All the Ways Facebook Tracks You—and How to Limit It

David Nield

It won't come as much of a surprise that Facebook tracks you on its platform—that's why it can resurface your birthday photos from five years ago—but you might not yet realize the scope and the depth of its tracking all across the internet. Facebook's tentacles stretch out across other websites and services, into the various apps you're using on your phone, and to the places you physically visit in the real world—especially if you decide to check in on Facebook while you're there.

Some of this comes with the territory of using Facebook: If you want to take advantage of its features, then you have to give up a certain amount of information about yourself. But Facebook has ways of keeping tabs on people who aren't even signed up for the service. Fortunately, there are numerous ways to limit the volume of data that it logs.

How hard you want to pull back depends to a certain extent on how much you trust Facebook. The social network behemoth says it uses your data to show relevant ads and keep you safe; if someone signs into your account from a country you're not usually in, for instance, Facebook can flag the activity as suspicious.

However, this is not a company with a good track record when it comes to looking after your data. Irrespective of how Facebook itself has used your information, it's certainly been careless in the ways that information has been shared with third parties.

To make matters more complicated, Facebook owns WhatsApp and Instagram too, and can pool some of the information it gathers in those apps as well. The best way to limit Facebook's tracking is to quit all three apps for good. If that's too extreme for you, we've got some more suggestions.

For reference, the Facebook data policy is here, and you can read a more user-friendly explainer on how your data is handled here.

On the Web

Courtesy of Facebook

If you want to use Facebook, you give it permission to log your activity on the site: where you check into, the groups you join, who you interact with. This data is primarily used to serve up advertising that's more relevant to you, which in turn makes more money for Facebook.

You can't really stop Facebook from collecting this information—it's the deal you make when you sign up—but you can limit how it affects the advertising you see by visiting the ad preferences page in your account on the web. Open up **Your interests** to get a quick glance at what Facebook thinks you're into. It might have made some assumptions that are well wide of the mark.

Under the **Your information** tab, you can see some of the ways Facebook is targeting advertising at you: your relationship status, your job title, where you went to college, and more. If you don't want some or all of these pieces of information to be used by advertisers, hit the relevant toggle switch.

Open up **Ad settings** to make even more changes. Here you can control whether Facebook can use data from its marketing partners—and there are an awful lot of them—to put more relevant advertising in front of you. If you don't want this to happen, switch the setting from **Allowed** to **Not allowed**.

Bear in mind that these settings don't reduce the number of advertisements you see on Facebook, nor do they delete the data that Facebook has amassed on you. They just stop advertisers from specifically targeting you using that data. If you're happily married, you might suddenly start seeing ads for dating sites, but Facebook itself will still know your relationship status.

Facebook's reach also goes way beyond Facebook itself. It has partnerships with a whole host of marketing firms and ad networks so that activities on other sites—including but not limited to logging into a third-party service with your Facebook account—can be combined with your Facebook profile.

This activity has attracted enough bad press that Facebook announced a tool in August called "Off-Facebook Activity" that will disconnect this data from what you actually do on Facebook. It's a more comprehensive solution, but still not widely available. It also still doesn't affect how much data Facebook actually *collects*, it just breaks the association between what you do on Facebook and off it. If you're shopping for shoes on a third-party retail site, you won't suddenly see ads for them all over your News Feed.

Courtesy of Facebook

This off-Facebook activity is also monitored whether or not you have a Facebook account. Tracking tools like the Facebook Pixel enable websites and online retailers to get information about their visitors, including whether they come back. A vast number of third parties are using Facebook's advertising and tracking technologies, which means it isn't just Facebook you need to worry about.

Site owners are able to build up a profile of who is visiting their pages, and Facebook collects even more data about what people are shopping for and looking at on the web. If that data can be added to a Facebook profile so much the better for Facebook, but the social network can still use in general terms to analyze aggregated user behavior.

More broadly, you can stop some of the web activity being used to target you with ads by visiting the YourAdChoices site run by the Digital Advertising Alliance. You'll notice Facebook advertising targeting is on the list of entries—tick the **Opt Out** box to do just that. Note that you'll need to do this separately for each browser you use; for the biggest impact, you should opt out of all the other platforms as well.

Locking down tracking in your browser is also recommended: Look out for the option to block third-party cookies in your browser settings (the sort that can track activity across multiple

sites), and consider using well-respected tracker blocking browser extensions such as Ghostery or Privacy Badger.

On Mobile Devices

Courtesy of Facebook

Much of what we've already said applies to Facebook's mobile apps as well. If you want to limit what Facebook knows about you, you're best off not installing the mobile apps at all. Doing so gives Facebook permission to log the Wi-Fi networks you connect to, the type of phone you have, the other apps you have installed, and more besides, as well as everything you do on Facebook itself.

You can't stop all of this data collection, but you can curb it. Head to the Facebook permissions page—under **Apps and notifications** and **Facebook** in Android settings and under **Facebook** in iOS settings—to block Facebook's access to your phone's location, your contacts, your phone's microphone and camera, and more.

The bad news? Even with location tracking turned off, Facebook still makes note of the approximate location that you access the web from via your IP address. It's only a rough guide—and Facebook says it's necessary to keep accounts secure and users verified—but you can't stop this from happening if you use Facebook.

More bad news: Other apps send data to Facebook as well, often automatically. Almost everyone has a Facebook account, and third-party apps want to make use of that data, whether it's to target users with advertising or to simplify the login process and get more user data as a result. Facebook isn't working in isolation here, and has many profitable partnerships with other apps and data brokers.

It's worth emphasizing that Facebook, like Google, promises to use this treasure trove of data to improve its services and make life safer and more convenient for its users, as well as generating more profitable ads across its network. You are, after all, using everything Facebook offers for free. If you don't trust Facebook's intentions—which is by now understandable—then you really need to quit using it altogether.

If you're going to stay with it, limit your activity and become a social media lurker. Don't check into locations, don't tag photos, and don't fill out quizzes that tell you which Disney character you are. Keep your profile information down to a minimum, and think twice about sharing anything at all. On the phone, consider using Facebook on the mobile web instead of in the app.

Courtesy of Facebook

Keep the apps you've connected to Facebook down to a minimum as well; you can find a list on the web here. Not only does this restrict the third parties who have access to your data, it's also a good idea from a security point of view, limiting the number of ways hackers could potentially get at your data.

Facebook knows full well that users are uneasy about its data collection policies, and is trying

to push out tools that ostensibly offer more control. In reality, these don't do much in regards to data collection, and are more about how that data is used to personalize ads. At this stage, if you don't want Facebook to know a lot about you, you really need to close down your Facebook, Instagram, and WhatsApp accounts and not look back.

More general privacy tips can slow down Facebook, too: Use a VPN to disguise your location, lock down your browser's privacy settings so you're not tracked so extensively by marketers, and make liberal use of your browser's incognito mode wherever you can. Ultimately though, using Facebook comes with a cost, even if it's not paid up front in dollars and cents.
