidad de Apple ofrecen a Juan mayor transparencia y control sobre sus datos

La historia de lo que hacen en un día Juan y Emma nos sirve para ilustrar los problemas de privacidad y las soluciones en las que estamos trabajando en Apple.



Juan quiere pasar un día en el parque con su hija

Si Juan hubiera usado Safari como navegador para consultar el tiempo en su ordenador, el antirrastreo inteligente habría evitado el rastreo de su actividad de forma predeterminada.

Si Juan hubiera usado Apple News para leer las noticias por la mañana, Apple le habría mostrado contenido basado en sus intereses, sin saber quién es ni recordar lo que ha leído.

Si Juan hubiera usado Mapas de Apple para consultar el estado del tráfico, sus datos de localización se habrían vinculado con un identificador aleatorio que cambia con frecuencia y que no se habría vinculado a él. De esta forma, solo Juan habría sabido en qué sitio estaba.

Si hubiera usado un iPhone, este le habría recordado a Juan cada cierto tiempo qué apps acceden a su ubicación en segundo plano. Antes de compartir su ubicación con una app, Juan podría haber elegido compartir solo su ubicación aproximada o hacerlo solo una vez.

Emma juega a un juego de camino al parque

En un iPad, la transparencia en el seguimiento de las apps, que estará disponible pronto, habría dado a Juan la opción de permitir o no que el juego registrara la actividad de Emma en las apps y sitios web de otras empresas.

Las redes de anuncios que usan la API SKAdNetwork de Apple habrían podido medir la eficacia total de sus anuncios sin acceder a información que pudiera asociarse con el dispositivo de Juan.

Juan y Emma se hacen un selfie en el parque

En un iPhone, Juan habría tenido la opción de dar acceso a la app de filtros solo al selfie, y no a toda la biblioteca de fotos.

Una parada de camino a casa para comprar un helado

Si Juan hubiera pagado el helado con la Apple Card, su banco no habría usado la información sobre la transacción con fines de marketing. Si hubiera pagado con Apple Pay, Apple podría haber usado las tecnologías de inteligencia integradas para que Juan viese los movimientos de su tarjeta en el iPhone, y Apple no habría obtenido información sobre su compra, dónde la hizo y cuánto se gastó.

Al final del día, los productos y las prestaciones de privacidad de Apple ofrecen a Juan mayor transparencia y control sobre los datos que comparte y cómo se usan.

Transparencia en el seguimiento de las apps y nueva sección de información sobre privacidad en el App Store

Apple va un paso más allá a la hora de proteger la privacidad de los usuarios dentro del ecosistema de apps. Ahora que cada vez más entidades acceden, rastrean y monetizan los datos personales de los consumidores, Apple va a introducir dos nuevas prestaciones que buscan ofrecer a los usuarios más transparencia, visibilidad y opciones para tomar decisiones mejor fundadas y ejercer un mayor control sobre su privacidad.

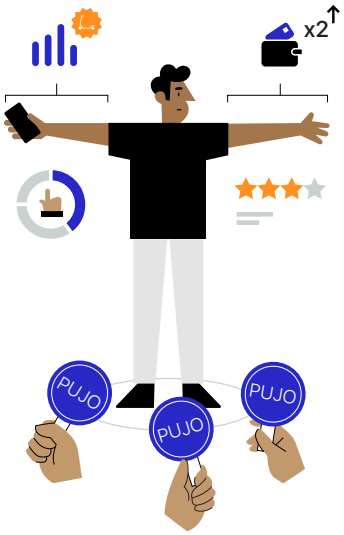
Muy pronto, nuestra nueva beta incluirá la transparencia en el seguimiento de las apps, que pedirá permiso a los usuarios antes de rastrear sus datos en apps y sitios web de otras empresas. Dentro de Ajustes, los usuarios podrán ver qué apps han solicitado permiso para rastrear sus datos y así poder hacer los cambios que quieran. Esta prestación se implantará de manera general a principios de primavera en la próxima actualización de iOS 14, iPadOS 14 y tvOS 14, y ya se ha ganado el apoyo de los defensores de la privacidad en todo el mundo. Con el diseño de esta prestación, Apple quiere dar a los usuarios más transparencia y control, y al mismo tiempo dejar que la publicidad siga siendo una forma adecuada y viable de apoyar las apps y el contenido web. Otras prestaciones anteriores, como el antirrastreo inteligente en Safari, han demostrado que la publicidad puede seguir funcionando bien sin poner en peligro la privacidad de los usuarios. Gracias a la transparencia en el seguimiento de las apps, los usuarios pueden elegir con un mayor nivel de información qué apps quieren usar y qué permisos les conceden. De esta forma, los usuarios pueden decidir si dejan que las apps los rastreen o no y, si se trata de apps en las que confían y a las que dan permiso, los desarrolladores podrán seguir haciéndolo.

