Tips & Tricks for iPhone

Privacy, Please

Simple, practical tips to help protect your personal data on iPhone

Privacy, Please

Simple, practical tips to help protect your personal data on iPhone

---

Written and edited by Tom Rolfe.

Additional copy by Craig Grannell.

Layout by Holly Rolfe.

Copyright © 2022 Intelligenti, Ltd.

All rights reserved.

Everything you need to know about privacy

Privacy, says Apple, is a fundamental human right. They're not wrong.

There was a time when minding your own business was enough, but in an increasingly online world, there are more and more pitfalls to worry about when it comes to your digital presence. When your iPhone knows your address, your bank details, where you've been, which websites you visit, and even what your kids look like, it's no understatement to say that protecting that data is key.

iPhones might have a bigger focus on privacy than rival smartphones, but even so it's vitally important to know when your data is collected, how it's used, and how you can stop it from happening. What you share, and when, should be up to you.

Here, we've compiled some of our best-loved articles from the past few years on the topic of iPhones and privacy, to give you a leg-up and ensure you don't inadvertently leave yourself open to oversharing.

Chapter one looks at Apple's stance on privacy, and the measures it automatically takes to protect you. Chapter two contains recommendations for the iPhone settings you should change ASAP to keep snoopers away. Chapter three focuses on the tech giants that trade in personal data, and how to keep them at bay.

Welcome to **Privacy, Please**.

All the best,

Tom Rolfe
Editor, Tips & Tricks for iPhone

Contents

CHAPTER 1

Apple on Privacy

iPhone and privacy

Why Apple deserves your trust

For Apple, the issue of privacy is nothing new. For some time, it has been a differentiator between Apple and rivals who are a bit too eager to sell your data to advertisers.

With Apple, which primarily makes money from hardware sales and first-party services, you are of course the *customer*. But with certain other companies, you just think you are; in reality, you are also the *product* – something to be sold, when a company relies heavily on partners, advertising, and data sales to make ends meet.

Face Off

Apple has on iPhone and iPad gone the extra mile with security interface concepts now considered largely ubiquitous within the industry. Touch ID was always secure and private, but Face ID is far more so, due to the sheer amount of technology smarts Apple packed in. Face identification systems on some (notably cheaper) Android devices, though, are worryingly easily fooled – even by something as simple as holding a photo of the device owner up to the camera.

There are also questions about data usage, and who can gain access to your data. With Apple, however, you're safe in the knowledge strictly personal data is held on your device, in the Secure Enclave that's part of the A-series processor. This means your biometric data cannot be accessed by iOS or apps. In fact, it can't even be accessed by Apple, because it's not stored on Apple servers nor backed up to iCloud.

There are occasions where Apple does work with data to create better experiences, but even then the company utilizes Differential Privacy – scrambling your data and combining it with sets from millions of other users. The result is Apple can only see general patterns, and nothing that can be traced back to an individual.

Location, location, location

Since iOS 13, Apple is taking things further. When apps require location data, **Always Allow** is no longer be an immediately accessible option – you'll instead have to go to Settings for that. Instead, when an app asks for permission, you'll choose from **Allow While Using App, Allow Once**, or deny location access entirely. This makes it much harder for apps to nefariously track your movements and data in the background.

Another big change – one that feels like Apple slamming its fists on the table and yelling "enough" – is **Sign in With Apple**. This upends the way in which people sign into apps and websites. Previously, you may have used a social network sign-in button to sign into an app, primarily for speed and convenience; alternatively, perhaps you've grudgingly given your email address to app developers, who subsequently spammed you with marketing material.

As apps are updated, you'll be able to sign in using your existing Apple ID, and then Face ID or Touch ID. Apps may still ask for your details, but you can optionally have iOS create a unique email address for that specific app/service. This will forward to your real address, and can be turned off at any point.

An uneven playing field

Apple's privacy revamp extends into other areas of technology that have made for terrifying headlines, like home security cameras. Companies in the past have abused trust, or lacked the security such systems demand. Apple says its end-to-end encrypted system will store your video on iCloud, where it'll only be accessible to you and those you choose to invite. Storage won't count against your existing iCloud plan either.

Naturally, all these things – limitations on location data; Sign in with Apple; HomeKit Secure Video – have certain other companies in the tech space up in arms. There are shouts about anticompetitive behavior, not least due to the amount of control this affords Apple in the ecosystems the company has interests in.

Such pushback suggests Apple has got things right. Had the rest of the industry not allowed itself to get into this state, where privacy was sidelined in favor of commercial interests, Apple wouldn't have had to push privacy so hard – it would have been a given anyway. And it's not as if Apple's rivals can't follow suit – they just have to stop snooping on you and selling your data. In other words, they will have to prioritize privacy, too.

The future of privacy

The future is uncertain. Apple's privacy plans could fail, or the company could end up as a tiny niche concern with little leverage and influence. Also, there is a question of trust when you're relying heavily on Apple – and recent events have shown the company doesn't always get everything right.

After a spate of news stories surrounding smart home kit listening in on your every word, Apple got caught up in the row. The Guardian revealed Apple contractors regularly heard confidential details on Siri recordings. The snippets were anonymized, not traceable to a source, and "typically only a few seconds long". Even so, when your main differentiator is privacy, you must be squeaky clean across the board, and not merely better than everyone else.

Fortunately, Apple quickly made good. The program was halted, and in future you'll be able to opt-in. Notably, rivals more often fight against you having more privacy, because this reduces how much money they can make from what you do. Assuming Apple doesn't fall from grace, then, and continues to bang the privacy drum, we may years from now look back and be grateful the biggest technology company in the world – while imperfect –was also the one that actually cared about privacy, giving you a choice rather than taking it from you.

Privacy at Apple

How are its key apps kept secure?

Privacy is a big deal these days, and Apple is increasingly making its protection of user data a key selling point. One of its most compelling ads, Private Side, argues that "if privacy matters in your life, it should matter to the phone your life is on." It's hard to argue with that.

Now, Apple has updated the Privacy page on its website to make its policies even clearer to the average user. It's a beautifully designed web page that uses colorful animations and short explainers to break down exactly how each of its core apps keeps your data private. If you've ever been curious how *Safari* blocks tracking, how *Maps* anonymizes your travel, how *Photos* protects your images, or how *Messages* encrypts your chats, this is the place to go.

One thing we're pleased to see is confirmation that Apple has reversed its stance on Siri's controversial quality control program to give users a clear choice on whether they're happy to take part. This is one of the few times Apple has failed to meet its own high privacy standards and it's good to see the company making amends.

The Privacy page also goes into detail on *News*, *Wallet*, *Apple Pay*, *Health*, and the *App Store* – plus one of our favorite iOS features in Sign in with Apple.

If you're interested in the nitty-gritty of how these features work, the Features section of the site includes links to detailed white papers. And the Control section has some solid tips on how to secure your devices and control your privacy settings.

One thing that's not clear is how to view and access all the data Apple *does* tie to your Apple ID. Luckily, we've got you covered with a tutorial on how to do just that (written last time the Privacy site was updated).

You may think that privacy and security notices are boring, and – well, they usually are. But Apple has done a great job making the topic clear and easily digestible, and we strongly suggest you take a look.

Apple's privacy stance

Is it a help or a hindrance?

From clipboard notifications to slapping down tracking, iOS wants to keep what you do on your device private.

If you were using an iPhone in 2020, you might have noticed something new when using certain apps: a new notification. Specifically, a notification that warns you when an app grabs the content of your clipboard.

Comically, TikTok users found the alert appeared *every few keystrokes* they made, meaning the app was constantly checking the clipboard. Naturally, the company denied any wrongdoing, and argued this 'feature' was "designed to identify repetitive, spammy behavior".

TikTok subsequently updated its app, despite said claims it was doing nothing untoward. But it's far from alone — other apps have been similarly caught out, with their owners blaming clipboard polling on everything from outdated software development kits to previously unknown bugs.

Bumps in the road

Ultimately, what's really happening is Apple again surfacing potential privacy violations. We've already seen this in iOS warning about apps that use location data

without your knowledge. Now Apple's decided even your clipboard needs protection — but is that warranted?

After all, there are legitimate reasons why an app should read the clipboard. For example, a social networking app can check whether you'd already copied a web page link, and then automatically send you on to the relevant content.

This kind of streamlined experience is what people have come to expect from iPhone. Increasingly, though, we are looking at repeated moments of added friction — and there's more to come.

Locking down data

Apple adds new features with each update; each new version of iOS is the most privacy-oriented version of iOS to date. Apple's doubling down on one of its main differentiators from Android, presenting iOS as a system that will keep your data private.

Sometimes, it merely provides information for those who look for it, such as upcoming mandatory privacy policy listings for the App Store, and website privacy reports in Safari. Other features are passive, such as a new recording indicator when an app's using the mic or camera. But there will be times when you'll get new alerts and have to make new decisions.

