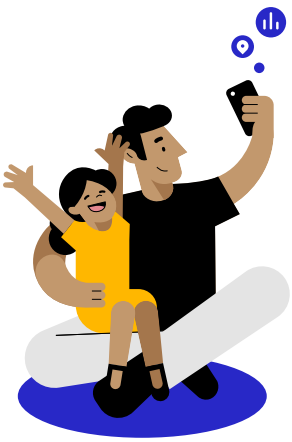


A Day in the Life of Your Data

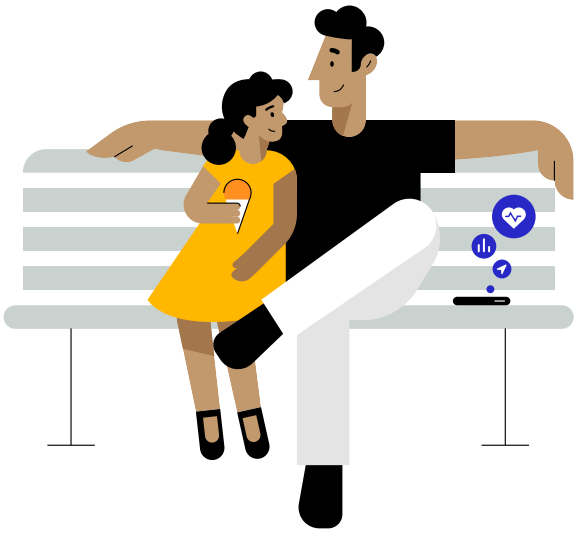
A Father-Daughter Day at the Playground

April 2021

“I believe people are smart and some people want to share more data than other people do. Ask them. Ask them every time. Make them tell you to stop asking them if they get tired of your asking them. Let them know precisely what you’re going to do with their data.”

Steve Jobs

All Things Digital Conference, 2010



Over the past decade, a large and opaque industry has been amassing increasing amounts of personal data.[1,2]

A complex ecosystem of websites, apps, social media companies, data brokers and ad tech firms track users online and offline, harvesting their personal data. This data is pieced together, shared, aggregated and used in real-time auctions, fuelling a $227 billion-a-year industry.[1] This occurs every day, as people go about their daily lives, often without their knowledge or permission.[3,4] Let's take a look at what this industry is able to learn about a father and daughter during an otherwise pleasant day at the park.

Did you know?

Trackers are embedded in apps you use every day: the average app has six trackers.[3] The majority of popular Android and iOS apps have embedded trackers.[5,6,7]

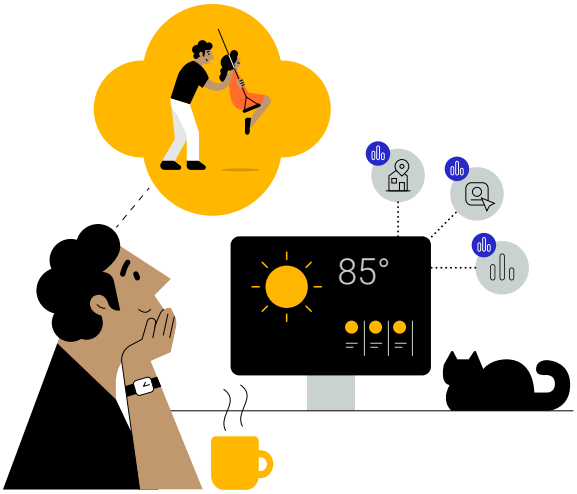
Trackers are often embedded in third-party code that helps developers build their apps. By including trackers, developers also allow third parties to collect and link data you have shared with them across different apps and with other data that has been collected about you.