Además de solicitar el permiso del usuario para el rastreo, Apple acaba de introducir cambios en las páginas de producto con el fin de ofrecer una mayor transparencia. Con la nueva sección Privacidad de la App, el App Store permite comprender mejor algunas de las prácticas de privacidad de las apps. Todas las páginas de producto deben ofrecer a los usuarios un resumen fácil de leer sobre las políticas de privacidad del desarrollador. En cada ficha, se incluye información sobre los tipos de datos que recopila la app, como fotos, ubicación e información de contacto. Aquí, los usuarios también pueden saber más sobre cómo usa el desarrollador de la app cada tipo de información, y si se usa con fines de rastreo o si se vincula con el usuario. Todos los desarrolladores de apps, incluido Apple, deben realizar un autoinforme sobre sus prácticas de privacidad.

Además de los ajustes de rastreo de las apps y de transparencia y privacidad, la información en las páginas de producto del App Store permite a los usuarios conocer más fácilmente cómo se usan sus datos personales. Así pueden hacerse una idea más clara de determinadas prácticas que solían ser confusas e inaccesibles, y tener un mayor control sobre sus datos.

Apple seguirá desarrollando tecnologías innovadoras de privacidad y trabajando para encontrar nuevas formas de garantizar la seguridad de la información personal de los usuarios.

Un día en la vida de un anuncio



Subastas de anuncios

Que Emma viera un anuncio de un patinete en la pantalla del dispositivo de Juan no fue casualidad. Los anunciantes pujan en una subasta para mostrar su anuncio en el dispositivo.[37] A continuación, ofrecemos una explicación simplificada de cómo, en una fracción de segundo, se eligió el anuncio que se mostró a Emma:

1.
El desarrollador de la app que está usando Emma contrata a una empresa de tecnología publicitaria que saca a subasta su espacio publicitario en tiempo real.[14]

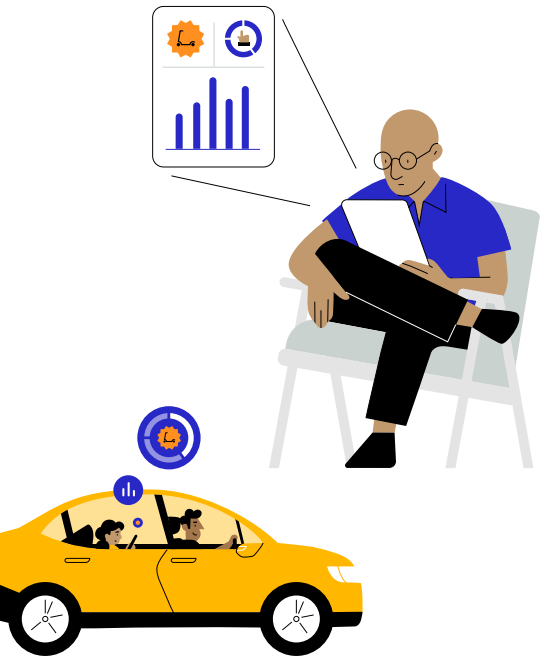
2.
Cuando Emma abre la app, la red de publicidad recopila datos a partir del uso del dispositivo de Juan (por ejemplo, qué app ha abierto Emma, dónde está y el identificador de publicidad de Juan), y también de otras empresas que se basan en ese identificador o en otro tipo de información que permite el rastreo.[3]