Apps will now have to ask for tracking permission, and you'll be able to check (and prune) a list of apps afforded said permission. You'll be able to approximate your location, should you choose to do so, and instead of providing apps with access to all your photos, only give them access to what they need to perform a specific task.

The new normal

The question is whether this new cognitive load is worth it, and whether Apple will be able to train iPhone and iPad users that this new normal is for their benefit.

People won't be safer if they don't take a few moments to consider what an alert is asking for, and just stab OK to dismiss it. (App and game creators also need to be better in explaining *why* such permissions need granting.) Similarly, it could fast become irritating if you keep seeing clipboard pop-ups as you switch between apps.

Apple's bet is that you will put up with minor niggles, in order to be better informed when apps are behaving in a way they shouldn't. In short, iOS looks to be a little more intrusive when it comes to the user experience, but the flip side is third parties will be less likely to intrude on your data and usage patterns.

Security comparison

iOS beats Android by a mile

A group of security experts has published a report on the global availability of security updates for smartphones, with iOS devices easily topping the comparison chart. While it's not a big surprise that Apple would beat out the competition in a "caring about security" fight, it's a little shocking to see just how badly some of the big Android manufacturers fared in the comparison.

Microsoft and Nokia also scored remarkably well, with smartphones running Windows OS coming in a close second to iOS devices in terms of security releases. Unfortunately, Windows phones can't really compete with the diverse app choice and rich feature sets of iOS and Android devices.

The report, which was carried out by independent analysts *SecurityLab*, looks at how quickly each company provides security updates once a flaw is discovered, and how

long each company's smartphones are continually supported with security updates after the launch of the device.

According to the report, Apple typically responds to security threats within a few days. Google and Essential are the only Android vendors who can boast the same, with most Android response times measured in weeks or even months.

Apple is also miles ahead of the competition in terms of overall support duration, with all devices fully supported with security updates for a full five years after release. (With the exception of iPhone 5C, which was only supported for four years.) This duration is unheard of in the Android world, with companies like Samsung, LG, and Huawei supporting devices for anywhere between 1 and 2.5 years after release.

To be fair, the fact that Android devices are so far behind is in part due to the fact that so many different models and variations exist. It's difficult to maintain support for such a wide product base, which is probably why Android smartphones aren't typically supported with security updates for more than a couple of years. By comparison, Apple has much tighter control over iOS and far fewer devices to worry about.

Though this study is fairly limited in scale, it does hammer home one of the big advantages of using an Apple device. With iOS, users are kept safe for longer than any other platform.

CHAPTER 2

Permission Impossible

Message privacy

Hide your lock screen previews

Depending on how your device is configured, new messages could appear on the Lock screen in all their glory — ready for prying eyes to read through! Fortunately, it's possible to customize whether a message is displayed in full when your device is locked.

Open **Settings** and navigate to **Notifications**, then **Messages**. Towards the bottom of the screen is a button labelled **Show Previews.**

This should be set to **When Unlocked** by default, but if it isn't, choose this option. This will prevent the full content of messages from appearing on your device's Lock screen — instead, the content will only appear following Face ID or Touch ID verification, or when you've unlocked your device using a passcode.

You can also configure previews to appear **Always** or **Never**, depending on your preference.

This is possible for email messages, too. Open **Settings**, **Notifications**, then select **Mail** and follow the above steps. Now, neither text or email previews will appear on your device when received.

You'll find similar options in the settings for third-party messaging apps like **Facebook Messenger** and **WhatsApp**.

Privacy permissions

Choose what you're happy to share

Some apps can access your location, contacts, calendar events, reminders, or pictures. To check which apps use these, open the **Settings** app then select **Privacy** and look into each option to see which apps are accessing those details.

This function can be turned off for each app if you don't want them to have this access. Note that this might affect usability in some apps.

Limited Photos access

The Privacy settings for Photos are more nuanced if you have iOS 14 or above. Apps now give you the option to only allow access to **Selected Photos** when granting permissions.

You can review and change these permissions on an app-by-app basis from **Settings** > **Privacy** > **Photos**.

Review location data

Take control of your location privacy

No time to drop into the Apple Store and ask the Genius Bar for help with your iPhone or iPad? Maybe one of our resident experts can help!

As Apple nerds, we get asked *a lot* of tech support questions – and some of those questions crop up time and time again. Here's a recent query that we think will be familiar to many of you.

"Is there a way to review which apps are using my location data?"

For years, iPhones and iPads have been able to track your location. It's a really useful capability that helps provide directions from your current location in Maps, serves up localized stories in News, and tracks your daily steps for the Health app. There are countless utilities that wouldn't be possible without this in-built GPS tech.

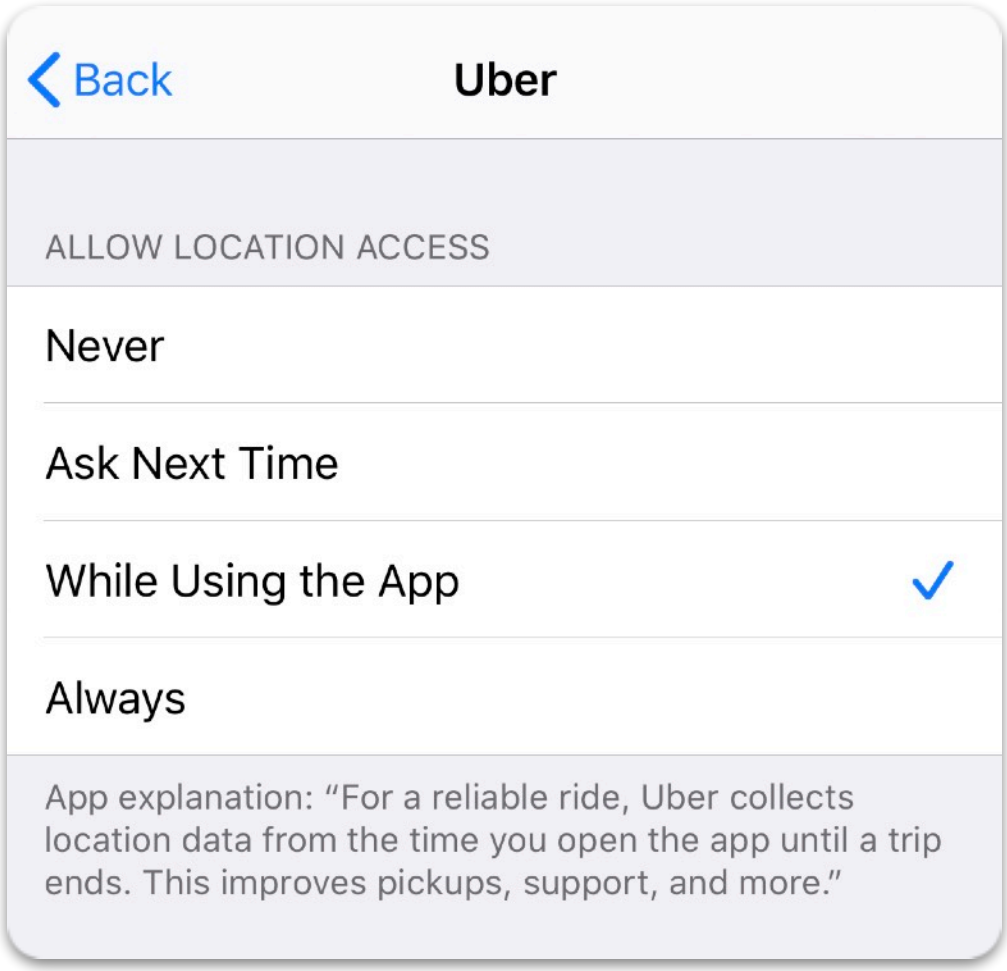
But many users are rightfully concerned about the availability of their location data, not least because tracking it can be a significant power drain.

Apple's security rules mean apps must ask for user permission before accessing your location data, but they usually only ask on first install and it's easy to lose track of which apps have been granted access.

Luckily, iOS allows users to easily keep tabs on which apps have permission to access this data, and when.

Open the **Settings** app and tap **Privacy** followed by **Location Services**. Here you'll see an alphabetical list of all your currently installed apps that have ever requested access to your location. If you see a grey or purple arrow next to an app, it means it has recently used your location data.

From this menu, you can flip the switch at the top to turn off ALL location services if you so wish – though we'd recommend setting your preferences on an app-by-app basis instead.



The level of user control was improved a while back – tap on any specific app and you'll see various levels of access to allow, plus a message from the app's developers explaining how and why they need your location data.

We'd recommend the **While Using** option as appropriate for most apps, though if you don't believe they require your location data to perform their basic functions you can select **Never** to ensure your privacy. Only a few select apps that clearly need it to work properly – such as **Tile** –should ever be granted the **Always** setting as this can drain your battery pretty fast.

iCloud+ private relay

How the new privacy feature works

At WWDC recently, Apple announced a change to its paid iCloud plans. Anyone currently shelling out for extra iCloud storage will, in the Fall, be automatically switched to a new service called iCloud+.

