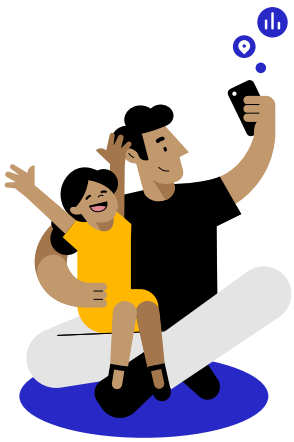


Un giorno nella vita dei tuoi dati

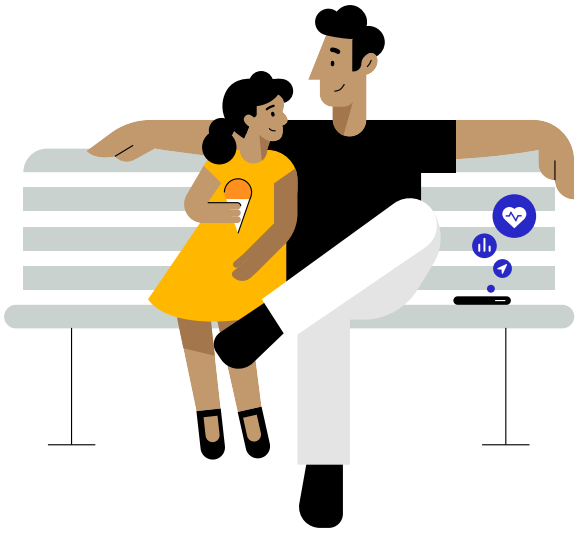
Una giornata al parco giochi tra padre e figlia

Aprile 2021

“Penso che le persone siano intelligenti e che alcune vogliano condividere più dati di altre. Quindi chiedi. Chiediglielo ogni volta. Fino a quando non ti diranno di smetterla perché si sono stancate di sentirselo chiedere. Spiega con precisione alle persone cosa farai con i loro dati.”

Steve Jobs

All Things Digital Conference, 2010



C’è un intero settore dell’economia, opaco e ramificato, che negli ultimi dieci anni ha accumulato una quantità crescente di dati personali.[1,2] Un complesso ecosistema di siti web, app, social media, rivenditori di dati e aziende di tecnologie pubblicitarie tiene traccia di quello che le persone fanno online e offline, raccogliendo i loro dati personali. Queste informazioni vengono aggregate, condivise e utilizzate in tempo reale per le aste pubblicitarie, alimentando un’industria da 227 miliardi di dollari l’anno.[1] Succede tutti i giorni, mentre le persone vivono la loro vita senza sapere nulla di cosa succede ai propri dati e senza aver mai espresso il proprio consenso.[3,4] Vediamo tutto quello che queste aziende sono in grado di scoprire su un padre e una figlia che trascorrono una normale giornata al parco.

Lo sapevi?

I tracker sono integrati nelle app che usi ogni giorno: in media, ognuna ne contiene sei,[3] e si trovano nella stragrande maggioranza delle app più usate per Android e iOS.[5,6,7]

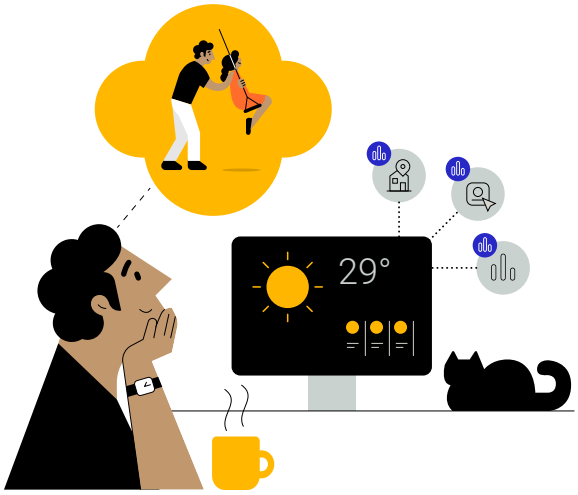
Spesso i tracker sono incorporati in codice di terzi che agevola lo sviluppo di app. Includendo i tracker, chi sviluppa le app permette anche a terzi di raccogliere e collegare i dati che hai condiviso con loro nelle varie app e di combinarli con altre informazioni raccolte su di te.

