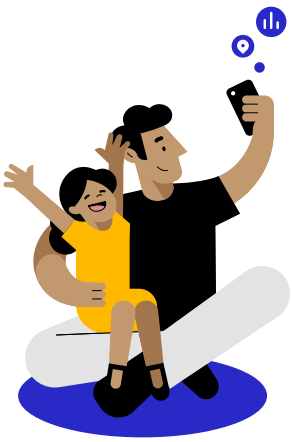


Un día en la vida de tus datos

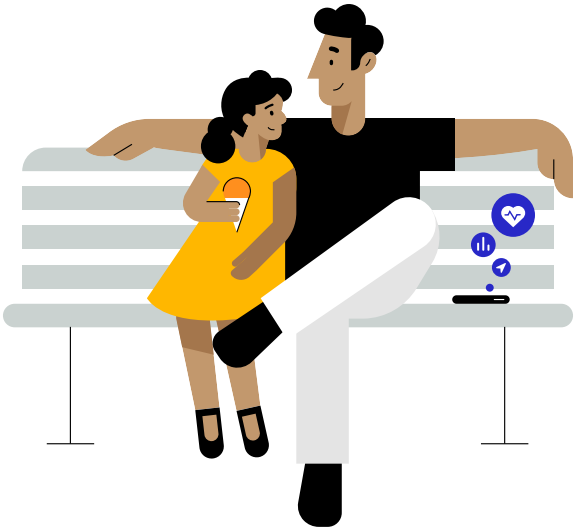
El día de un padre y su hija en el parque

Abril de 2021

“Creo que las personas son inteligentes, y algunas están dispuestas a compartir más datos que otras. Pregúntales. Pregúntales siempre. Haz que te pidan que dejes de hacerlo si se cansan de que les preguntes. Diles exactamente lo que vas a hacer con sus datos.”

Steve Jobs

Conferencia All Things Digital, 2010



En la última década, una industria gigantesca y no del todo transparente ha estado acumulando cantidades cada vez mayores de datos personales.[1,2] Un complejo ecosistema formado por sitios web, apps, empresas de redes sociales, revendedores de datos y empresas de tecnología publicitaria rastrean a los usuarios, incluso cuando no están en línea, y recopilan su información personal. Estos datos se juntan, se comparten, se agrupan y se subastan en tiempo real para alimentar una industria que genera 227,000 millones de dólares al año.[1] Esto sucede a diario en la vida de las personas, muchas veces sin su consentimiento o permiso.[3,4] Veamos lo que esta industria es capaz de aprender sobre un padre y su hija cuando deciden pasar un agradable día en el parque.

¿Sabías esto?

Las apps que usas todos los días tienen rastreadores integrados: una app promedio tiene 6.[3] La mayoría de las apps más populares de Android y iOS tienen rastreadores integrados.[5,6,7]

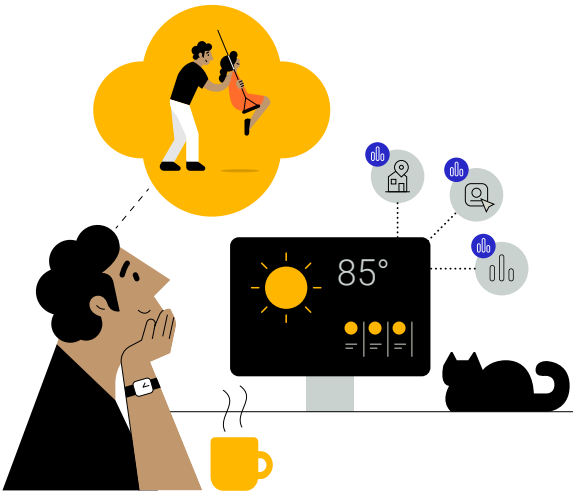
Los rastreadores generalmente están integrados en el código de terceros que ayuda a los desarrolladores a crear sus apps. Al incluir estos rastreadores, los desarrolladores permiten que los datos que compartes con ellos sean recopilados por terceros y vinculados a otros datos tuyos que ya se hayan recopilado.