Data brokers collect and sell, license or otherwise disclose to third parties the personal information of particular individuals with whom they do not have a direct relationship.[3]

Hundreds of data brokers harvest online and offline data.[8] One broker collects data on 700 million consumers worldwide, creating consumer profiles with up to 5,000 characteristics.[9]

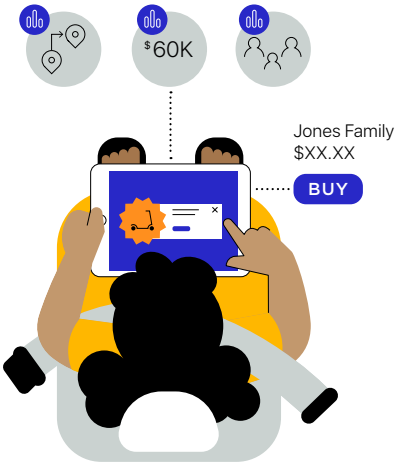
A study found that in nearly 20% of children's apps, developers collected and shared personally identifiable information without verifiable parental consent.[10]

Every hour of every day, billions of digital ads are shown to users online.[11,12,13] In the milliseconds it takes an ad to load, a real-time auction takes place, during which advertisers bid on the ad space, often relying on tracked personal data about the individual[14,15]



John plans a day at the park with his daughter

John and his seven-year-old daughter, Emma, are spending the day together. In the morning, John uses his computer to look up the weather, read the news and check a map app on his smartphone for traffic conditions for a trip to the playground next to his daughter's school. During the ride, there are four apps on his phone collecting and tracking their location data periodically in the background.[16,17,18] After the data has been extracted from the device, app developers sell it to a host of obscure third-party data brokers that John has never heard of.[16,17] Although the location data collected is claimed to be anonymous, user tracking allows data brokers to match John's location history from these apps with information collected from his use of other apps.[16,19] This means information tracked across different apps and from multiple sources is available for any company or organization to purchase, and could be used to create a comprehensive profile about him that includes his precise day-to-day movements.[3,16]



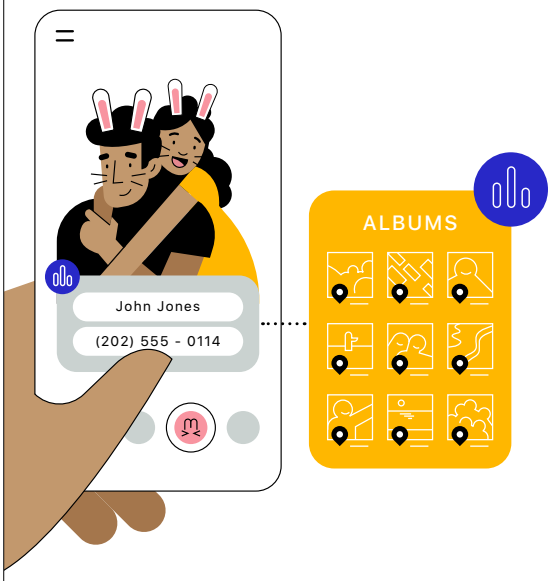
Emma plays a game on the ride to the park

On the ride to the playground, John lets his daughter play a game on his tablet. When she opens the app, she sees an ad for a scooter—and that was no accident. In the split second the app loaded, an auction occurred for the ad space.[14] Through intermediaries, the advertising companies working on behalf of the scooter company learned about the available ad.[15] Then, using personal data collected about John and Emma, they bid on the ad.[15] The scooter company's advertising partners continue to collect information about John and Emma's behaviour after seeing the ad, to determine if they clicked on it, or bought the scooter.[3] And they will continue to advertise the scooter in every way they can to John and Emma, following them across different apps and websites on all of John's devices.[3,20,21]

Some apps request access to more data than is required to provide their service, such as a keyboard app requesting precise location access.[5]

The exchange of information can go to advertising networks, advertising publishers, attribution and measurement providers, data brokers, other private companies and even governmental organizations.[3,15,40,41,42] Social media and ad tech companies either face or have paid millions in fines for using personal data for purposes outside those they had specified to the user at the time of collection.[22,23,24,25]