3.
La red de publicidad comparte algunos de estos datos, en concreto el identificador de publicidad, con posibles anunciantes. Antes de pujar, los anunciantes suelen tratar de saber todo lo posible sobre el usuario, a partir de sus propios datos y de los datos personales que han recopilado y reunido mediante el rastreo y la creación de perfiles.[3,15]

4.
Cuantas más características de Juan y de Emma (las que se obtuvieron a partir de sus datos) coincidan con el público objetivo del anunciante, más anunciantes pujarán por el espacio.[15,38]

5.
En la pantalla del dispositivo que está usando Emma aparece un anuncio del patinete que ha ganado la subasta.[14]

Como la subasta del anuncio tiene lugar en una fracción de segundo, los compradores y los vendedores recopilan, intercambian y usan datos personales para pujar por el espacio y mostrar los anuncios.[14,15]



Atribución de anuncios

Ahora que Emma ha visto el anuncio, lo que les interesa a las empresas de publicidad de la marca de patinetes es medir su efecto en su comportamiento. Este proceso recibe el nombre de atribución de anuncios.

Para ello, el anunciante intenta rastrear el comportamiento en el dispositivo que está usando Emma para recopilar información sobre lo que hace en internet, en las apps e incluso cuando no está conectada.

- **Si el anuncio era de un producto,** el anunciante podría tratar de rastrear si el usuario visitó su sitio web más tarde o una tienda física para comprarlo.[3]
- **Si el anuncio era de una app,** el anunciante podría tratar de rastrear si el usuario la instaló. Esto se llama atribución de la instalación de una app.[39]

Los anunciantes también usan la atribución de apps para «optimizar» sus campañas dirigiéndolas a grupos con los que sean más eficaces.[3]

Esto no tiene por qué ser así. Los anunciantes pueden medir el impacto que tienen sus campañas de publicidad en determinados grupos sin rastrear a los usuarios. Apple ha estado trabajando en herramientas que lo consiguen sin poner en peligro la privacidad del usuario:

SKAdNetwork permite a los anunciantes saber cuántas veces se ha instalado una app después de que se mostraran sus anuncios, así que se puede medir el impacto de una campaña en concreto. Sin embargo, esta información se ha diseñado para que no se comparta ningún dato de la persona ni del dispositivo, por lo que no se puede rastrear a los usuarios.

La medición de clics privada para las apps de iOS y iPadOS 14.5 permite a los anunciantes medir el impacto de los anuncios que llevan a los usuarios a un sitio web y limitar los datos que se recopilan mediante procesos que se ejecutan dentro del dispositivo. Cuando un usuario hace clic en el anuncio de un producto dentro de una app, el propio navegador web, mediante la medición de clics privada, puede informar al anunciante de que un usuario hizo clic en su anuncio y que eso generó una acción determinada en su sitio web, como una visita o una compra, pero sin recibir ninguna información específica sobre la persona.

Preguntas frecuentes

¿Podré seguir usando todas las funciones de la app si selecciono «Pedir a la app que no rastree»?

Sí. Los desarrolladores de apps no pueden pedirte que aceptes que te rastreen para poder usar la app al completo.

¿Qué son los identificadores y cómo se usan?

El identificador de publicidad (o IDFA, «Identifier For Advertisers»), otros identificadores y la dirección de correo electrónico pueden identificar un dispositivo concreto en una red. También permiten a los anunciantes crear un perfil detallado de la actividad del usuario en las distintas apps y sitios web cuando ven el identificador de su dispositivo y lo vinculan con su actividad.

¿Qué es el identificador de publicidad o IDFA?