I rivenditori di dati raccolgono e vendono, cedono o divulgano a terzi informazioni personali di utenti individuali con cui non hanno alcun rapporto diretto.[3]

Centinaia di rivenditori di dati raccolgono informazioni online e offline.[8] Un solo rivenditore raccoglie dati su 700 milioni di utenti in tutto il mondo, creando profili che includono fino a 5000 caratteristiche.[9]

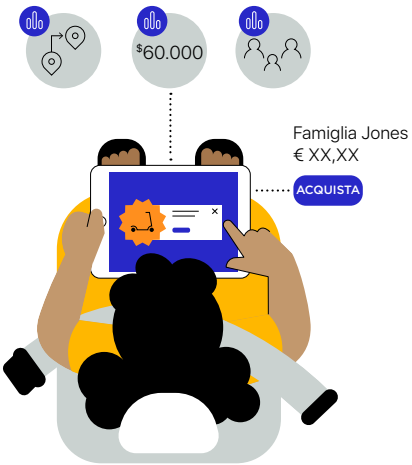
Uno studio ha rilevato che quasi il 20% delle app per bambini analizzate raccoglieva e condivideva informazioni personali identificabili senza il consenso verificabile dei genitori.[10]

Miliardi di annunci pubblicitari digitali vengono mostrati agli utenti online a ogni ora del giorno.[11,12,13] Nei millisecondi che servono per caricare un annuncio si svolge un'asta in tempo reale in cui gli inserzionisti si contendono lo spazio pubblicitario, spesso basandosi sui dati personali raccolti su ogni individuo.[14,15]



John vuole passare una giornata al parco con la figlia

John e la figlia di sette anni, Emma, trascorreranno la giornata insieme. Al mattino, John usa il computer per controllare il meteo e leggere le notizie, e apre un'app di mappe sullo smartphone per dare un'occhiata al traffico previsto nel tragitto verso il parco giochi vicino alla scuola della bambina. Una volta in auto, quattro app sul suo telefono raccolgono e tracciano periodicamente i dati sulla posizione in background.[16,17,18] Chi ha sviluppato le app estrae queste informazioni dal dispositivo e le vende a una serie imprecisata di rivenditori di dati di cui John non ha mai sentito parlare.[16,17] I dati di localizzazione sono formalmente anonimi, ma il tracciamento utente permette ai rivenditori di dati di associare la cronologia della posizione di John in queste app alle informazioni raccolte dalle altre app che ha usato.[16,19] In pratica, ora le informazioni raccolte da app e fonti diverse sono a disposizione di chiunque le voglia acquistare, e potrebbero essere usate dalle aziende per creare un profilo completo di John con tutti i dettagli sui suoi spostamenti quotidiani.[3,16]



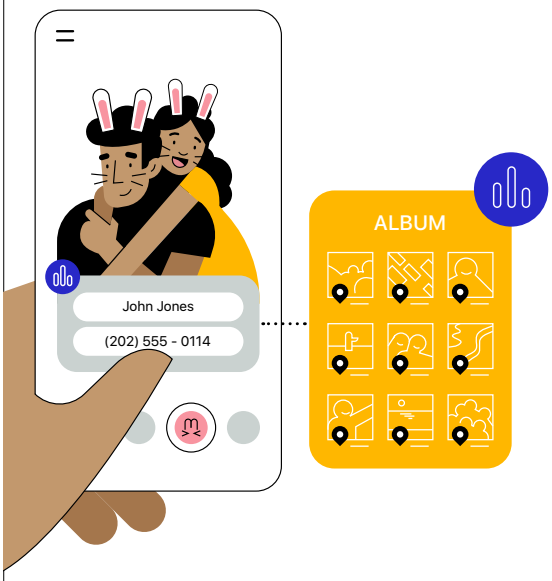
Emma gioca sul tablet mentre vanno al parco

Nel tragitto verso il parco, John lascia che la figlia usi il tablet per giocare. Appena Emma apre un gioco, vede la pubblicità di un monopattino. Questo non è un caso: nei millisecondi in cui si è caricata l'app, c'è stata un'asta per quello spazio pubblicitario.[14] Tramite intermediari, le agenzie pubblicitarie che lavorano per conto dell'azienda di monopattini hanno saputo dello spazio disponibile.[15] Quindi, usando i dati personali raccolti su John e Emma, hanno fatto un'offerta per aggiudicarselo.[15] I partner pubblicitari dell'azienda di monopattini continuano a raccogliere informazioni sul comportamento di John e Emma dopo la visualizzazione dell'annuncio, per determinare se l'hanno cliccato o se hanno acquistato il monopattino.[3] E continueranno a pubblicizzare quel prodotto a John e Emma in ogni modo possibile, seguendo le loro tracce mentre usano app e siti web su tutti i dispositivi di John.[3,20,21]