Apple glossed over some of the details of iCloud+, but perhaps the most notable inclusion was a new feature called Private Relay, available at the flick of a Settings switch to anyone on any iCloud+ plan.

At first glance, Private Relay sounds similar to a VPN – it reroutes all your web traffic through two encrypted "relays" to stop advertisers, ISPs, and website owners from tracking your browsing. Though features like Private Browsing in Safari can protect your history from showing up on your device, it's often still possible for all your browsing to be pieced together by cross-referencing with your IP address and the location it came from.

Essentially, with Private Relay turned on, there is no way for anyone to piece together your browsing history from your IP or location. You'll still be able to use an approximate location for websites that need it to function, while masking the exact location tied to your IP that can often be aggregated to build an advertising profile around your online behavior.

Macworld has a really good piece explaining the ins and outs of the feature, so if you're curious to see exactly how it works, check out their explainer.

At its core, though, Private Relay is a fantastic addition for users who may not ever consider setting up a VPN. But to be clear, it doesn't offer *everything* a VPN offers. For starters, it only protects you in Safari, and its usage may be blocked by large networks in offices or schools. It also can't be used to fake your location to access region-locked content on websites like Netflix, which is a common use case for VPNs. (Even though it's a legally grey area).

Private Relay should be available with the launch of iOS this September, but if you don't want to pay for iCloud or are looking for even more protection, consider getting a VPN instead.

Sign in with Apple

Quick and secure app logins

Sign in with Apple is a “single sign-on” service similar to those offered by Google and Facebook. It allows you to register an account with a new website or app without filling out all your details every time. Apple handles all your credentials for you, and puts a much bigger emphasis on privacy than the alternative solutions.

To use **Sign in with Apple**, just look for the **Continue with Apple** button when signing up for an account on a website or app. When selected, it will let you use your existing **Apple ID** to log in to that service, removing the need for more form-filling and yet another password to remember.

Protect your email

Sign in with Apple also allows you to hide your email address from the service or app in question, so your personal address can’t be shared within anyone else.

Apple can even automatically register a one-time burner email for use with a new service if you don’t wish to share your real contact details. Correspondance to the burner email will be routed to your main account, but you can turn this off at any time.

Upgrade your accounts

Safari can help you to upgrade to **Sign in with Apple** if it detects a potential data breach with one of your stored passwords, for example. Existing accounts can also be converted to **Sign in with Apple** – just follow the prompts.

Privacy Report

How Safari protects your browsing

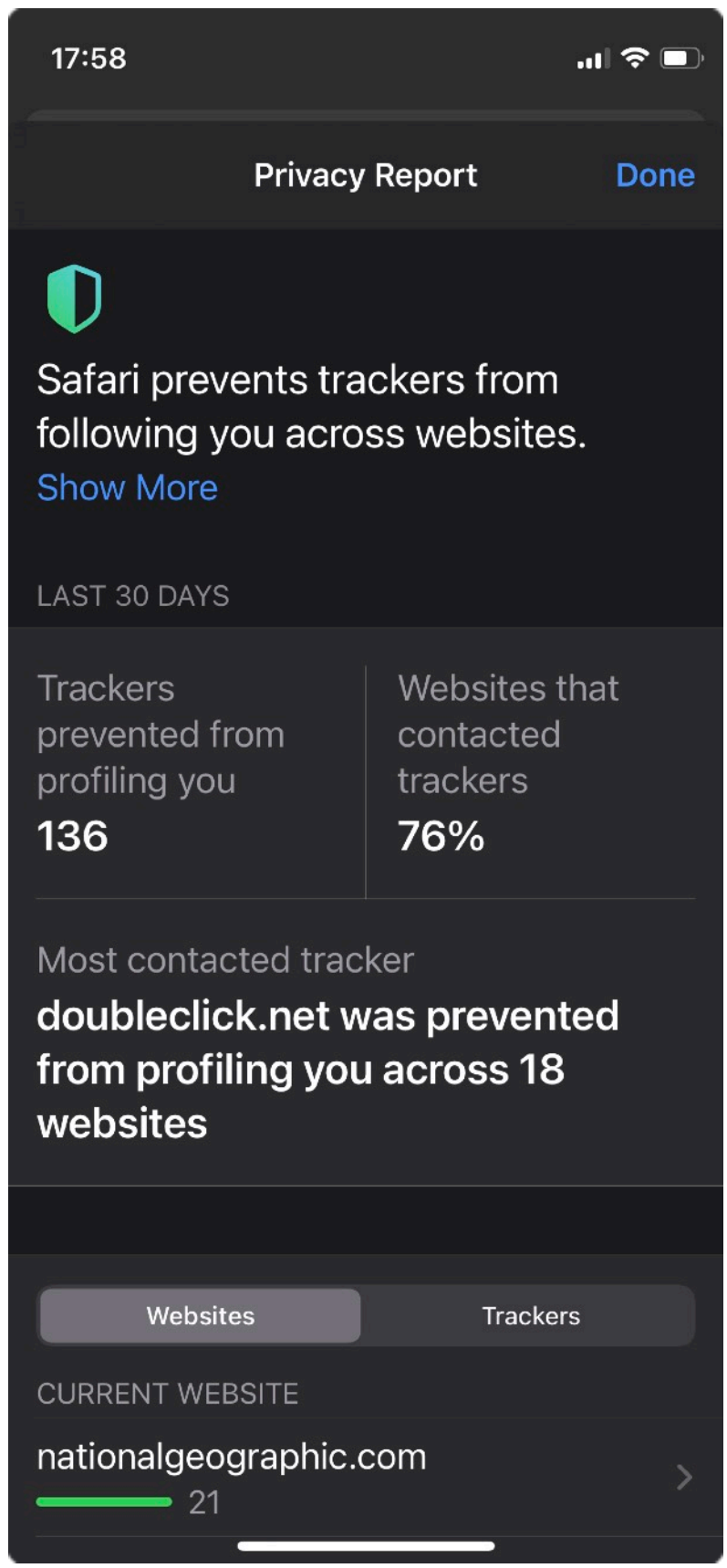
Apple has always been a stickler for privacy. To that end, Safari gained a powerful new feature called **Privacy Report**.

Let's run through what **Privacy Report** is, and how you can check it to be assured that Apple is protecting your information when browsing the internet on your iPhone or iPad.

What is Privacy Report?

Previous versions of Safari have introduced the ability to prevent websites from tracking your cookies, which means that advertisers and data collection companies can no longer build a picture of your browsing habits.

Privacy Report shows you precisely how many and which websites have attempted to track you, as well as the precise identity of the trackers that **Safari** has blocked during your browsing sessions.



How does Safari block trackers?

Apple's Intelligent Tracking Prevention employs on-device machine learning to pick out trackers and stop them from accessing your browsing data. It also uses the privacy-focused web search engine **DuckDuckGo** to independently identify known trackers.

How do I access Privacy Report?

It's very simple to obtain a report of the work Safari has been doing behind the scenes to keep your browsing data protected.

Just open Safari and tap the **Aa** icon at the top left. Then, select **Privacy Report** at the bottom of the list.

How do I use Privacy Report?

At the top of your **Privacy Report**, you'll see the number of trackers prevented from profiling you and the percentage of websites that attempted to contact trackers.

Scroll down, and you'll see the number of trackers contacted by the current website, followed by a list of the websites with the most trackers contacted. Tap on any of these websites for a breakdown of the trackers that have been prevented from profiling you.

Tap the **Trackers** tab, and this view will switch to show you the trackers most commonly contacted by the websites you've used. Tap any of these for a rundown of those websites.

Alternative privacy tools for iOS

We've already mentioned DuckDuckGo as a privacy tool that's used by Safari, but it also exists as a free stand-alone web browser on the App Store. We've long recommended it as the best web browser for the privacy-conscious.

If you're particularly wedded to Safari, there's always 1Blocker. It's a particularly fastidious content blocker extension that, once downloaded, lives within Safari, but supplies a much broader range of 'rules' to filter out even more unwanted attention from nosy websites.

App Store privacy

How to keep your purchases to yourself

Apple does a lot for user privacy by default, but sometimes you need even more. Here are two ways to keep your historical app purchases from surfacing unexpectedly or changing your browsing experience.

Personalized recommendations

Apple is pretty vocal about its respect for user privacy. But the fact is that the company nevertheless uses your data to try and increase the likelihood of you buying a new iOS app or game. This happens through "personalized recommendations", a feature added a few years back that presents users with the kind of apps which Apple thinks users want to see. This selection, of course, is based on the apps you've previously purchased.

There are a number of reasons why you might prefer "vanilla" search results in the App Store, as opposed to an algorithmically-determined selection. You might prefer to see a more balanced, neutral search result for a particular term, in order to get a broad overview of what's available on the App Store for that particular category. Equally, you may not be comfortable with Apple using your data to tailor App Store content, which would be understandable.