Los revendedores de datos recopilan, venden, otorgan licencias o divulgan a terceros la información privada de personas con las que no tienen una relación directa.[3]

Cientos de revendedores de datos recolectan datos en línea y fuera de línea.[8] Un revendedor recopila datos de 700 millones de consumidores de todo el mundo y crea perfiles personales con hasta 5,000 características.[9]

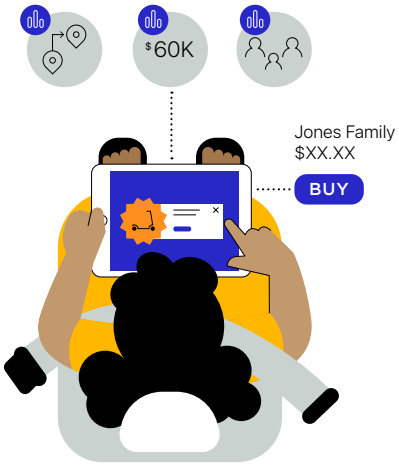
Un estudio reveló que en cerca del 20% de las apps para niños, los desarrolladores recopilaron y compartieron información de identificación personal sin el consentimiento verificable de los padres.[10]

Todos los días y a todas horas, los usuarios de Internet están expuestos a miles de millones de anuncios digitales.[11,12,13] En la milésima de segundo que tarda en cargar un anuncio, se lleva a cabo una subasta en tiempo real en la que los anunciantes pujan por el espacio publicitario. Para ello suelen basarse en los datos personales que el rastreador ha conseguido sobre ese usuario.[14,15]



Juan planea un paseo al parque con su hija

Juan y su hija de 7 años, Emma, van a pasar el día juntos. Temprano por la mañana, Juan usa su computadora para checar el pronóstico del tiempo y leer las noticias. En su smartphone, usa una app de mapas para ver cómo está el tráfico rumbo al parque que está cerca de la escuela de su hija. Durante el trayecto, hay cuatro apps en su teléfono recopilando y rastreando periódicamente sus datos de ubicación en segundo plano.[16,17,18] Los desarrolladores de apps venden los datos recopilados a revendedores de datos de terceros de los que Juan nunca ha oído hablar.[16,17] Aunque los datos de ubicación recopilados son supuestamente anónimos, el rastreo de usuario permite que los revendedores de datos asocien el historial de ubicación de Juan de esas apps con la información recopilada por otras apps que él ha estado usando.[16,19] Esto significa que cualquier empresa u organización puede comprar la información rastreada por diferentes apps y múltiples fuentes y usarla para crear un perfil completo de Juan, con todos los detalles de sus movimientos diarios.[3,16]



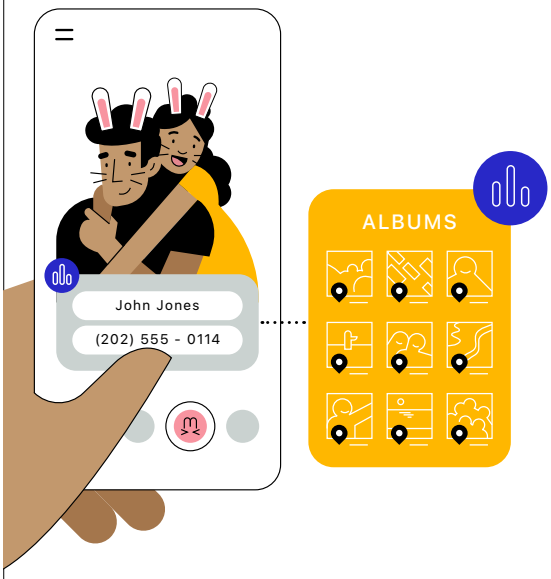
Emma se pone a jugar en la tablet de camino al parque

En el coche, Juan deja que su hija juegue en la tablet. Al abrir la app, le sale un anuncio de un scooter, y no es por casualidad. En la fracción de segundo que tardó en cargar la app, se llevó a cabo una subasta por el espacio publicitario.[14] Las empresas de publicidad que trabajan para el fabricante de scooters recibieron, a través de intermediarios, un aviso sobre la disponibilidad del espacio.[15] Con los datos personales que habían recopilado sobre Juan y Emma, pujaron por el anuncio.[15] Los socios publicitarios de la empresa de scooters continúan recopilando datos sobre el comportamiento de Juan y Emma después de haber visto el anuncio, para saber si hicieron clic en él o si compraron el scooter.[3] Y seguirán mostrando este anuncio de todas las formas que puedan, siguiéndolos por las distintas apps y sitios web que visiten en todos los dispositivos de Juan.[3,20,21]