Alcune app chiedono di accedere a più dati di quanti ne servano per fornire il servizio, per esempio quando un'app per tastiera vuole usare la tua posizione.[5]

Lo scambio di informazioni può finire a reti pubblicitarie, inserzionisti, fornitori di servizi di attribuzione e misurazione, rivenditori di dati, altre aziende private e persino istituzioni pubbliche.[3,15,40,41,42] Aziende di tecnologie pubblicitarie e social media si trovano a dover pagare, o hanno già pagato, multe di milioni di dollari per l'uso di dati personali con finalità diverse da quelle descritte all'utente al momento della raccolta.[22,23,24,25]

I rivenditori di dati usano le informazioni raccolte per assegnare attributi agli utenti e inquadrarli in segmenti di mercato iperdettagliati, per esempio persone che "stanno provando a perdere peso ma amano le pasticcerie".[26] Questi profili, tuttavia, sono spesso sbagliati: secondo uno studio, oltre il 40% degli attributi è impreciso.[27,28]

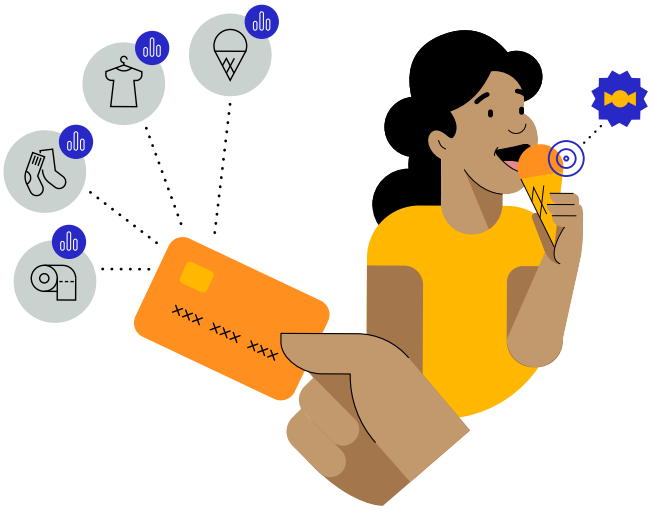


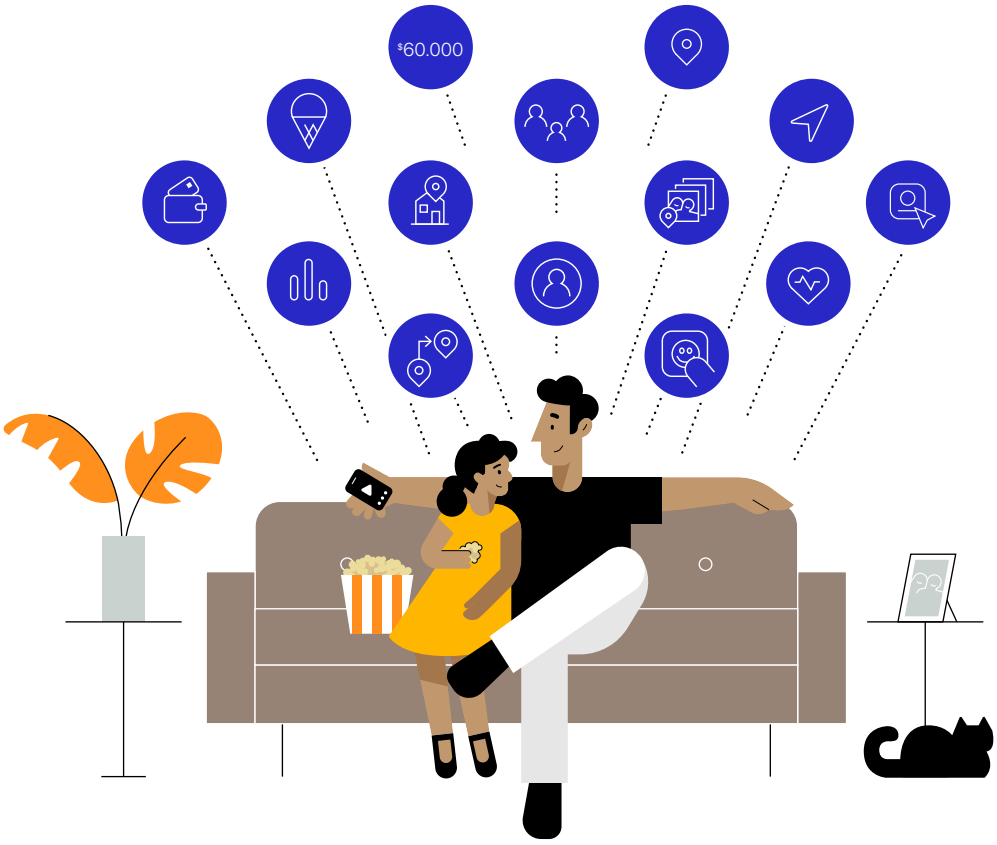
John e Emma si fanno un selfie al parco

Più tardi, mentre sono al parco, John e Emma si fanno un selfie. Provano un'app di filtri e aggiungono delle orecchie da coniglio alla foto. L'app di filtri, però, oltre a quel selfie è in grado di accedere anche a tutte le foto sul dispositivo e ai metadati associati.[29,30] Poi, John pubblica la foto nell'app di un social network. L'app collega l'attività online di John a una miriade di dati raccolti da altre app, come informazioni demografiche e sulle sue abitudini di acquisto, utilizzando un indirizzo email, un numero di telefono o un identificatore pubblicitario.[3]

Un salto in gelateria prima di rientrare

Mentre tornano a casa, John e Emma si fermano a prendere un gelato. John paga con la carta di credito, e al profilo delle sue preferenze si aggiungono altre informazioni: l'indirizzo della gelateria e quanto ha speso.[31,32,33] Una delle app che registra la posizione di John è in grado di rilevare che lui e Emma hanno anche fatto tappa in un negozio di giocattoli.[3] Le informazioni sui posti in cui hanno fatto acquisti durante la giornata vengono trasmesse ai rivenditori di dati, che li combinano con quello che già sanno di John (il fatto che ha una bambina) per tempestare il suo dispositivo di pubblicità personalizzate di dolci e caramelle e annunci del negozio di giocattoli appena visitato.[17]