Fortunately, you can disable personalized recommendations easily by visiting your Apple ID's **Account** page. To get there, tap your profile picture in the top-right corner of the App Store app, and then touch your name. Here, a simple toggle button for Personalized Recommendations is available to switch on or off. Of course, you can re-enable the feature at any time from within the same interface.

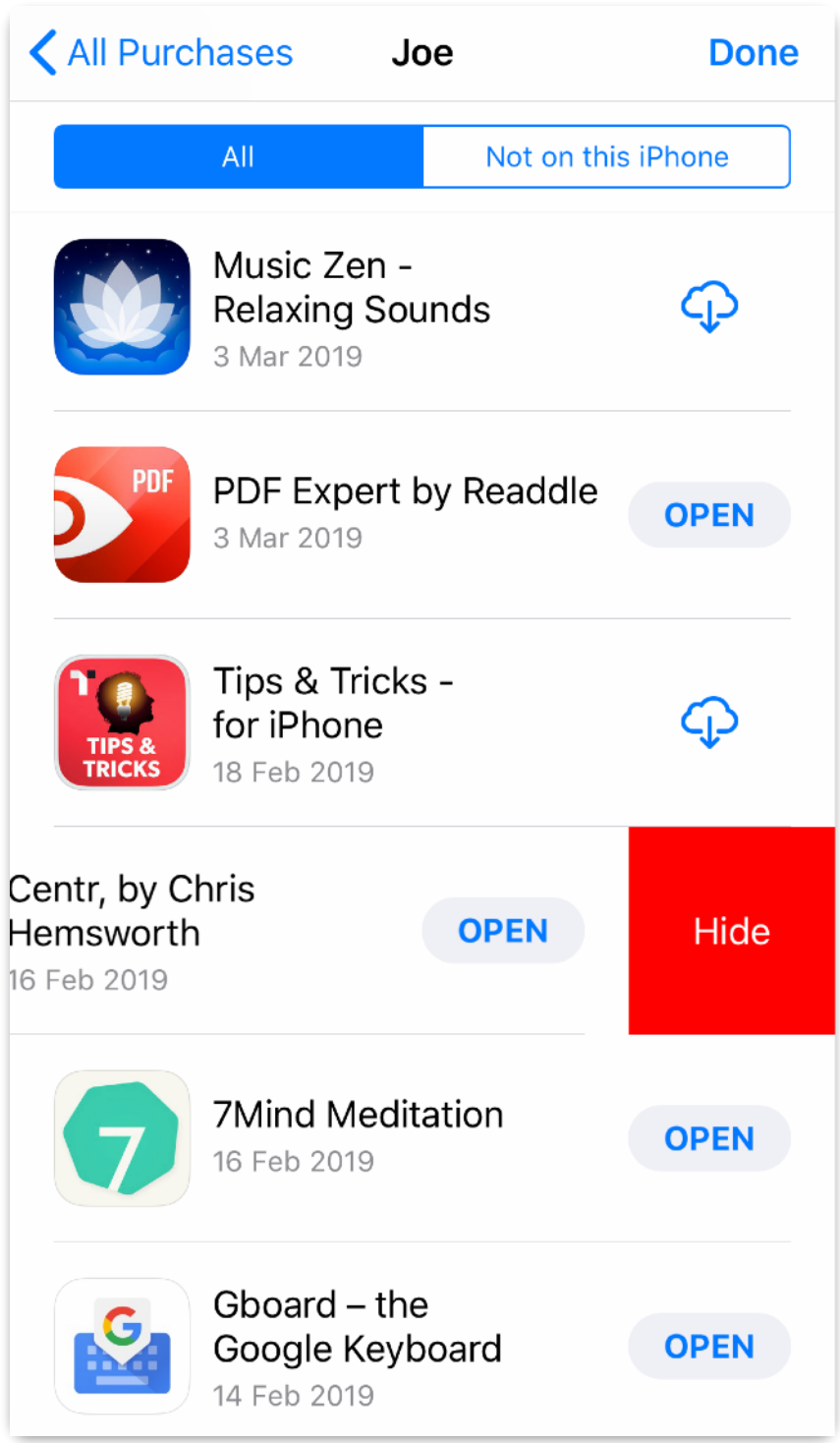
Hide your purchased apps

Did you know the App Store keeps a running and visible record of all the iOS apps you've purchased? You can find that list by launching the App Store app, tapping your profile picture in the top-right of the screen, and choosing **Purchased**. There, the

purchases of both you and individuals in your iCloud Family can be viewed in their entirety. If you've had iPhones and iPads for a long time, that list is likely to be pretty long.

To hide an iOS app from your Purchased list, simply locate the app (you can search for apps, or scroll through the entire selection), and swipe to the left on it. This will reveal a red **Hide** button, which removes the app in question from your list – it's as simple as that.

So, there you have it: two ways you can take control of user privacy within the App Store. For a more general overview of iOS privacy across a number of apps and services, we'd recommend you call by the **Privacy** section of the Settings app.



Sharing options

Protect your privacy when sharing photos

A few years ago, Apple users were introduced to a brand new share sheet. Though a little cluttered, it allows you to quickly and easily share items like photos through a variety of methods.

But one little addition is less noticeable. If you select a few photos and hit the share button, you'll see a little tappable link at the top that says **Options**. There are some

very useful things scurried away here – so let's take a look at what these settings do, and why you may want to use them.

Send as

The first option allows you to select how you may want to share the photos. By default, this is set to **Automatic**, which – when sending via **Messages** – will automatically choose the best format. This takes into account file size and number of images to get the best results.

The second choice, **Individual Photos** allows you to specify to directly send the photo files. This is the most straightforward route but can become problematic if you're sending a lot of files at once.

The third option allows you to send the photos as an **iCloud Link**. This is best used if you are sending a large number of files. The device will then upload these items to your iCloud Drive and instead of sending the photos to the recipient, it will email them a link where they can view and optionally download them. This means they can preview the pictures quickly, but download them later – handy if you're sending a large batch, or if the recipient isn't somewhere with a stable internet connection.

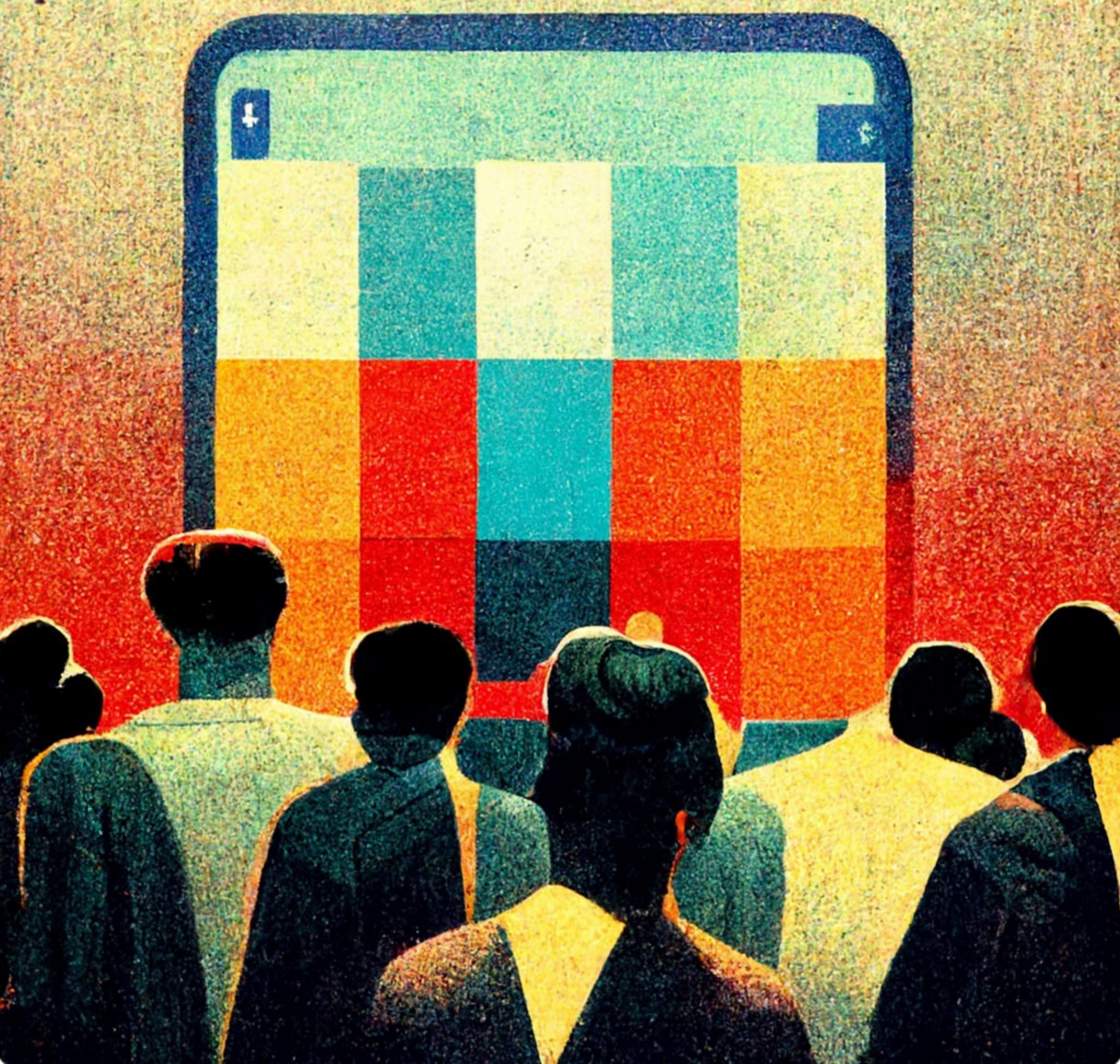
Include

This option lets you choose what to include data-wise when you send the photos. You can toggle **Location** on or off, granting you control over whether the location data captured when you took the photo is included. If you're concerned about privacy, turn this off so no one can see where the photo was taken.