Algunas apps solicitan acceso a más datos de los necesarios para brindar sus servicios, como una app de teclado que solicita acceso a la ubicación exacta del usuario.[5]

El intercambio de información puede llegar a redes de publicidad, anunciantes, proveedores de mediciones y atribuciones, revendedores de datos, otras empresas privadas e incluso entidades 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 información personal con fines distintos a los especificados a los usuarios en el momento de la recopilación de datos.[22,23,24,25]

Los revendedores de datos usan la información recopilada para asignar atributos a los usuarios y agruparlos en segmentos de mercado muy específicos. Por ejemplo, personas que "quieren bajar de peso pero aman los dulces".[26] El problema es que estos perfiles suelen estar equivocados: un estudio demostró que más del 40% de los atributos son inexactos.[27,28]

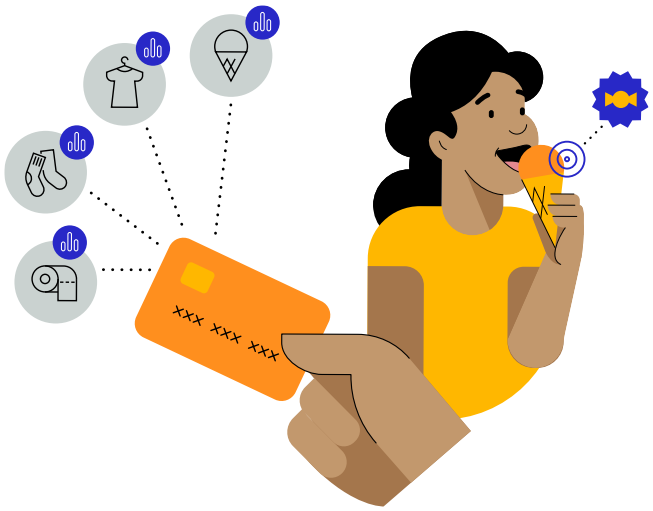


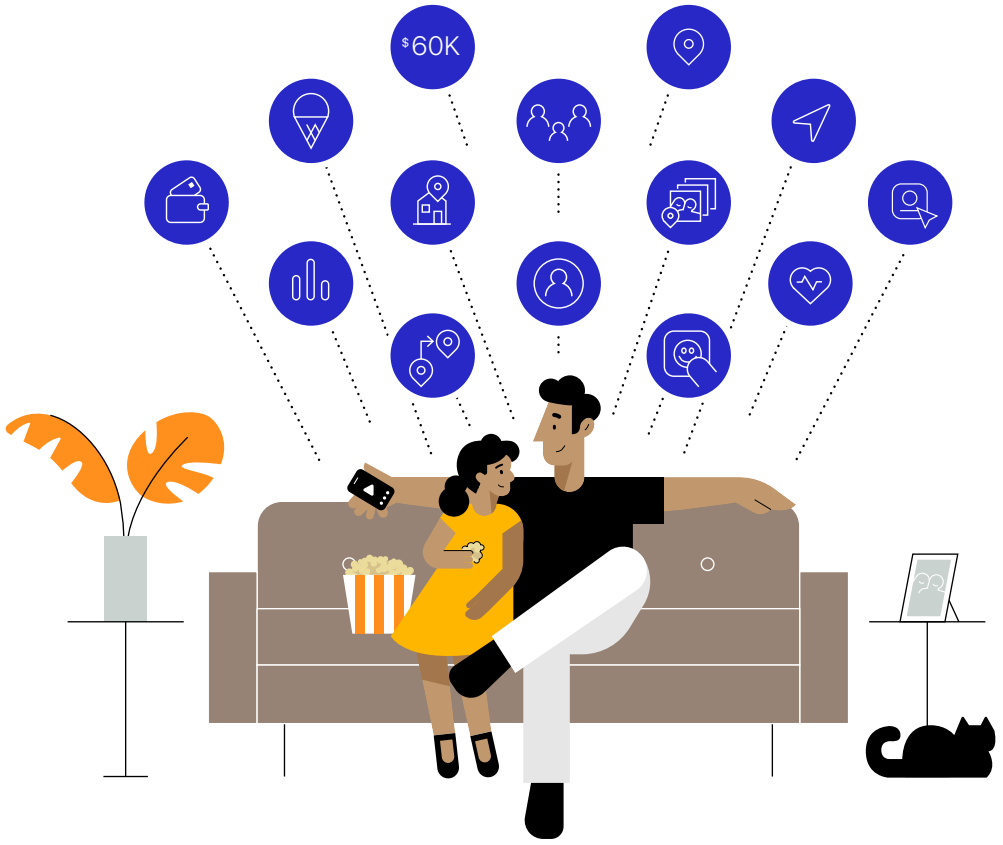
Juan y Emma se toman una selfie

Ya en el parque, Juan y Emma se toman una selfie. Se ponen a jugar con una app de filtros y terminan eligiendo uno de orejitas de conejo. La app de filtros puede acceder a todas las fotos del dispositivo y a los metadatos integrados, en lugar de acceder sólo a la selfie que se acaban de tomar.[29,30] Juan publica la imagen en una app de redes sociales. La app vincula la actividad en línea de Juan con un conjunto de datos recopilados por otras apps, como su información demográfica y hábitos de compra, por medio de una dirección de email, un número de teléfono o un identificador publicitario.

Una parada en la nevería

Antes de volver a casa, Juan y Emma van por un merecido helado. Juan usa su tarjeta de crédito para pagar. Con esto suma más información al perfil de datos de sus preferencias: la dirección de la tienda y cuánto gastó.[31,32,33] Una de las apps que rastrea la ubicación de Juan se da cuenta de que también pasaron por una juguetería.[3] La información de los lugares donde compraron durante el día se transfiere a los revendedores de datos, que ya saben que Juan tiene una niña pequeña y que por lo tanto pueden llenar sus dispositivos con anuncios específicos de dulces y de la tienda de juguetes a la que fueron.[17]