Alla fine della giornata, svariate aziende di tutto il mondo, con cui John non ha mai interagito, hanno aggiornato i loro profili con informazioni su di lui e su sua figlia. Queste aziende sanno dove i due abitano e che parco frequentano, e sanno anche quali siti di informazione hanno letto, che prodotti hanno cercato, che pubblicità hanno guardato, quali sono le loro abitudini di acquisto e i negozi che hanno visitato.[3,34] Questi dati sono stati raccolti e tracciati dalle diverse app che John e la figlia hanno usato durante la giornata, nonché da altre fonti. Tutto questo senza che John sapesse quanti dati venivano raccolti, senza che avesse il pieno controllo sulla loro condivisione, e senza che potesse dare o negare consapevolmente il suo consenso.[3,4] E mentre John e Emma usano un'app sulla smart TV per cercare un film da guardare in serata, il ciclo di tracciamento, scambio di dati, aste e retargeting continua senza sosta.[35,36]

Per saperne di più sulle funzioni Apple per la privacy e su quello che facciamo per proteggere le informazioni di ogni utente, vai su **apple.com/it/privacy.**

Per sapere come Safari protegge la tua privacy, leggi il **documento ufficiale su Safari.**

Per sapere come Apple protegge i dati sulla tua posizione, leggi il **documento ufficiale sui servizi di localizzazione.**

I principi di Apple sulla privacy

Per Apple, la privacy è un diritto fondamentale di ogni persona. Progettiamo i nostri prodotti e servizi sulla base di quattro principi:

Minima condivisione dei dati

Raccogliamo solo la quantità minima di dati necessaria per offrirti il servizio di cui hai bisogno.

Elaborazione on-device

Ogni volta che è possibile, elaboriamo i dati sul dispositivo invece di inviarli ai server Apple; questo per proteggere la privacy dell'utente e limitare al minimo la raccolta dei dati.

Trasparenza e controllo per l'utente

Ci assicuriamo che ogni utente sappia quali dati vengono condivisi, come vengono usati e come può controllarli.