Data brokers use the data they harvest to assign attributes to users and bucket them into hyper-detailed market segments, such as individuals who are "trying to lose weight but still love bakeries."[26] But these profiles are often wrong: a study found that over 40% of the attributes are inaccurate.[27,28]

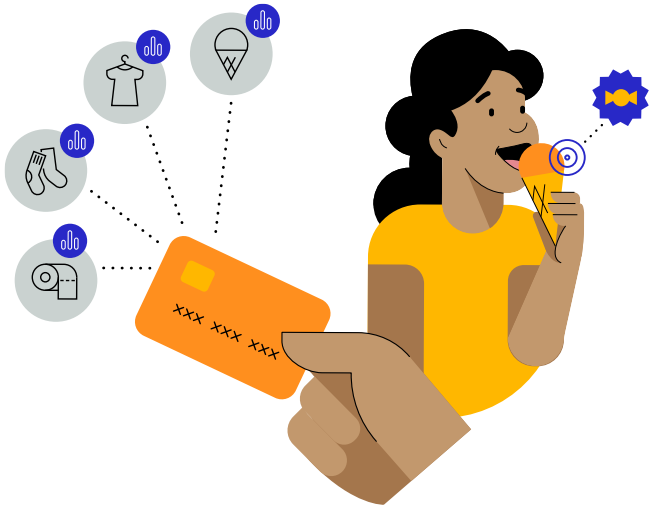


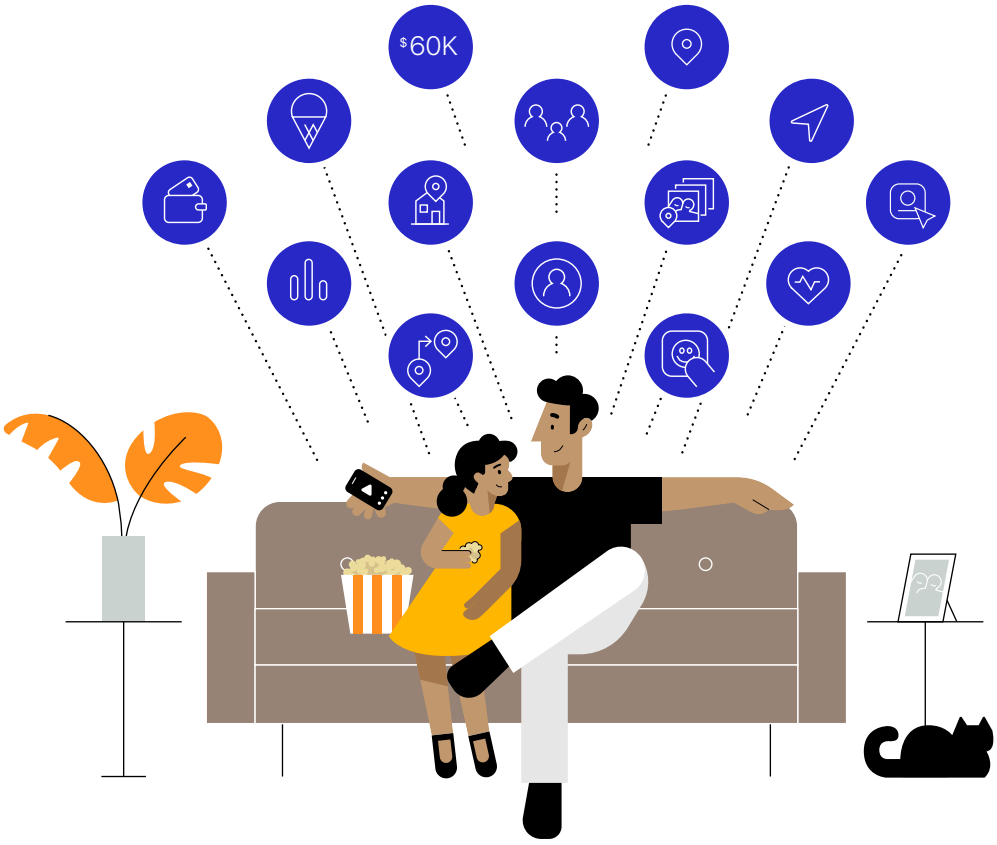
John and Emma take a selfie at the park

Later, at the playground, John and Emma take a selfie. They play with a photo filter app, settling on adding bunny ears to the photo. The filtering app, however, is able to access all the photos on the device and the attached metadata, rather than only the playground selfie.[29,30] John posts the picture on a social media app. The app links John's current online activity to a trove of data collected by other apps, such as his demographic information and purchasing habits, using an email address, a phone number or an advertising identifier.[3]

A stop at the ice cream shop on the way home

On the way home, John and Emma stop for ice cream as a treat. John pays for the ice cream with a credit card, and more information is added to the comprehensive data profile of his preferences: the location of the store and how much he spent.[31,32,33] One of the apps that track John's location is able to observe that John and Emma also stopped by a toy store.[3] The information about where the family shopped during the day is passed along to data brokers, who combine it with the knowledge that he has a young child to pepper John's devices with targeted ads for sugary treats and for the toy store they visited.[17]





At the end of the day, a number of companies John has never interacted with, all around the world, have updated their profiles with information about him and his daughter. These companies know the location of the family's house, the park they visited, the news websites they read, the products they browsed, the ads they watched, their purchasing habits and the stores they visited.