The second option, **All Photos Data**, goes a step further, removing all edits and most of the metadata from the image. This option applies when using AirDrop to share the photos to another Apple device. If you choose not to send the data then it preserves the photos and any edits or crops you made so the recipient can't edit them. This gives you better control over the images. However, leaving it switched on will give you more flexibility if you want the option to edit further on another device.

CHAPTER 3

Social Media and Big Tech



Apple vs Facebook

The fight for user privacy

The battle for control over user data finds industry giants brawling once again.

Facebook isn't happy with Apple – and it's not being subtle about it. In fact, Facebook isn't being subtle to the tune of taking out full-page newspaper adverts regarding its unhappiness, writing blog posts about its displeasure, and having CEO Mark Zuckerberg slam Apple during Facebook's most recent earnings call. There are even threats of a lawsuit – but why? It all comes down to privacy – and how everything shakes out will have big ramifications for your own personal user data well into the future.

The gripe stems from a promise Apple made at its developer conference last summer. In short, it would introduce and mandate app tracking transparency. This would require every app to secure someone's permission before it was allowed to track their data across apps and websites owned by other companies. Within the Settings app, people would be able to check which apps have requested such permissions, and make changes as they see fit. This would make tracking "transparent and under your control."

This was all supposed to happen with the release of iOS 14, but Apple delayed the feature's rollout, to give companies more time to prepare. It's now imminent, arriving as part of iOS 14.5, hence Facebook's urgency to lob a spanner into the works and hope Apple will think different.

Facebook's argument is a curious one though. It seeks to frame Apple as having an unfair advantage through forcing third-party apps to gain user consent for tracking, when that won't apply to Apple's own apps. However, Facebook omits the fairly important point that Apple products don't use this kind of tracking in the first place.

Zuckerberg also reportedly said of Apple: "They say they are doing this to help people, but the moves clearly track their competitive interests." This doesn't help

Facebook as much as he thinks it does, because both statements are true.
Apple *is* doing this to help people, and it *does* track with the company's competitive interests. It just so happens those interests are markedly different from Facebook's.

All this is starkly outlined in an Apple white paper (PDF) that tells the story of a dad and his daughter on a nice day out. Beneath the fun bits – time at the park; playing a game on a phone; taking a selfie; buying ice cream – there is a parallel dystopian tale being told about data being recorded and sold to third parties eager to send precise, targeted advertising the family's way. Facebook succeeds when few protections are in place, cementing its dominance of online activity. It can then better leverage people's dependence on the reach of its social network, and the reliance businesses have of successfully advertising to users through Facebook advertising. Apple, by contrast, has defined *privacy* as a differentiator and key interest, wanting to at the very least provide individuals with the means to understand how and why they are being tracked – and to do something about it.

Ultimately, this all comes down to mindsets. Do you, as an individual, prefer to be aware of when your personal data – location; purchases; interests – about you is being collected and shared, and be able to opt in or opt out? If so, you should be Team Apple in this fight.

App tracking transparency

What's up with these privacy changes?

With iOS 14.5, Apple finally released a privacy feature it has been talking about for months: App Tracking Transparency. In the simplest terms, this allows users to choose whether or not to be tracked. Developers will now have to request permission in order to do things like showing targeted adverts in their apps.

For users, it's hard to see a downside – apart from yet another annoying permission pop-up when you install a new app. But companies with very lucrative targeted ad networks (Facebook, Google, etc) aren't so keen, as it means anyone who opts out will have to be shown un-targeted ads instead – which those companies can't charge as much for. Facebook argues that small businesses may suffer, as they rely on targeted ads to find new customers.

There's also the question of whether the change will benefit Apple's own (much smaller) ads business, as by default it retains the ability to serve targeted ads in a much more limited capacity. Apple doesn't collect user data for targeting in the same way those other companies do, but if you were advertising an app via an App Store Search ad, for example, you would still be able to target based on some basic factors like the device used and what apps the person already has installed.

Overall it's a mixed bag as far as corporate interests go, but good news for consumers.

How it works

If you have iOS 14.5, you'll start to see pop-ups in apps that rely on advertising asking for your permission to track some of your information in order to serve you targeted ads.

Developers are allowed to display a splash screen explaining why they wish to access the tracking data, and if that's enough to convince you, you can simply agree to the terms and things will continue as usual within that app.

If you don't want to be tracked, you can decline permission from the pop-up. This won't remove ads from the app, but you'll start seeing generic ads instead of those targeted to your interests or demographic.

Note that Apple does not allow developers to incentivize granting permission – they can't offer you in-app or monetary rewards for saying yes. Any devs who try this will get their apps booted from the App Store.

If you don't want to be tracked by **anyone** and all those pop-ups sound annoying, you can make a blanket decision and turn of all tracking. Head to the **Settings** app and choose **Privacy** > **Tracking** > **Allow Apps to Request to Track**.

Facebook privacy

A simple guide to basic privacy

Facebook has been experiencing a particularly tough time of late when it comes to the transparency of its privacy settings, but for the majority of us, the concerns are simple. Here's a straightforward guide to basic Facebook privacy: who can find me, and who can see what I post?

How to customize who can find you on Facebook

The more visible you are on Facebook, the more likely it is that your data can be used by third parties. Follow these steps to select how public your profile is:

1. In the **Facebook** app, tap the **menu** tab in the bottom right corner.

2. Scroll down and tap **Settings**.

3. On the pop-up menu tap **Account Settings**.

4. Then tap **Public posts** near the bottom.

Here, you can decide whether your profile is entirely public or available only to friends, who can post public comments or interact with you on your profile.

How to customize who can see your posts on Facebook

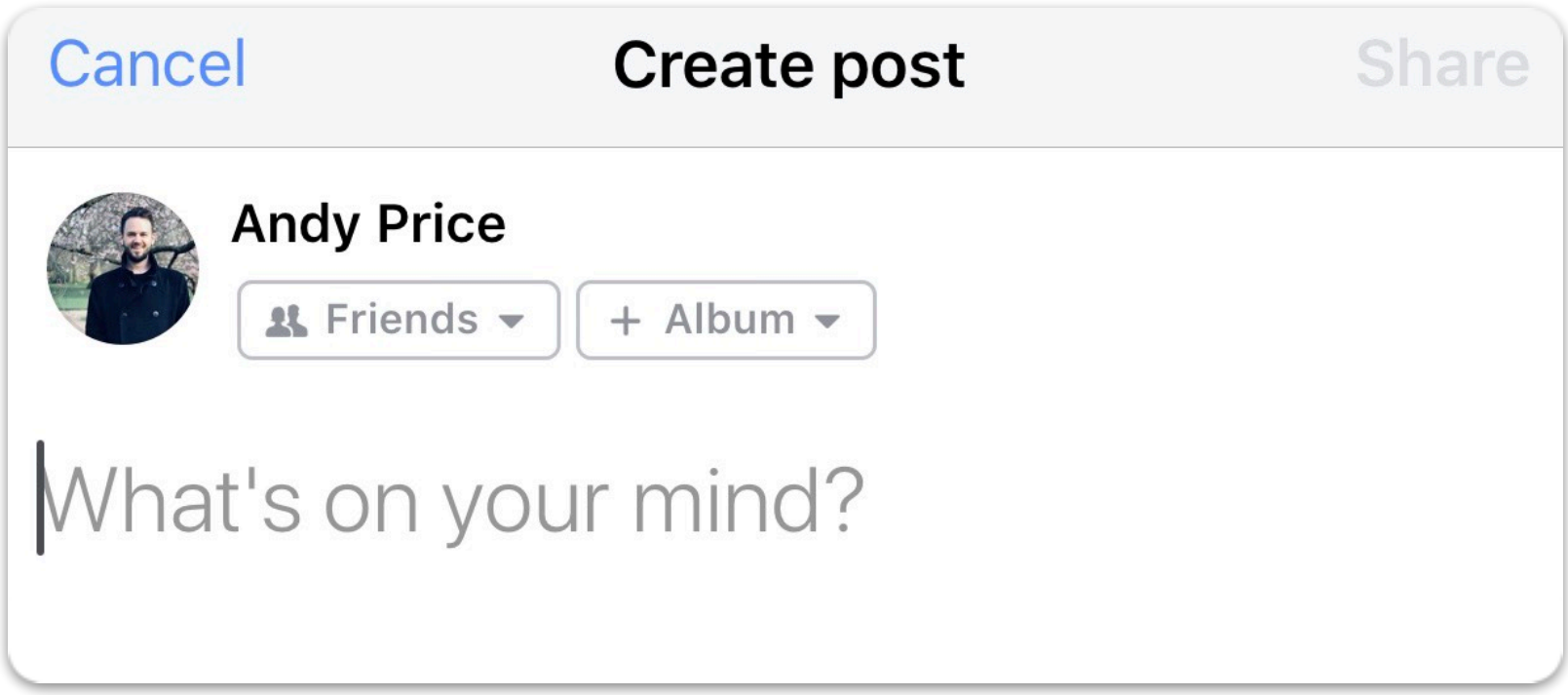
Here's how to customize who can see each and every post you make:

1. Tap on the box at the top of your newsfeed that says **What's on your mind?** This will take you to the screen where you can make a post.

2. Under your name, tap on the left-hand box which displays your current settings. This will give you the option to customize – from just yourself, to entirely public, or you can choose "Friends except" which you can use to add individuals that you never want to see your posts.

3. Once you've tapped on an option, tap **Done**.

4. This setting will be used for this post, and automatically applied to all future posts until you manually change it.



If you're concerned about who can see your past posts, it's easy to go back through your updates and edit who can see them by. Simply tap the three dots in the top right of an individual post and tap **Edit post** and follow the instructions above.

How to customize who can tag you on Facebook

Facebook allows other users to tag you in photos and posts by default. But it's possible to customize who is able to do this, and whether you wish to review these tags before having them appear on your profile. Here's how:

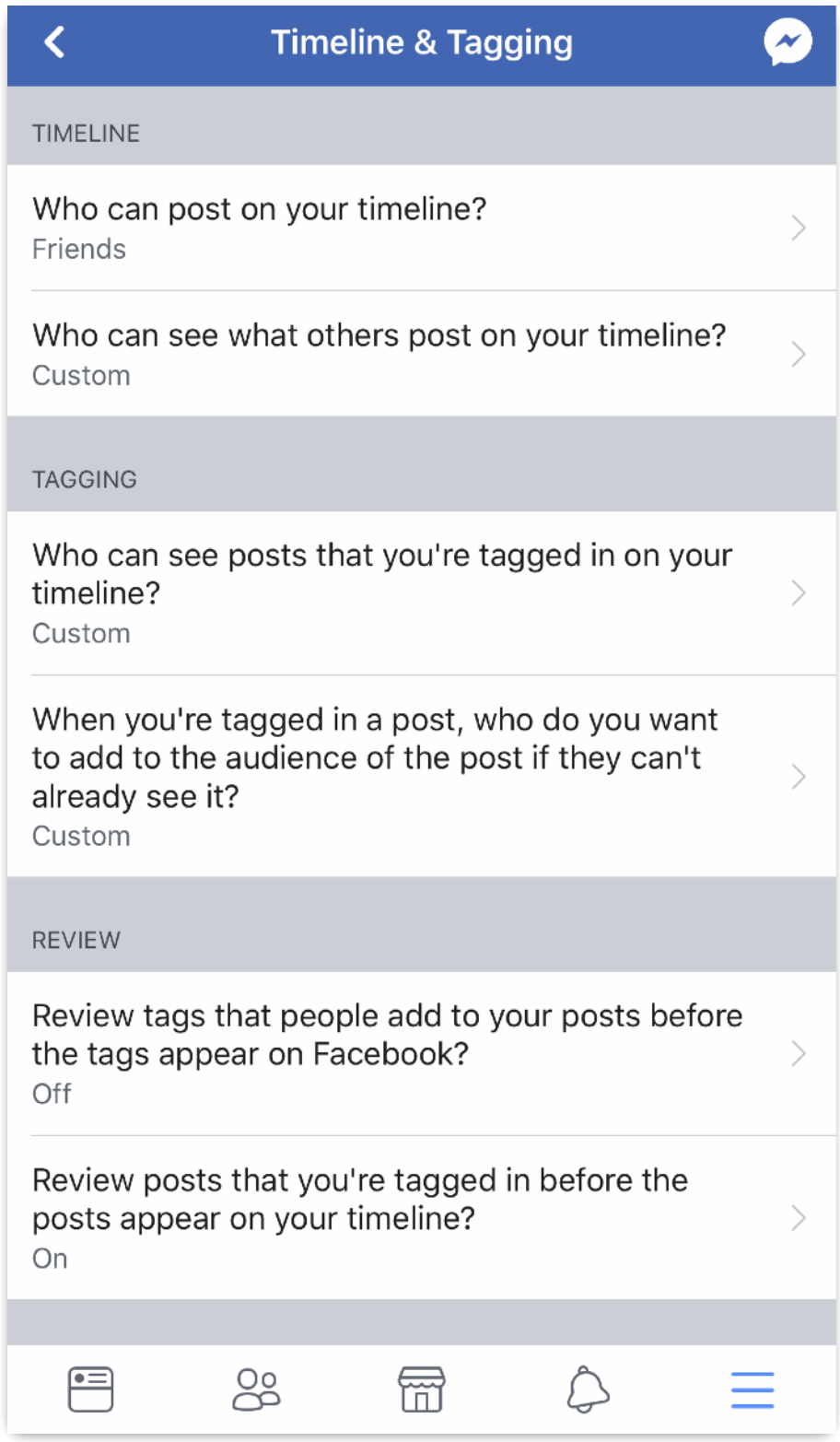
1. Tap the **menu** icon in the bottom right corner.

2. Scroll down and tap **Settings**.

3. On the pop-up menu tap **Account Settings**.

4. Tap **Timeline and Tagging** – the fourth option down.

5. Review the various tagging options and tap on one to customize.



Each option gives you the same choices as other levels of privacy when it comes to tagging so you can select whether you want these tags to be public, viewable only by friends, or by certain people.

Under the review section, you can also turn on the option to review tags before they appear on Facebook. This means they won't be viewable until you accept them. If you turn this on you'll receive a notification when someone tags you which you can then tap on and select whether to accept the tag or not.

Amazon privacy

How to clear your browsing history

Amazon sells a lot of great stuff, and if you use the shopping service you'll notice it gradually gets to know you based on your browsing activity. If you've ever opened the app to the "your recommendations" section, you'll know that Amazon not only keeps track of your purchases but also every product you've ever so much as glanced at.

These recommendations can often be genuinely helpful, highlighting interesting products you wouldn't otherwise have thought to search for. But there are plenty of reasons you might not want Amazon tracking your every online interest.

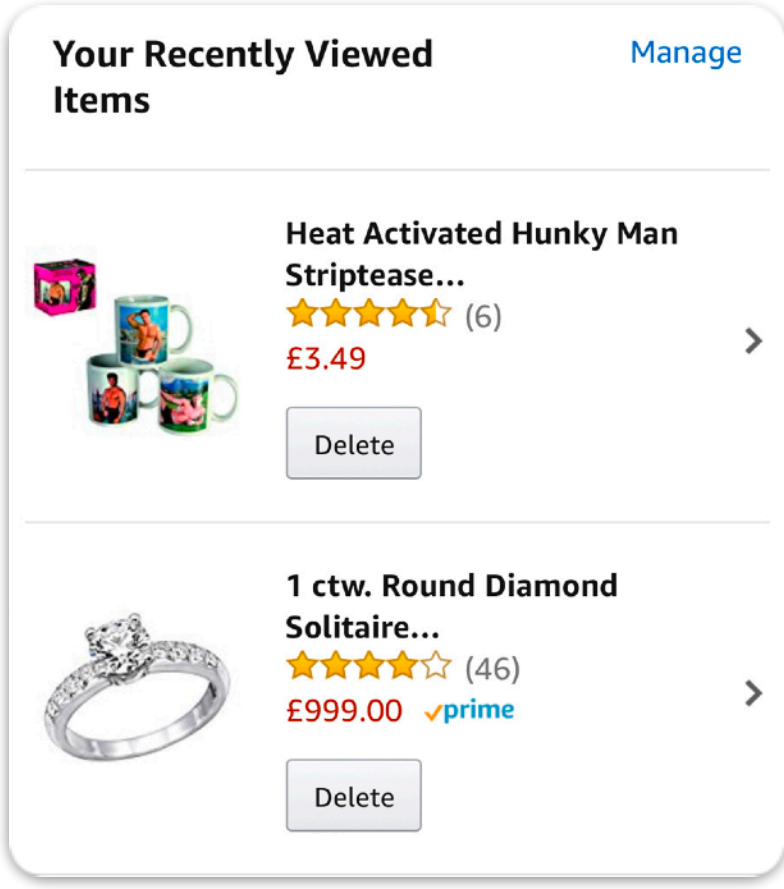
Maybe you've been looking for a surprise gift and don't want your significant other to find out. Maybe you're sick of seeing targeted ads based on your browsing history. Or maybe your recommendations have been out of whack ever since you clicked on that weird product link in a *Buzzfeed* article.