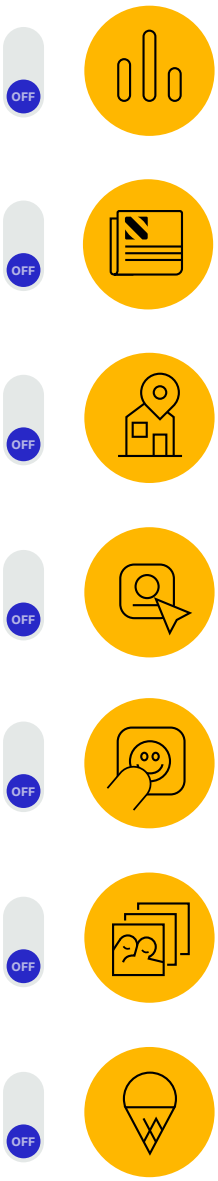
Sicurezza

Hardware e software lavorano insieme per tenere i dati al sicuro.

Con questi quattro principi, l'obiettivo di Apple è da sempre quello di consentire all'utente di condividere i dati come preferisce, con la massima sicurezza e in modo comprensibile e controllabile. Ecco perché negli ultimi vent'anni abbiamo continuato a introdurre innovazioni per proteggere la privacy di ogni utente su tutti i nostri prodotti e servizi. Per esempio, utilizziamo l'intelligenza on-device e altre funzioni per ridurre al minimo i dati raccolti nelle nostre app, nei nostri browser e nei servizi online, e nell'ecosistema delle app e dei servizi che offriamo non creiamo mai un singolo profilo utente che aggrega tutti i dati di una persona.

Le funzioni Apple per la privacy offrono a John più trasparenza e controllo sui suoi dati

Il racconto della giornata di John e Emma illustra bene i problemi di privacy con cui dobbiamo confrontarci e le soluzioni a cui Apple sta lavorando.



John vuole passare una giornata al parco con la figlia

Se John avesse usato Safari per controllare il meteo sul computer, l'antitracking intelligente attivo di default avrebbe impedito automaticamente il tracciamento della sua attività.

Se avesse usato Apple News per leggere le notizie al mattino, Apple avrebbe mostrato a John contenuti basati sui suoi interessi, ma senza raccogliere informazioni su chi è o cosa legge.

Se avesse usato Mappe di Apple per controllare il traffico, i dati di localizzazione sarebbero stati associati a un identificatore casuale, reimpostato periodicamente e non riconducibile a John. Di conseguenza, nessuno avrebbe potuto conoscere la sua posizione.

Inoltre, un iPhone ricorderebbe periodicamente a John quali app accedono alla sua posizione in background. Prima di permettere a un'app di rilevare dove si trova, John potrebbe scegliere di mostrare solo una posizione approssimativa, o di condividerla soltanto una volta.

Emma gioca sul tablet mentre vanno al parco

Su un iPad, John potrebbe usare le impostazioni sul tracciamento da parte delle app (disponibili prossimamente) per scegliere se consentire al gioco di tracciare l'attività di Emma nelle app e nei siti web di altre aziende.

Le reti pubblicitarie che usano l'API SKAdNetwork di Apple sono comunque in grado di misurare l'efficacia complessiva degli annunci senza accedere a informazioni che potrebbero essere ricollegate al dispositivo di John.

John e Emma si fanno un selfie al parco

Su un iPhone, John avrebbe potuto autorizzare l'app ad accedere solo a quel selfie invece che all'intera libreria di foto.

Una sosta in gelateria prima di rientrare

Se John avesse pagato il gelato con una Apple Card, la sua banca non avrebbe potuto usare i dati sulla transazione a scopi di marketing. E se avesse usato Apple Pay, l'intelligenza on-device avrebbe permesso a John di visualizzare la cronologia dei suoi pagamenti sull'iPhone senza fornire a Apple informazioni su dove ha fatto acquisti, cosa ha comprato o quanto ha speso.

A conti fatti, i prodotti e le funzioni Apple per la privacy possono dare a John più trasparenza e controllo sui dati che vengono condivisi nell'arco della giornata e su come vengono utilizzati.

Trasparenza nel tracciamento da parte delle app e nuove informazioni sulla privacy nell'App Store

Apple sta compiendo un ulteriore passo per proteggere la privacy dell'utente all'interno dell'ecosistema di app. Visto il numero crescente di soggetti di vario tipo che accedono ai dati personali di consumatori e consumatrici e li controllano a scopo di lucro, stiamo introducendo due nuove funzioni che daranno all'utente più trasparenza, visibilità e possibilità di scelta; chi usa i nostri prodotti potrà decidere in modo più consapevole e avere un maggiore controllo sulla propria privacy.