[3,34] This data was collected and tracked across multiple apps John and his daughter used throughout the day, as well as from other sources. John had no idea how much data was being collected throughout the day, didn't always have control over it and didn't knowingly give permission for it to occur.[3,4] As they search for a kid's movie on an app in their smart TV to kick back for the evening, the cycle of tracking, exchanging data, auctioning and re-targeting relentlessly continues.[35,36]

Apple's privacy principles

Apple believes that privacy is a fundamental human right. We design our products and services guided by our four key privacy principles:

Data Minimization
Collecting only the minimum amount of data required to deliver what you need for a given service.

On-Device Processing
Processing data on the device, wherever possible, rather than sending it to Apple servers, to protect user privacy and minimize data collection.

User Transparency and Control
Making sure that users know what data is shared and how it is used, and that they can exercise control over it.

Security
Hardware and software working together to keep data secure.

Through those four principles, Apple's goal has always been to let users share data as they wish, in a way that is safe, and that they understand and control. This is the reason why, for the last two decades, Apple has continuously innovated to preserve user privacy through all of our products and services. For example, we employ on-device intelligence and other features to minimize the data that we collect in our apps, browsers and online services, and we do not create a single comprehensive user data profile across all of our apps and services.

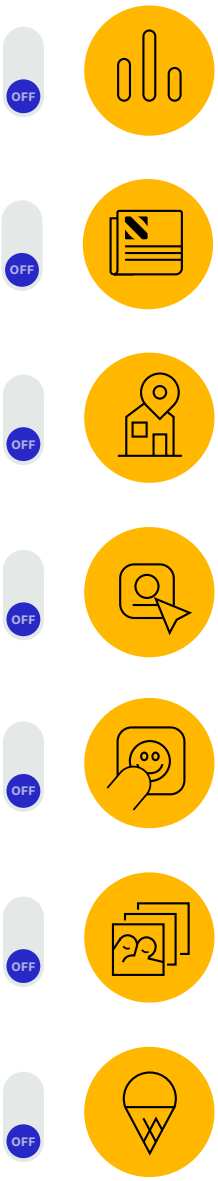
To learn more about the privacy features Apple has introduced, and the work Apple is doing to protect users' privacy, visit apple.com/ca/privacy.

To learn more about how Safari protects your privacy, read the Safari White Paper.

To learn more about how Apple protects your location data, read the Location Services White Paper.

Apple's privacy features give John more transparency and control over his data

The story of John and Emma's day illustrates the privacy problems and solutions we're working on at Apple.