Al final del día, varias empresas de todo el mundo con las que Juan jamás ha interactuado actualizan sus perfiles con información de él y de su hija Emma. Estas empresas conocen la ubicación de su casa, el parque que visitaron, los sitios de noticias que leen, los productos que buscan, los anuncios que vieron, sus hábitos de compra y las tiendas a las que fueron.[3,34] Estos datos se recopilaron y rastrearon a través de las apps que Juan y su hija usaron durante el día, además de otras fuentes. Juan no estaba al tanto de que se estuvieran recopilando todos esos datos. No necesariamente tuvo control sobre ello y tampoco dio una autorización explícita para que eso pasara.[3,4] En la noche, mientras buscan una película para niños en una app de su smart TV antes de irse a dormir, el ciclo de rastreo, intercambio de datos, subastas y segmentación sigue su curso.[35,36]

Para obtener más información sobre las funcionalidades de privacidad introducidas por Apple y el trabajo que realiza para proteger la privacidad de los usuarios, visita apple.com/mx/privacy.

Para obtener más información sobre cómo Safari protege tu privacidad, lee el informe técnico sobre la privacidad en Safari.

Para obtener más información sobre cómo Apple protege tus datos de ubicación, lee el informe técnico sobre la privacidad de los servicios de localización.

Los principios de privacidad de Apple

En Apple creemos que la privacidad es un derecho humano fundamental. Por eso creamos nuestros productos y servicios sobre la base de cuatro principios de privacidad esenciales:

Recopilación mínima de datos

Recopilamos la cantidad mínima de datos necesarios para brindar un servicio determinado.

Procesamiento en el dispositivo

Siempre que sea posible, los datos se procesan en el dispositivo en lugar de enviarlos a los servidores de Apple, para proteger la privacidad del usuario y minimizar la recopilación de datos.

Transparencia y control del usuario

Nos aseguramos de que los usuarios sepan qué datos comparten y cómo se usan, y que tengan control sobre ellos.

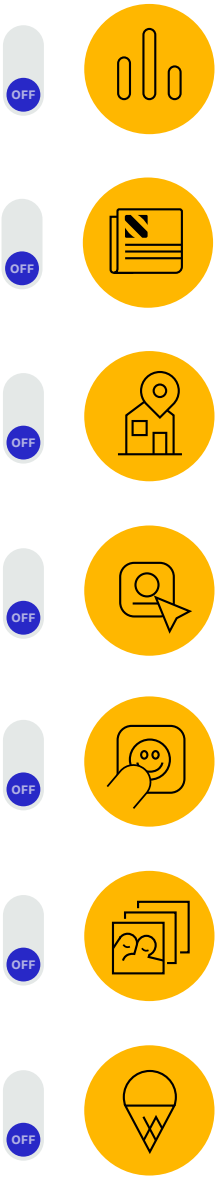
Seguridad

El hardware y el software trabajan en equipo para mantener los datos seguros.