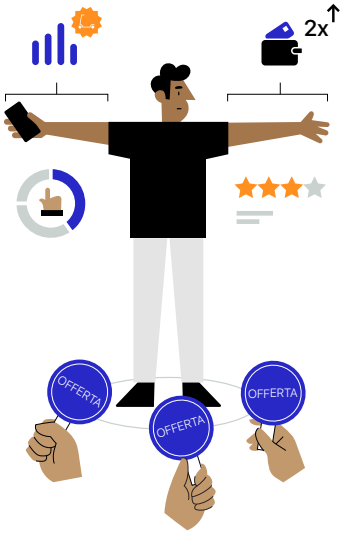
A breve metteremo a disposizione un aggiornamento beta con una nuova funzione per la trasparenza nel tracciamento: le app saranno obbligate a ottenere il consenso dell'utente prima di tracciare i suoi dati nelle app e nei siti web di altre aziende. In Impostazioni, sarà possibile vedere quali app hanno richiesto il consenso e modificare le proprie scelte. Si tratta di un'innovazione già approvata da molte organizzazioni che si occupano di privacy e che sarà implementata su larga scala in primavera con la prossima release di iOS 14, iPadOS 14 e tvOS 14. Nel progettare questa funzione, Apple ha cercato di offrire all'utente più trasparenza e controllo pur continuando a permettere gli annunci commerciali, che ritiene un modo adeguato per sostenere app e contenuti web. In passato l'introduzione di funzioni come il sistema antitracking intelligente di Safari ha dimostrato che si può fare pubblicità in modo efficace anche mantenendo intatta la privacy di consumatori e consumatrici. La funzione per la trasparenza nel tracciamento da parte delle app permette all'utente di scegliere con più consapevolezza quali app utilizzare e quali permessi concedere. Sarà l'utente a decidere se autorizzare o meno il tracking: se si fida e dà il suo consenso, chi ha sviluppato l'app potrà continuare a tracciare le sue attività.

Oltre a richiedere il consenso per il tracciamento, di recente Apple ha anche introdotto alcuni cambiamenti alle descrizioni delle app sull'App Store per aumentarne la trasparenza. Ora l'utente può capire meglio come le app trattano i suoi dati consultando la nuova sezione "Privacy dell'app", una scheda presente in tutte le descrizioni dove gli sviluppatori spiegano, in modo semplice e chiaro, come affrontano la questione della privacy. Sono incluse informazioni sui tipi di dati raccolti dall'app, come foto, posizione e informazioni di contatto, nonché dettagli sull'uso dei vari tipi di dati, per esempio se verranno utilizzati per il tracciamento e se sono riconducibili all'utente. Le informazioni sulla privacy sono richieste a chiunque pubblichi un'app, Apple inclusa.

Le impostazioni per il tracciamento da parte delle app e le informazioni sulla privacy nelle descrizioni delle app sull'App Store fanno luce su pratiche che prima erano poco chiare o sotterranee; in questo modo chi usa i dispositivi Apple può capire meglio come vengono usati i suoi dati personali e può controllarli più facilmente.

Apple continuerà a sviluppare tecnologie innovative per la privacy e a cercare nuovi modi per tenere al sicuro le tue informazioni personali.

Un giorno nella vita di una pubblicità



Aste pubblicitarie

Il fatto che Emma abbia visto la pubblicità di un monopattino sullo schermo di John non è casuale: gli inserzionisti hanno partecipato a un'asta per mostrare i loro annunci sul dispositivo.[37] Ecco una spiegazione semplificata di come, in una frazione di secondo, sia stata scelta proprio quella pubblicità.

1.
Chi ha sviluppato l'app usata da Emma assume una società di tecnologie pubblicitarie che mette all'asta il suo spazio di inserzione in tempo reale.[14]