John plans a day at the park with his daughter

If John had used the Safari browser to check the weather on his computer, Intelligent Tracking Prevention would have prevented tracking of this activity by default.

If John had used Apple News to read the news in the morning, Apple would have delivered John content based on his interests, without knowing who he is or learning what he read.

If John had used Apple Maps to check the traffic, his location data would have been linked to a random identifier, which is regularly reset and not linked to John. As a result, no one but John would end up with knowledge of his location.

On an iPhone, John would be periodically reminded of which apps are accessing his location in the background. Before sharing location with an app, John could choose to only share his approximate location, or only share his location once.

Emma plays a game on the ride to the park

On an iPad, the upcoming App Tracking Transparency feature would give John a choice as to whether to allow the game to track Emma's activity across apps and websites owned by other companies.

Ad networks that use Apple's SKAdNetwork API would be able to measure the overall effectiveness of their ads without getting access to information that could be traced back to John's device.

John and Emma take a selfie at the park

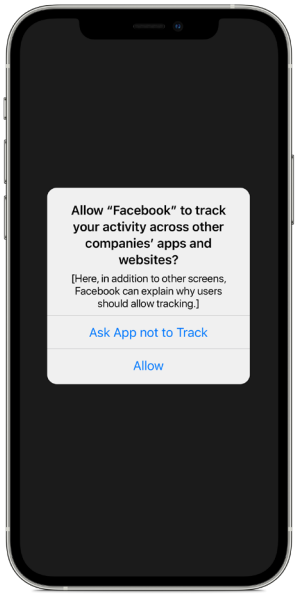
On an iPhone, John would have had the choice to give the filter app access to only the selfie, instead of the entire photo library.

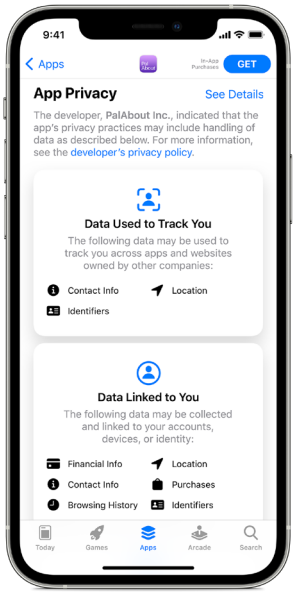
A stop at the ice cream shop on the way home

If John had bought the ice cream using Apple Card, his bank would not use his transaction information for marketing purposes. Had he used Apple Pay, Apple would have used on-device intelligence so that John could view his transaction history on his iPhone without Apple obtaining information about where he shopped, what he purchased or how much he spent.

At the end of the day, Apple products and privacy features can give John better transparency and control throughout the day over how much of his data is shared, and how it is used.

App Tracking Transparency and the new privacy information section on the App Store





Apple is taking the next step to protect users’ privacy within the app ecosystem. As a complex and growing set of entities access, track and monetize personal consumer data, Apple is introducing two new features aimed at providing users with increased transparency, visibility and choice so that they can make informed choices and exert greater control over their privacy.

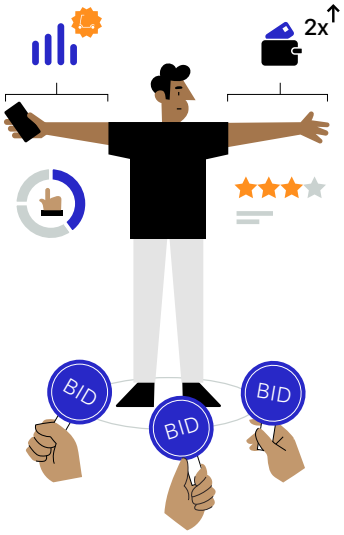
Starting soon, with our next beta update, App Tracking Transparency will require apps to get the user’s permission before tracking their data across apps or websites owned by other companies. Under Settings, users will be able to see which apps have requested permission to track so they can make changes as they see fit. This requirement will roll out broadly in early spring with an upcoming release of iOS 14, iPadOS 14 and tvOS 14, and has already garnered support from privacy advocates around the world. In designing this feature, Apple sought to give users more transparency and control while continuing to enable advertising as an appropriate and viable means of supporting apps and web content. The introduction of past features, such as Safari Intelligent Tracking Prevention, have shown that advertising can continue to be successful while enhancing users’ privacy protections. App Tracking Transparency allows users to make more informed choices about the apps they use and the permissions they grant to those apps. With App Tracking Transparency, users can now choose whether to allow apps to track them. For apps that users trust and provide permission to track, developers can continue to do so.