Con estos cuatro principios, el objetivo de Apple siempre ha sido permitir que los usuarios compartan sus datos como prefieran, de una forma segura, que entiendan y que puedan controlar. Por esta razón, en las últimas dos décadas, Apple ha estado buscando nuevas formas de proteger la privacidad del usuario en todos los productos y servicios. Por ejemplo, usamos la tecnología inteligente del dispositivo y otras funcionalidades para minimizar los datos que recopilamos en nuestras apps, navegadores y servicios en línea. Y no generamos un perfil único de datos de usuario en ninguna de nuestras apps o servicios.

Las funcionalidades de privacidad de Apple le dan a Juan más transparencia y control sobre sus datos

La historia de Juan y Emma ilustra los problemas de privacidad y las soluciones que estamos desarrollando en Apple.



Juan planea un paseo al parque con su hija

Si Juan hubiera usado Safari para checar el pronóstico del tiempo en su computadora, el sistema de prevención de rastreo inteligente hubiera evitado que su actividad fuera rastreada de forma predeterminada.

Si Juan hubiera usado Apple News para leer las noticias por la mañana, Apple le hubiera mostrado contenido de acuerdo a sus intereses, sin registrar su identidad ni lo que lee.

Si Juan hubiera usado Mapas de Apple para ver cómo estaba el tráfico, sus datos de ubicación se hubieran asociado a un identificador aleatorio que se restablece con regularidad y no está vinculado a él. De esta manera, nadie más que Juan sabría su ubicación.

En un iPhone, Juan recibiría notificaciones periódicas sobre las apps que tienen acceso a su ubicación en segundo plano. Antes de compartir su ubicación con una app, Juan podría elegir si quiere compartir su ubicación aproximada o compartirla sólo una vez.

Emma se pone a jugar en la tablet de camino al parque

En un iPad, con la funcionalidad de transparencia del rastreo en apps, que estará disponible próximamente, Juan tendría la opción de permitir o no que el juego rastree la actividad de Emma en apps y sitios web de otras empresas.

Las redes de publicidad que usan la API SKAdNetwork de Apple habrían podido medir la eficacia general de los anuncios sin acceder a información que pudiera vincularse con el dispositivo de Juan.

Juan y Emma se toman una selfie en el parque

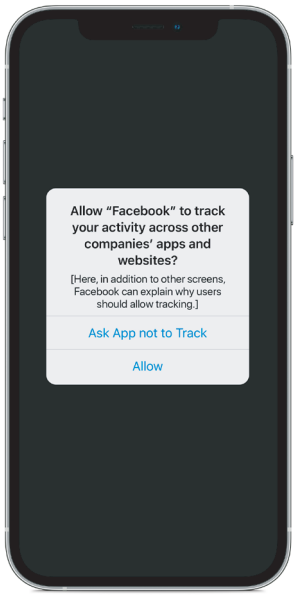
En un iPhone, Juan hubiera podido elegir que la app de filtros sólo tuviera acceso a la selfie y no a toda su biblioteca de fotos.

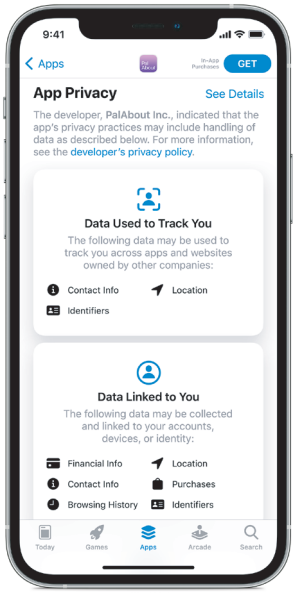
Una parada en la nevería antes de volver a casa

Si Juan hubiera pagado el helado con la Apple Card, su banco no hubiera usado la información de la transacción con fines de marketing. Y si hubiera usado Apple Pay, la tecnología inteligente en el dispositivo hubiera permitido a Juan ver su historial de transacciones en su iPhone sin que Apple tuviera acceso a la información sobre el lugar donde compró, qué compró o cuánto gastó.

En resumidas cuentas, los productos y las funcionalidades de privacidad de Apple le dan a Juan mayor transparencia y control sobre la cantidad de datos que se comparten y cómo se usan.