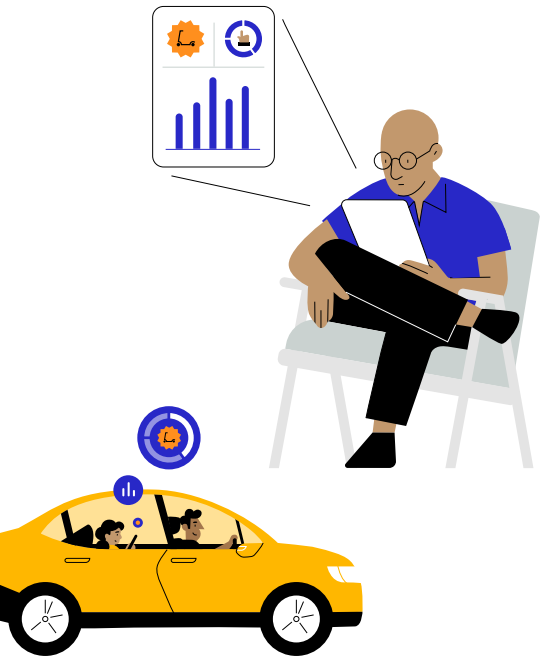
2.
Quando Emma apre l'app, la rete pubblicitaria raccoglie i dati dal dispositivo di John (per esempio quale app sta usando, dove si trova e l'ID pubblicitario di John) e da terzi, basandosi sull'ID pubblicitario di John o su altre informazioni che consentono il tracciamento.[3]

3.
La rete pubblicitaria condivide alcune di queste informazioni, in particolare l'ID pubblicitario, con potenziali inserzionisti. Prima di fare un'offerta, in genere l'inserzionista cerca di scoprire il più possibile sull'utente, sfruttando le informazioni in suo possesso e i dati personali raccolti e aggregati tramite il tracciamento e la profilazione.[3,15]

4.
Più le caratteristiche di John e Emma (ricavate dai loro dati) sono in linea con il pubblico target degli inserzionisti, più alte saranno le offerte per lo spazio pubblicitario.[15,38]

5.
La pubblicità del monopattino si aggiudica l'asta e viene mostrata sul dispositivo usato da Emma.[14]

L'asta pubblicitaria dura una frazione di secondo, mentre tutte le parti coinvolte raccolgono, scambiano e utilizzano i dati personali per cercare di aggiudicarsi gli spazi disponibili e mostrare gli annunci.[14,15]



Attribuzione della pubblicità

Dopo che l'annuncio viene mostrato a Emma, le agenzie pubblicitarie che lavorano per l'azienda di monopattini vogliono misurarne l'effetto sul suo comportamento. Questo processo si chiama "attribuzione della pubblicità".

Per farlo, l'inserzionista prova a tracciare il comportamento sul dispositivo usato da Emma per raccogliere informazioni su quello che fa sul web, nelle app e persino offline.

- **Se l'annuncio pubblicizza un prodotto,** l'inserzionista potrebbe provare a capire se in seguito l'utente ha visitato il sito web o un negozio fisico per acquistarlo.[3]
- **Se l'annuncio pubblicizza un'app,** l'inserzionista potrebbe provare a capire se l'utente l'ha installata. Questa procedura è detta "attribuzione dell'installazione di app".[39]

Con l'attribuzione della pubblicità, l'inserzionista può "ottimizzare" la sua campagna per i gruppi verso cui risulta più efficace.[3]

Ma non deve per forza andare così. L'inserzionista può misurare l'efficacia delle campagne pubblicitarie senza tracciare l'attività dell'utente. E Apple sta lavorando a strumenti capaci di farlo nel pieno rispetto della privacy.

Con **SKAdNetwork**, l'inserzionista può sapere quante volte un'app è stata installata dopo la visualizzazione delle sue pubblicità, per misurare l'efficacia della campagna. Ma questa informazione viene fornita senza condividere alcun dato sull'utente o sul dispositivo, e perciò senza possibilità di tracciamento.

Private Click Measurement, una funzione disponibile per le app su iOS e iPadOS 14.5, permette all'inserzionista di misurare l'efficacia delle pubblicità che portano l'utente su un sito web riducendo al minimo la raccolta dei dati grazie all'elaborazione on-device. Quando l'utente clicca sulla pubblicità di un prodotto dentro un'app, grazie a Private Click Measurement il browser stesso può far sapere all'inserzionista che c'è stato un clic e che questo ha portato a un determinato risultato sul suo sito web, come una visita o un acquisto, senza fornire informazioni specifiche sulla persona che ha cliccato sull'annuncio.

Domande frequenti

Potrò comunque usare appieno tutte le funzioni dell'app se seleziono "Chiedi all'app di non eseguire il tracciamento"?

Sì. Chi ha sviluppato l'app non può importi di accettare il tracciamento per usare tutte le funzioni.

Cosa sono gli identificatori e come vengono usati?