In addition to requiring user permission for tracking, Apple also recently introduced changes to App Store product pages to increase transparency. With the new App Privacy section, the App Store helps users better understand some of an app’s privacy practices. Each app’s product page is required to provide users an easy-to-view summary of developers’ privacy practices. The details pages include information on the types of data that the app collects, such as photos, location and contact information. The pages also provide users with additional details about how each kind of information is used by the app developer, including whether it is used for tracking, and whether the data is linked to the user. All app developers, including Apple, are required to self-report information regarding their privacy practices.

The addition of app tracking settings and transparency and privacy information on App Store product pages empowers users to more easily learn how their personal data is used, shedding light on practices that were previously opaque and hidden, allowing them to take greater control of their data.

Apple will continue to develop innovative privacy technologies and work on new ways to keep your personal information safe.

A Day in the Life of an Ad



Ad Auctions

When Emma saw an ad for a scooter on John's screen, it wasn't an accident. Advertisers bid in an auction to show their ad on the device.[37] Here is a simplified explanation of how, in a fraction of a second, the ad displayed on the device's screen was picked:

1.
The developer of the app Emma is using hires an ad tech company that auctions off their ad space in real time.[14]

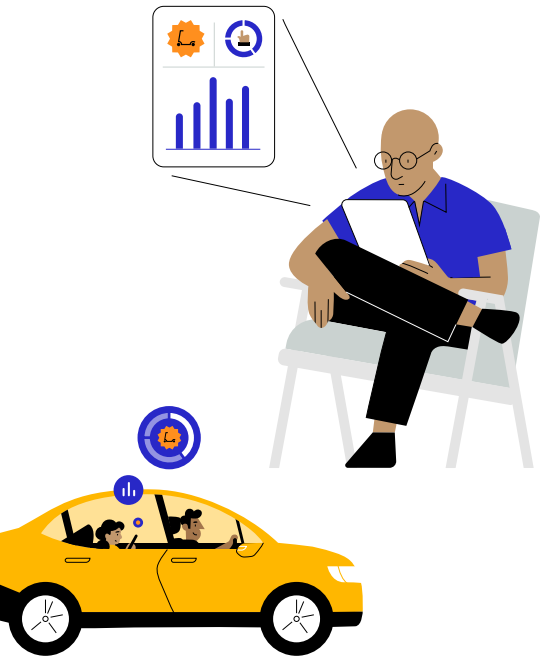
2.
When Emma opens the app, the advertising network gathers data from the use of John's device (for instance, which app she's using, her location and John's advertising ID), as well as from third parties, relying on John's advertising ID or other information that enables tracking.[3]

3.
The advertising network shares some of this information, in particular the advertising ID, with potential advertisers. Before bidding, advertisers typically try to learn as much as possible about the user, from their own data as well as from personal data collected and aggregated via tracking and profiling.[3,15]

4.
The more John and Emma's characteristics — which are derived from their data — align with the advertiser's target audience, the more advertisers will bid for the ad space.[15,38]

5.
The winning bidder's ad for a scooter is displayed on the device Emma is using.[14]

Because the ad auction process happens in a fraction of a second, both buyers and sellers collect, exchange and use personal data to bid for space and display ads.[14,15]



Ad Attribution

After its ad is shown to the user, the scooter company's advertising companies are interested in measuring its effect on Emma's behaviour. This process is called ad attribution.