La transparencia del rastreo en apps y la nueva sección de información de privacidad en el App Store





Apple va un paso más allá para proteger la privacidad de los usuarios dentro del ecosistema de apps. Para hacerle frente a la compleja y creciente cantidad de entidades que acceden, rastrean y monetizan los datos personales de los consumidores, Apple presentará dos nuevas funcionalidades cuyo objetivo es brindar a los usuarios más transparencia, visibilidad y opciones. De esta forma podrán tomar decisiones informadas y ejercer un mayor control sobre su privacidad.

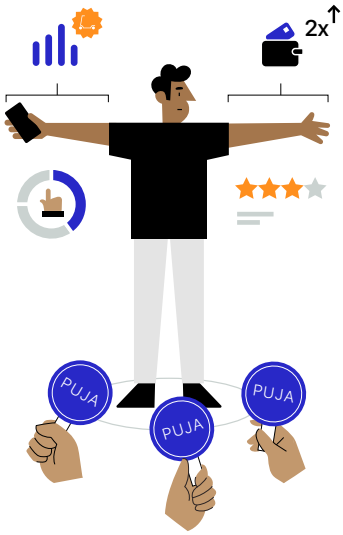
Muy pronto, con la próxima actualización beta, la funcionalidad de transparencia del rastreo en apps exigirá que las apps cuenten con el permiso del usuario antes de rastrear sus datos en apps o sitios web de otras empresas. En Configuración, los usuarios podrán ver las apps que han solicitado permiso para rastrear y podrán hacer los cambios que deseen. Este requisito se implementará próximamente con el lanzamiento de iOS 14, iPadOS 14 y tvOS 14, y ya cuenta con el apoyo de defensores de la privacidad de todo el mundo. Con esta funcionalidad, Apple busca dar a los usuarios más transparencia y control y, al mismo tiempo, continuar permitiendo la publicidad como un medio apropiado y viable para apoyar apps y contenido web. La introducción de funcionalidades anteriores, como la prevención de rastreo inteligente de Safari, ha demostrado que se puede proteger la privacidad de los usuarios y a la vez permitir que la publicidad sea eficaz. La funcionalidad de transparencia del rastreo en apps permite a los usuarios tomar decisiones más informadas sobre las apps que usan y los permisos que les otorgan. Además, ahora les da la opción de elegir si quieren que las apps los rastreen o no. Cuando los usuarios confían en ciertas apps y dan su permiso para que los rastreen, los desarrolladores pueden continuar haciéndolo.

Además de exigir el permiso del usuario para el rastreo, Apple también introdujo cambios recientes en las páginas de productos del App Store para aumentar la transparencia. Con la nueva sección Privacidad de Apps, el App Store ayuda a los usuarios a entender mejor algunas de las prácticas de privacidad de las apps. Cada página de producto debe proporcionar a los usuarios un resumen claro sobre las prácticas de privacidad de los desarrolladores. Estos resúmenes incluyen información sobre los tipos de datos que la app recopila, como fotos, ubicación e información de contacto. Los usuarios también obtienen detalles adicionales sobre cómo el desarrollador usa los distintos tipos de datos. Por ejemplo, si la información se usa para el rastreo o si los datos quedan o no vinculados al usuario. Todos los desarrolladores de apps, incluido Apple, están obligados a informar sobre sus prácticas de privacidad.

Gracias a la transparencia y los ajustes del rastreo en apps y a la información de privacidad en las páginas de productos del App Store, los usuarios podrán descubrir con mayor facilidad cómo se usa su información personal y tendrán más control sobre sus datos, ya que algunas prácticas que antes estaban ocultas o no muy claras saldrán a la luz.

Apple seguirá desarrollando tecnologías innovadoras para la protección de la privacidad y la información personal de cada usuario.

