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. 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. This occurs every day, as people go about their daily lives, often without their knowledge or permission. 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. The majority of popular Android and iOS apps have embedded trackers.

- **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.
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. 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. 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. This means information tracked across different apps and from multiple sources is available for any company or organisation to purchase, and could be used to create a comprehensive profile about him that includes his precise day-to-day movements.

Emma plays a game on the way to the park

On the way 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. Through intermediaries, the advertising companies working on behalf of the scooter company learned about the available ad. Then, using personal data collected about John and Emma, they bid on the ad. 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 it or bought the scooter. 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 John’s devices.
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. One of the apps that track John’s location is able to observe that John and Emma also stopped at a toy shop. 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 the toy shop they visited.

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. 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.

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

The exchange of information can go to advertising networks, advertising publishers, attribution and measurement providers, data brokers, other private companies and even governmental organisations. 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.

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

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. One of the apps that track John’s location is able to observe that John and Emma also stopped at a toy shop. 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 the toy shop they visited.
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 shops they visited.\textsuperscript{3,4} 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.\textsuperscript{3,4} As they search for a kid’s film on an app in their smart TV to watch in the evening, the cycle of tracking, exchanging data, auctioning and retargeting continues relentlessly.\textsuperscript{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 Minimisation
Collecting only the minimum amount of data required to deliver what you need for a given service.

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.

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

Security
Hardware and software working together to keep data secure.

Through these 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 our products and services. For example, we employ on-device intelligence and other features to minimise the data we collect in our apps, browsers and online services, and we do not create a single comprehensive user data profile across all our apps and services.
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 way 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 monetise personal consumer data, Apple is introducing two new features aimed at providing users with increased transparency, visibility and choice so 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. 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.

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. 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.

4. The more John and Emma’s characteristics — that are derived from their data — align with the advertiser’s target audience, the more advertisers will bid for the ad space.

5. The winning bidder’s ad for a scooter is displayed on the device Emma is using.

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.
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 shop 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 “optimise” 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 towards 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 minimising data collection using on-device processing. After a user clicks an ad for a product in an app, the web browser itself, using Private Click Measurement, can give advertisers information that a user clicked 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 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 them to 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 in to 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.