To do so, the advertiser tries to track behaviour on the device Emma's using, to collect information on what she does on the web, on apps, and even where she goes offline.

- **If the ad is for a product,** the advertiser could try to track whether the user later visited its website or physical store to purchase it.[3]
- **If the ad was for an app,** the advertiser would try to track whether she installed it. This is called app install attribution.[39]

Advertisers also use ad attribution to "optimize" their ad campaign towards groups for which the ad campaign is more effective.[3]

It doesn't have to be that way. Advertisers can measure the impact of their ad campaigns toward groups without tracking users. Apple has been working on tools that do this while preserving user privacy:

SKAdNetwork lets advertisers know how many times an app was installed after ads for it were seen, so advertisers can measure the impact of their ad campaign. But this information is designed not to share any user or device-level data, so advertisers don't track users.

Private Click Measurement for apps in iOS and iPadOS 14.5 allows advertisers to measure the impact of ads that lead users to a website while minimizing data collection using on-device processing. After a user clicks on an ad for a product in an app, the web browser itself, using Private Click Measurement, can give advertisers information that a user clicked on their ad, and that it led to a certain outcome on their website, such as a visit or a purchase — without giving them information about who specifically clicked on the ad.

Frequently Asked Questions

Will I still be able to use the app's full capabilities if I select "Ask App not to Track"?

Yes. App developers cannot require you to permit tracking in order to use the app's full capabilities.

What are identifiers and how are they used?

Identifiers such as the Identifier For Advertisers (IDFA) and email address help identify a specific device across a network. They also allow advertisers to create a detailed profile of your activity across different apps or websites when they see your device identifier and associate your activity with it.

What is the Identifier For Advertisers (IDFA)?

The Identifier For Advertisers (IDFA) is a user-controllable identifier assigned by iOS to each device. As a software-based identifier rather than one that is tied to the hardware itself, the IDFA can be blocked for a particular app by the user via the App Tracking Transparency prompt. This gives the user control over IDFA-based tracking.

Can Apple guarantee that an app isn't tracking me if I select "Ask App not to Track"?

If you select "Ask App not to Track," the developer will not be able to access the identifier for advertisers (IDFA), which is often used to track. The app developer is also required to respect your choice beyond the advertising identifier. This is required by the policies the developer agrees to when submitting their app for distribution on the App Store — if we learn that a developer is tracking users who ask not to be tracked, we will require that they update their practices to respect your choice, or their app may be rejected from the App Store.

If I use my social media account to sign into an app, can the social media company track what I do in that app?

This depends on whether you've given the app permission to track you. If you select "Ask App not to Track," then the app should not engage in tracking you across other companies' apps or websites for advertising, or share your information with a data broker. That means they should not provide your information to the social media company if it will be used for that purpose.

How does Apple ensure the privacy information on App Store product pages is accurate?

Similar to how Age Ratings work on the App Store, developers report their own privacy practices. If we learn that a developer may have provided inaccurate information, we will work with them to ensure the accuracy of the information.

What is a data broker?

In general, a data broker is a company that regularly collects and sells, licenses or otherwise discloses to third parties the personal information of particular end-users with whom the business does not have a direct relationship. Data brokers are defined by law in some jurisdictions.

Sources

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16. Thompson, Stuart A., and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times*, December 19, 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*, July 21, 2018.

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

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

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

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

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

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

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

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

26. Thompson, Stuart A., "These Ads Think They Know You," *The New York Times*, April 30, 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*, April 5, 2018.

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

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

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

32. Ramirez, Edith, Julie Brill, et al., "Data Brokers: A Call for Transparency and Accountability," *Federal Trade Commission*, May 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*, August 1, 2017.

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

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

37. If the user age associated with the Apple ID registered to a device is under 18, IDFA access is disabled by default, and cannot be granted to any developer.

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*, February 4, 2019.

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

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

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