Un día en la vida de un anuncio



Subastas de anuncios

Que Emma viera un anuncio de un scooter en el dispositivo de Juan no fue casualidad. Los anunciantes pujan en una subasta para mostrar sus anuncios en el dispositivo.[37] A continuación, presentamos un ejemplo simplificado de cómo, en una fracción de segundo, se eligió qué anuncio se iba a mostrar en la pantalla del dispositivo:

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

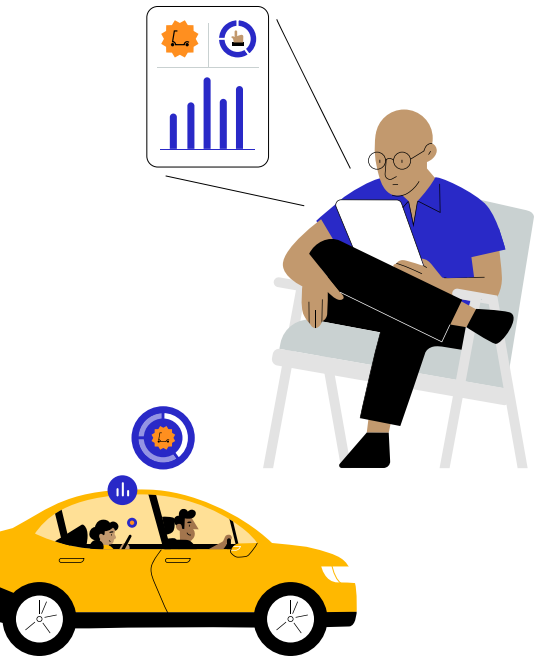
2.
Cuando Emma abre la app, la red de publicidad recopila datos a partir del uso del dispositivo de Juan (por ejemplo, qué app está usando Emma, su ubicación y el identificador de publicidad de Juan) y también de otras empresas que se basan en ese identificador o en otro tipo de información que permite 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 intentan aprender 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.
Entre más coincidencias existan entre el mercado objetivo del anunciante y las características que se hayan obtenido de Juan y Emma a partir de sus datos, más anunciantes pujarán por el espacio publicitario.[15,38]

5
En la pantalla del dispositivo que está usando Emma aparece el anuncio del scooter que haya ganado la subasta.[14]

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



Atribución de anuncios

Una vez que se ha mostrado el anuncio al usuario, las empresas de publicidad de la marca del scooter buscarán medir el impacto que tuvo el anuncio sobre el comportamiento de Emma. Este proceso se denomina atribución de anuncios.

- Para esto, el anunciante intenta rastrear el comportamiento en el dispositivo que Emma está usando para recopilar información de lo que hace online, en las apps e incluso cuando no está conectada.
- **Si el anuncio es de un producto,** el anunciante podría tratar de rastrear si el usuario finalmente visitó su sitio web o una tienda física para comprarlo.[3]
- **Si el anuncio es de una app,** el anunciante podría tratar de rastrear si el usuario la instaló. Esto se llama atribución de instalación de una app.[39]

Los anunciantes también usan la atribución de anuncios para "optimizar" sus campañas de publicidad y dirigirlas a grupos entre los cuales serán más efectivas.[3]

Nada de esto 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 hagan esto sin menoscabar la privacidad del usuario:

SKAdNetwork les permite a los anunciantes saber cuántas veces se ha instalado una app después de que se hayan mostrado sus anuncios, para así poder medir el impacto de una campaña de publicidad. Sin embargo, esta información está diseñada de modo que no se comparten datos personales ni de los dispositivos, por lo cual los anunciantes no pueden rastrear a los usuarios.

La medición de clics privada para las apps de iOS y iPadOS 14.5 les permite a los anunciantes medir el impacto de los anuncios que logran que los usuarios visiten un sitio web y limitar los datos que se recopilan mediante procesos que se ejecutan en el dispositivo. Cuando un usuario le da clic a un anuncio de un producto dentro de una app, los anunciantes pueden saber, gracias a la medición de clics privada, 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 revelar información específica sobre la persona.

Preguntas frecuentes

¿Puedo seguir usando todas las funciones de la app si selecciono “Solicitar a la app no rastrear”?

Sí. Los desarrolladores de apps no pueden exigirte que actives la opción de rastreo para poder usar todas las funciones de la app.

¿Qué son los identificadores y cómo se usan?

Identificadores como el identificador de publicidad (o IDFA, por sus siglas en inglés) y el correo electrónico pueden ayudar a identificar un dispositivo específico en una red. También les permiten a los anunciantes crear un perfil detallado de la actividad del usuario en las distintas apps y sitios web cuando detectan el identificador de su dispositivo y lo vinculan con su actividad.

¿Que 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. Como es un identificador basado en el software en vez de estar vinculado al hardware, el usuario puede bloquearlo para apps específicas mediante la funcionalidad de transparencia del rastreo en apps. Esto le permite al usuario tener el control del rastreo basado en el IDFA.