Whatever the reason, you'll be pleased to know that Amazon allows users to delete items from their personal history. Here's how to do it.

Browsing history

Amazon keeps track of everything you look at, whether you buy it or not. Though you can't dig into a historical archive of everything you've ever viewed, it's pretty straightforward to take a look at a list of recently viewed items and remove any or all of them.

In the Amazon app for iPhone and iPadOS, tap the "three-lines" menu icon in the bottom right of the screen and select **Your Account**.



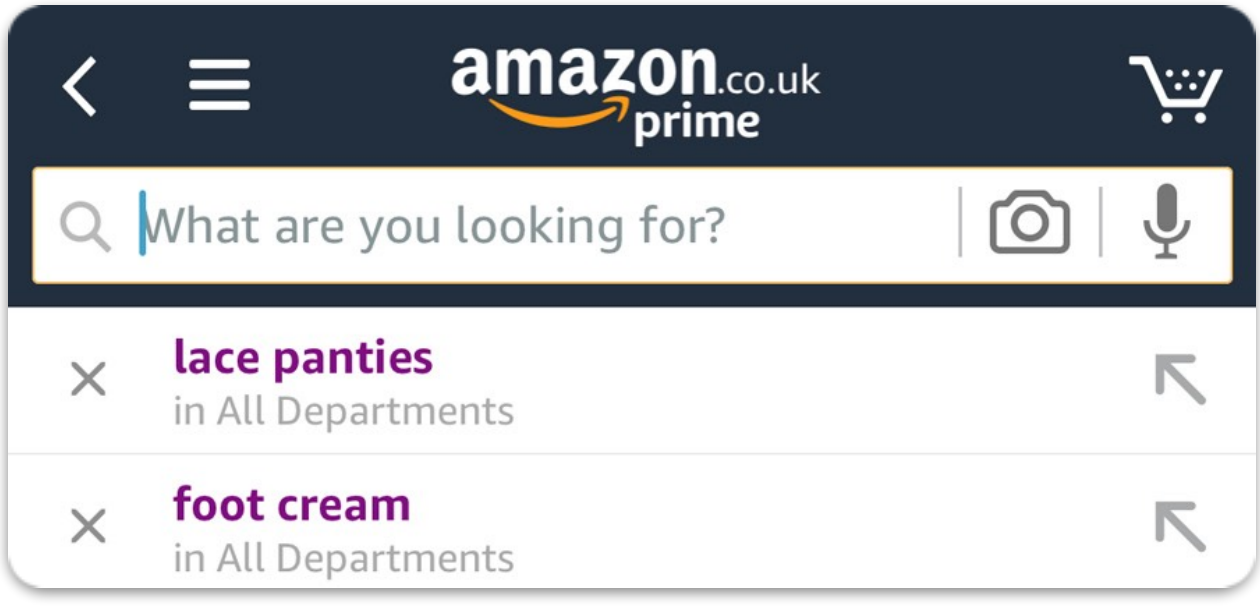
From the next menu, choose **Your Recently Viewed Items**. Here, you can press the **Remove from view** button to delete individual items from your history.

Alternatively, you can press **Manage** in the top right and then **Delete History** to remove everything from this list in one fell swoop. You'll also see the option to toggle off the browsing history feature altogether, so it won't keep track of future product views.

Delete saved searches

On top of the browsing history itself, you may want to remove any record of past searches. To do this from the app, simply tap into the "what are you looking for?" search box at the top.

You'll see a chronological list of recent searches; press the **X** to the left of any entry to delete it.



Multiple devices

It's worth noting that Amazon's recently viewed items and search history are unique to each device you browse Amazon on. If you use the app on an iPhone and an iPad, for example, you'll need to follow the above steps twice – once for each device.

Similarly, you'll need to manage your histories on any computer that you're logged into Amazon on. On the computer, go to Amazon's website and press **Your Amazon** from the top menu. You'll then see a **Your Browsing History** option from a sub-menu, from which you can delete items in much the same way as described above.

Alexa privacy

How to stop Amazon listening in on you

A new report from Bloomberg claims that "thousands of people around the world" are paid to listen in to recordings from Alexa-powered devices like the Amazon Echo.

"The Alexa voice review process, described by seven people who have worked on the program, highlights the often-overlooked human role in training software algorithms. In marketing materials Amazon says Alexa 'lives in the cloud and is always getting smarter.' But like many software tools built to learn from experience, humans are doing some of the teaching."

This should not be a huge reveal. Anyone paying attention to the small print in the Alexa app will have known this for a while, and both Google and Apple use similar practices to improve their own voice-recognition software. Having a human listen to audio and provide feedback to the system can be invaluable in making these features more reliable, but it does raise some ethical concerns.

Both Google and Apple take the effort to completely anonymize any stored chunks of audio. In contrast – and somewhat worryingly – it seems as though Amazon doesn't strip away all the identifying data from its recordings. Most details are removed before the clips are given over to a human, but according to the report, first names and account numbers remain intact.

Luckily, if you own an Alexa-powered device and this makes you feel at all uneasy, you can withdraw consent to block Amazon using your recordings. The setting is rather difficult to find, but we've got your back.

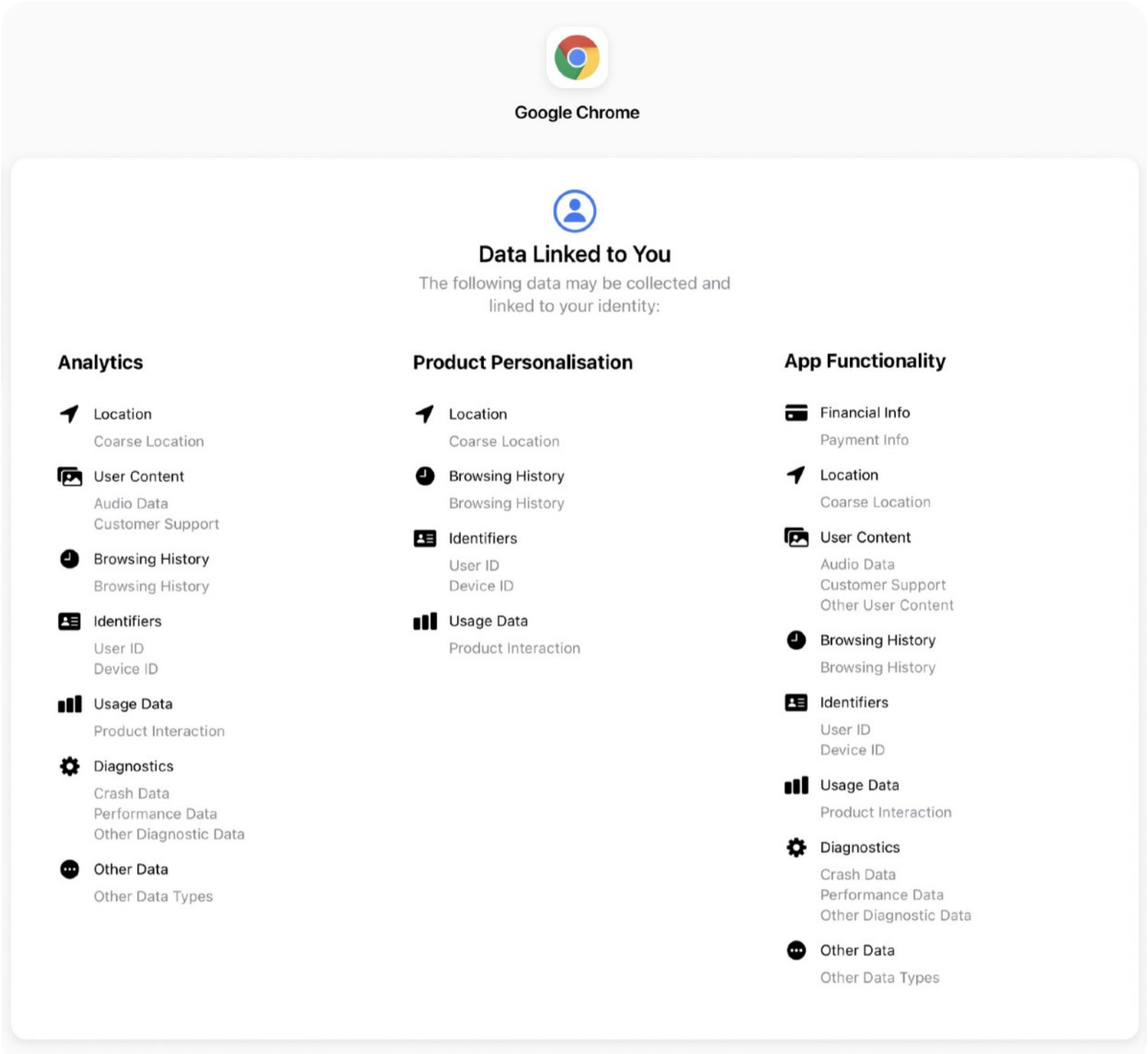
Open the **Alexa** app on your device and tap **Settings** from the main menu. Next, choose **Alexa Account** followed by **Alexa Privacy**. Finally, tap **Manage How Your Data Improves Alexa** and switch off the two settings here. Phew. How about making things a bit clearer in the future, Amazon?