Gli identificatori, come l'Identifier For Advertisers (IDFA) e l'indirizzo email, aiutano a identificare un dispositivo specifico su una rete. Inoltre consentono agli inserzionisti di creare un profilo dettagliato della tua attività su diversi siti web e app quando rilevano l'identificatore del tuo dispositivo e lo associano alla tua attività.

Cos'è l'IDFA (Identifier For Advertisers)?

L'IDFA è un identificatore controllabile dall'utente assegnato da iOS a ciascun dispositivo. È di tipo software e non legato all'hardware, perciò l'utente può bloccarlo per una specifica app quando compare il messaggio con le opzioni per il tracciamento trasparente da parte delle app. In questo modo, l'utente mantiene il controllo del tracking basato sull'IDFA.

Apple può garantirmi che un'app non tracci le mie attività se seleziono "Chiedi all'app di non eseguire il tracciamento"?

Se selezioni "Chiedi all'app di non eseguire il tracciamento", l'app non potrà accedere all'IDFA (Identifier For Advertisers), che viene spesso usato per il tracking. Chi ha sviluppato l'app ha anche l'obbligo di rispettare la tua scelta al di là dell'identificatore pubblicitario, in conformità con le policy che deve accettare per distribuire la sua app sull'App Store. Se ci accorgiamo che un'app viola le policy tracciando anche chi ha chiesto di non farlo, chiediamo che venga aggiornata in modo da rispettare la scelta dell'utente, e se ciò non avvenisse potremmo rimuoverla dall'App Store.

Se uso un mio account social per accedere a un'app, il social network può tracciare quello che faccio nell'app?

Dipende: può farlo se hai autorizzato l'app a tracciarti. Se selezioni "Chiedi all'app di non eseguire il tracciamento", l'app non può tracciare la tua attività in app o siti web di altre aziende a scopo pubblicitario, né condividere le tue informazioni con rivenditori di dati. Di conseguenza, non può fornire le tue informazioni all'azienda del social network se verranno usate a quello scopo.

Che cosa fa Apple per assicurarsi che le informazioni sulla privacy nelle descrizioni delle app sull'App Store siano accurate?

Le informazioni sulla privacy nell'App Store sono fornite da chi ha sviluppato l'app, come già avviene per l'indicazione dell'età consigliata. Se ci accorgiamo che le informazioni sono imprecise, collaboriamo con il team di sviluppo per assicurarci che vengano corrette.

Che cos'è un rivenditore di dati?

In generale, un rivenditore di dati è un'azienda che con regolarità raccoglie, vende, cede o divulga a terzi informazioni personali di particolari utenti finali con cui non ha un rapporto diretto. In alcune giurisdizioni, i rivenditori di dati sono definiti dalla legge.

Fonti

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

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

3. Competition & Markets Authority, "Online platforms and digital advertising", 1 luglio 2020.

4. Hitlin, Paul e Lee Rainie, "Facebook Algorithms and Personal Data", *Pew Research Center*, 16 gennaio 2019.

5. AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC", 24 settembre 2020.

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

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

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

9. Modulo 10-K 2018 di Acxiom Corporation, presentato il 25 maggio 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. 3, 2018, pp. 63-83.

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

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

13. Deighton, John e Leora Kornfeld, "The Socioeconomic Impact of Internet Tracking", *Interactive Advertising Bureau*, febbraio 2020.

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

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

16. Thompson, Stuart A. e Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy", *The New York Times*, 19 dicembre 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 luglio 2018.

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

19. Schechner, Sam e Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook", *The Wall Street Journal*, 22 febbraio 2019.

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

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

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

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

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

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

26. Thompson, Stuart A., "These Ads Think They Know You", *The New York Times*, 30 aprile 2019.

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

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

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

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

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

32. Ramirez, Edith, Julie Brill et al., "Data Brokers: A Call for Transparency and Accountability", *Federal Trade Commission*, maggio 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 agosto 2017.

35. Fowler, Geoffrey A., "You watch TV. Your TV watches back", *The Washington Post*, 18 settembre 2019.

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

37. Se la persona associata all'ID Apple registrato su un dispositivo ha meno di 18 anni, l'accesso all'IDFA è disattivato per impostazione predefinita e non può essere concesso a nessuno sviluppatore.

38. Guida di Google Ads, "Informazioni su Smart Bidding", support.google.com/google-ads/answer/7065882?hl=it.

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

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