¿Apple puede garantizar que una app no me está rastreando si selecciono “Solicitar a la app no rastrear”?

Al seleccionar “Solicitar a la app no rastrear”, el desarrollador no podrá acceder al identificador de publicidad (IDFA), que generalmente se usa para rastrear. El desarrollador de la app también está obligado a respetar tu decisión sobre el identificador de publicidad. Esto está incluido en las políticas que el desarrollador acepta al enviar una app para su distribución en el App Store. Si descubrimos que un desarrollador está rastreando usuarios sin haber sido autorizado, exigiremos que actualice sus prácticas para respetar la decisión del usuario. De lo contrario, la app podría ser retirada del App Store.

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

Eso depende de si le has dado permiso a la app para que te rastree. Si seleccionas “Solicitar a la app no rastrear”, la app no debería permitir que otras apps o sitios web de terceros te rastreen con fines publicitarios, ni compartan tu información con revendedores de datos.
Esto significa que no deberían darle tu información a la empresa de la red social si se va a usar para ese fin.

¿Cómo garantiza Apple que la información de privacidad de las páginas de productos en el App Store es correcta?

De la misma manera que lo hace con la clasificación por edad en el App Store. Los desarrolladores informan sobre sus propias prácticas de privacidad y si descubrimos que la información proporcionada es incorrecta, trabajaremos con ellos para garantizar su exactitud.

¿Qué es un revendedor de datos?

Es una empresa que recopila, vende, licencia o divulga a terceros la información personal de usuarios finales particulares que no tienen una relación directa con la empresa en sí.
En algunos lugares, la figura del revendedor de datos está contemplada en la ley.

Referencias

1. Gröne, Florian, Pierre Péladeau, et al. "Tomorrow's data heroes", *Strategy+Business*, 19 de febrero de 2019.

2. Reinsel, David, John Gantz, et al. "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. Hitlin, Paul y Lee Rainie. "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. 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. Departamento de Justicia del estado de California. "Data Broker Registry", oag.ca.gov/data-brokers.

9. Acxiom Corporation. 2018 Form 10-K, archivada el 25 de mayo de 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, n.º 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 de noviembre de 2012.

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

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

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

15. Australian Competition and Consumer Commission. "Digital advertising services inquiry - Interim report", diciembre de 2020.

16. Edelman, Gilad. "Can Killing Cookies Save Journalism?", *WIRED*, 5 de agosto de 2020.

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

18. 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 de julio de 2018.

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

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

21. O'Reilly, Lara. "New Facebook Tools Help Marketers Serve Ads to People Most Likely to Spend Money", *The Wall Street Journal*, 12 de junio de 2017.

22. Ramirez, Edith, Julie Brill, et al. "Data Brokers: A Call for Transparency and Accountability", *Comisión Federal de Comercio*, mayo de 2014.

23. Facebook for Business. "Measuring Conversions on Facebook, Across Devices and in Mobile Apps", 14 de agosto de 2014.

24. Bender, Brad. "New digital innovations to close the loop for advertisers", *Google Ads & Commerce Blog*, 26 de septiembre de 2016.

25. Comisión Federal de Comercio. "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook", 24 de julio de 2019.

26. Chin, Kimberly. "Twitter Could Pay FTC Fine Over Alleged Privacy Violations", *The Wall Street Journal*, 3 de agosto de 2020.

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

28. Schiffer, Zoe. "Period tracking app settles charges it lied to users about privacy", *The Verge*, 13 de enero de 2021.

29. Thompson, Stuart A. "These Ads Think They Know You", *The New York Times*, 30 de abril de 2019.

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

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

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

33. Germain, Thomas. "How a Photo's Hidden 'Exif' Data Exposes Your Personal Information", *Consumer Reports*, 16 de diciembre de 2019.

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

35. 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.

36. Hern, Alex. "'Anonymous' browsing data can be easily exposed, researchers reveal", *The Guardian*, 1 de agosto de 2017.

37. Si la edad del usuario asociado al Apple ID registrado en un dispositivo es inferior a 18 años, el acceso al IDFA se desactiva de forma predeterminada y no se le puede otorgar a ningún desarrollador.

38. Google Ads Help. "About Smart Bidding", support.google.com/google-ads/answer/7065882?hl=en.

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

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

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

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