El identificador de publicidad (IDFA, por sus siglas en inglés) es un identificador controlable por el usuario que iOS asigna a cada dispositivo. Se trata de un identificador basado en el software en vez de estar vinculado al hardware. Gracias a eso, el usuario puede bloquearlo para una app en concreto usando las opciones de transparencia en el seguimiento de las apps. Esto permite al usuario tener el control sobre el rastreo basado en el IDFA.

¿Puede Apple garantizar que una app no me va a rastrear si elijo la opción «Pedir a la app que no rastree»?

Si seleccionas «Pedir a la app que no rastree», el desarrollador no podrá acceder al identificador de publicidad (IDFA), que es el que suele usarse para rastrear, y tu decisión está por encima de ese identificador, por lo que el desarrollador de la app tiene que respetarla. Esta es una condición obligatoria en las políticas que los desarrolladores aceptan cuando presentan una app para su distribución en el App Store. Si descubrimos que un desarrollador está rastreando a usuarios que han pedido que no se los rastree, le pediremos que actualice sus prácticas para respetar su elección o, de lo contrario, podríamos eliminar su app del App Store.

Si uso mi cuenta de una red social para registrarme en una app, ¿puede esa red social rastrear lo que hago en la app?

Eso depende de si le das permiso para que te rastree o no. Si eliges «Pedir a la app que no rastree», la app no debería rastrear lo que haces en las apps o páginas web de otras empresas con fines publicitarios ni compartir tu información con un intermediario de datos. Esto significa que no debe facilitar tus datos a la empresa de redes sociales si se van a usar con ese fin.

¿Cómo se asegura Apple de que la información de privacidad de las páginas de producto del App Store es correcta?

Igual que ocurre con la clasificación por edades, los desarrolladores informan de sus prácticas de privacidad en el App Store. Si nos enteramos de que alguien ha facilitado información inexacta, nos ponemos en contacto con el desarrollador para que la corrija.

¿Qué es un intermediario de datos?

En general, un intermediario de datos es una empresa que se dedica a recopilar, vender, licenciar o ceder a terceros la información privada de personas con las que no tiene ninguna relación directa. Los intermediarios de datos son una figura recogida por la legislación de algunas regiones.

Referencias

1. Florian Gröne, Pierre Péladeau y otros: «Tomorrow's data heroes», *Strategy+Business*, 19 de febrero de 2019.

2. David Reinsel, John Gantz y otros: «The Digitization of the World: From Edge to Core», *IDC*, noviembre de 2018.

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

4. Paul Hitlin y Lee Raini: «Facebook Algorithms and Personal Data», *Pew Research Center*, 16 de enero de 2019.

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

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

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

8. Departamento de Justicia del Estado de California: «Data Broker Registry», oag.ca.gov/data-brokers.

9. Acxiom Corporation: Informe 10-K (2018) presentado el 25 de mayo de 2018, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.

10. Irwin Reyes, Primal Wijesekera y otros: «Won't Somebody Think of the Children? Examining COPPA Compliance at Scale», *Proceedings on Privacy Enhancing Technologies*, Vol. 2018, n.º 3, 2018, págs 63-83.

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

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

13. John Deighton y Leora Kornfeld: «The Socioeconomic Impact of Internet Tracking», *Interactive Advertising Bureau*, febrero de 2020.

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

15. Comisión Australiana de la Competencia y del Consumidor: «Digital advertising services inquiry - Interim report», diciembre de 2020.

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

17. Janelle Nanos: «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 de julio de 2018.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32. Edith Ramirez, Julie Brill y otros: «Data Brokers: A Call for Transparency and Accountability», *Federal Trade Commission*, mayo de 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. Alex Hern: «'Anonymous' browsing data can be easily exposed, researchers reveal», *The Guardian*, 1 de agosto de 2017.

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

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

37. Si la edad del usuario vinculado al ID de Apple registrado en un dispositivo es inferior a 18 años, el acceso al IDFA se desactiva por defecto y no se puede dar a ningún desarrollador.

38. Ayuda de Google Ads: «Acerca de Smart Bidding», support.google.com/google-ads/answer/7065882?hl=es.

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

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

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

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