Browser privacy

DuckDuckGo criticizes Google ‘spying’

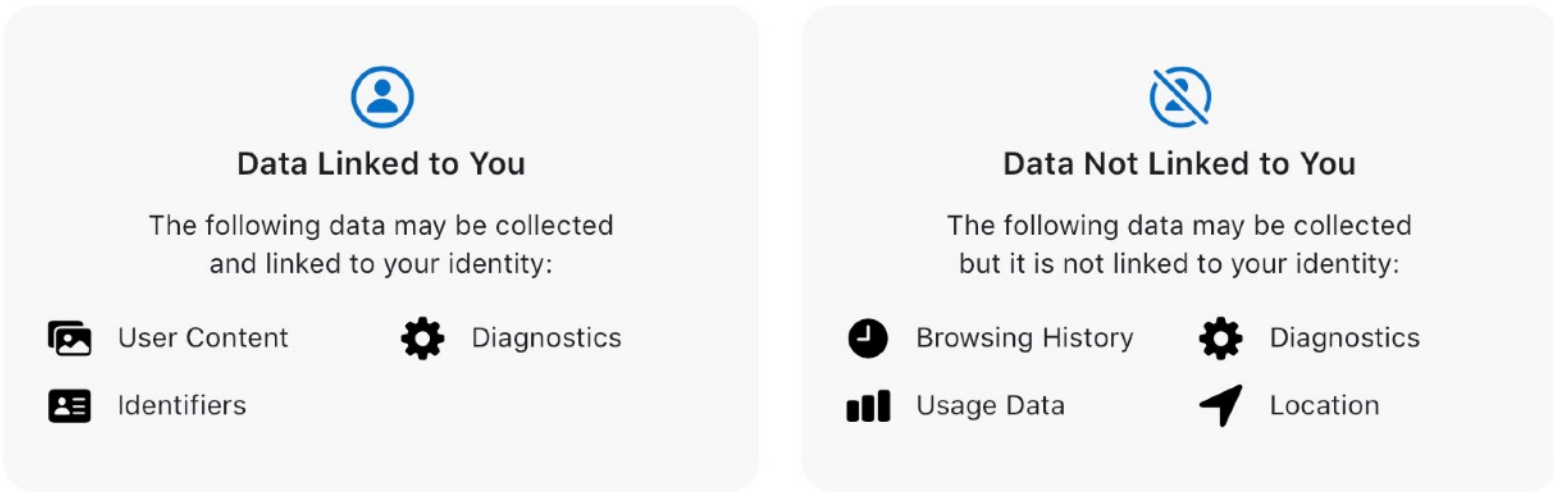
Google has finally updated its iOS apps to comply with Apple’s iOS 14 privacy changes, prompting rival browsers to scoff at just how much personal information Google requires from users.

Last year, Apple made it mandatory for developers to fill out a ‘Data Linked to You’ section on the App Store page for their apps, to give users a transparent look at what sort of data is collected or used for a given service. Google dragged its heels updating its apps to show this information almost right up until Apple’s deadline, which critics have said proves it had something to hide.



Certainly, the long list of permissions Google's apps require makes for worrying reading. You can scroll through this data in full for Google Chrome, Google Search, or indeed any app by scrolling to the bottom of its App Store page.

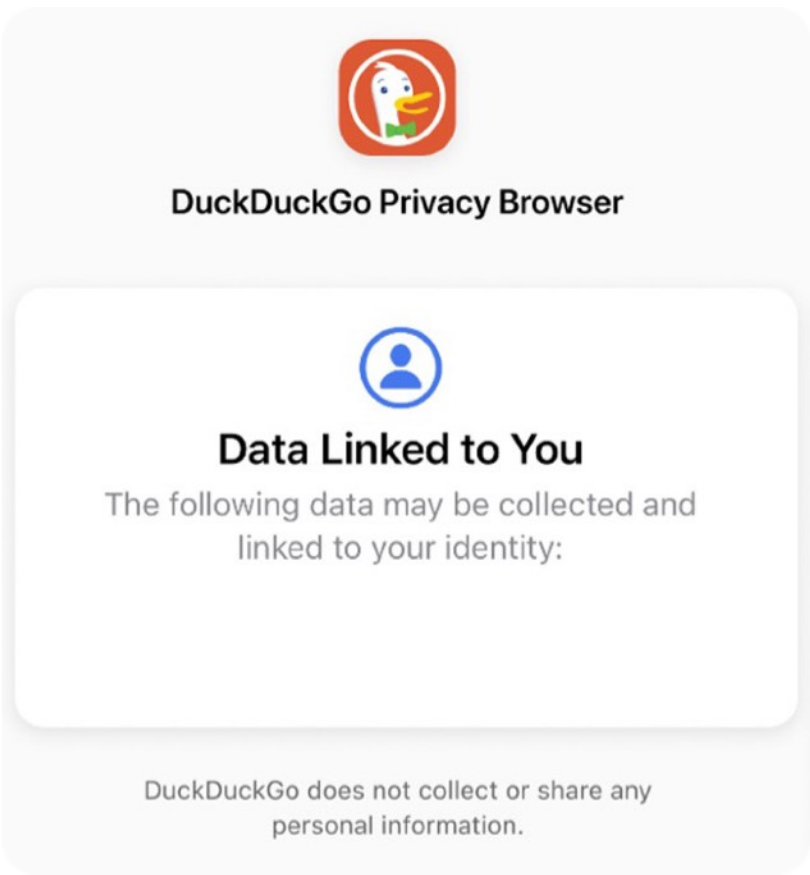
For Apple's built-in apps like Photos and Safari, which aren't listed on the App Store, you can visit Apple's privacy microsite to see the same app transparency data. Considering Apple's stance on privacy, it's no surprise to see that Safari asks for a lot less from users – and that it anonymizes data where possible.



With that in mind, privacy-first search engine DuckDuckGo has fired shots at Google in a tweet, saying "spying on users has nothing to do with building a great web browser or search engine." By comparison, its own web browser requires a total of zero permissions to operate. Even better than Safari.

Of course, that's a biased and slightly unfair comparison. Google and Apple offer plenty of features DuckDuckGo doesn't, many of which would be literally impossible without the requisite data. Most of these are optional.

But for those who aren't comfortable sharing so much personal data, it's another reminder that alternative browsers and search engines do exist – and we've got an in-depth roundup of the best in the biz coming up in the next few weeks, so stick around!



Good security PSA

Why you should use two-factor authentication

We often recommend setting up two-factor authentication to protect your Apple ID. It's simple to set up and helps to safeguard your account details against thieves and hackers.

That's all well and good for any details stored with Apple, but if you use any of Google's services you'll want to take similar precautions with that account. Any of your personal details stored with Apple or Google are accessible to anyone who knows your email and password – until you enable this type of added security, that is, which requires physical access to one of your secure devices in addition to login credentials.

Anyone who routinely uses any apps like Gmail, Google Docs, Google Maps, or Google Photos should take steps to lock down their account. When you consider that Google owns YouTube and knows all your web searches, it becomes even more important – doubly so if you've ever tied up your bank details to a Google-owned service. That's a lot of information on the line if your account gets hacked.

Which is why it's surprising to learn that less than 10% of Gmail users have two-step verification enabled. Which means there's around a nine-in-ten chance that you haven't set it up yet, either. Luckily, that's easy to remedy. Just head to Google's security website and press **Get Started**. While you're at it, make sure you have 2-FA enabled for your Apple ID, too!

The only real downside to setting this up is that you'll be occasionally asked to enter a verification code when logging in, to prove it's really you. (The code will be sent to your registered device.) Small price to pay for extra peace of mind, we think, but if you value convenience much more than security then you might decide to go without. Your call!

Thank you for reading!

If you enjoyed this book, try our free app for more great iPhone advice, plus daily news, reviews, and how-tos.

Tips & Tricks for iPhone

Download on the App Store