TECH FIX

The Default Tech Settings You Should Turn Off Right Away

These controls, which are buried inside products from Apple, Google, Meta and others, make us share more data than we need to.

By Brian X. Chen

Published July 27, 2022 Updated July 29, 2022

There's a catchy saying going around with a valuable lesson about our personal technology: The devil is in the defaults.

The saying refers to the default settings that tech companies embed deep in the devices, apps and websites we use. These settings typically make us share data about our activities and location. We can usually opt out of this data collection, but the companies make the menus and buttons hard to notice, likely in the hope that we don't immediately tweak them.

Apple, Google, Amazon, Meta and Microsoft generally want us to leave some default settings on, purportedly to train their algorithms and catch bugs, which then make their products easier for us to use. But unnecessary data sharing isn't always in our best interest.

Consider how several whistle-blowers confessed in 2018 that they had listened in on Apple's Siri recordings and Amazon's Alexa activations that inadvertently recorded couples having sex. The recent reversal of Roe v. Wade also underscored the many ways that women can be tracked through their personal tech when seeking options to terminate pregnancies.

So with every tech product we use, it's important to take time to peruse the many menus, buttons and switches to pare down the data we share. Here's a streamlined guide to many of the default settings that I and other tech writers always change.

Apple Phones

With iPhones, users can open the settings app and enter the privacy menu to change how they share data about their app use and location. (Apple technically asks people to opt in to some of these settings when they activate a new iPhone, but these steps can easily be missed. These tips would disable the data sharing.)

- Select Tracking and toggle off Allow Apps to Request to Track. This tells all apps to not share data with third parties for marketing purposes.
- Select Apple Advertising and toggle off Personalized Ads so that Apple can't use information about you to serve targeted ads on its App Store, Apple News and Stocks.
- Select Analytics & Improvements and toggle off Share iPhone Analytics to prevent the iPhone from sending device data to Apple to improve its products.
- Select Location Services, tap System Services and toggle off iPhone Analytics and Routing & Traffic to prevent the device from sharing geodata with Apple for improving Apple Maps.

Google Products

Google products, including Android phones and web services like Google search, YouTube and Google Maps, are tied to Google accounts, and the control panel for tweaking data management is on the website myactivity.google.com.

- For all three categories — Web & App Activity, Location History and YouTube History — set auto-delete to delete activity older than three months. This way, instead of creating a permanent record of every search, Google purges entries that are more than 90 days old. In the near term, it can still make helpful recommendations based on recent searches.
- A bonus tip for Android phones comes from Ryne Hager, an editor of the tech blog "Android Police": Newer versions of Android offer people the ability to share an approximate location rather than their precise location with apps. For many apps, like weather software, sharing approximate data should be the way to go, and precise geodata should be shared only with software that needs it to work properly, like maps apps.

Meta's Facebook

Meta's most important settings can be reached through the privacy checkup tool inside the settings menu. These are some important tweaks to prevent snooping by employers and marketers:

- For "Who can see what you share," select "Only me" for people with access to your friends list and pages you follow, and select "Friends" for who can see your birthday.
- For "How people can find you on Facebook," choose "Only me" for people who can look you up via email or phone number.
- For "Your ad preferences on Facebook," toggle off the switches for relationship status, employer, job title and education. This way, marketers can't serve targeted ads based on this information.

Amazon's Website and Devices

Amazon offers some control over how information is shared through its website and products like Alexa and Ring cameras. There are two settings that I highly recommend turning off:

- Amazon last year launched Amazon Sidewalk, a program that automatically makes newer Amazon products share internet connections with other devices nearby. Critics say Sidewalk could open doors for bad actors to gain access to people's data.

  To disable it for an Echo speaker, open the Amazon Alexa app and tap More in the lower right-hand side of the screen. Inside the settings, tap Account Settings, choose Amazon Sidewalk and toggle Sidewalk to the off position.

  For a Ring camera, in the Ring app, tap the three-lined icon in the upper left and then tap Control Center. Tap Amazon Sidewalk, and slide the button to the off position.
- On Amazon's website, some shopping lists — like items saved on a wish list — are shared with the public by default, which can be revealing information. Visit the Your Lists page and set each shopping list to private.

Microsoft Windows

Windows PCs come with a host of data-sharing settings turned on by default to help Microsoft, advertisers and websites learn more about us. The switches to toggle those settings off can be found by opening the settings menu and clicking on Privacy and security and then General.

Yet the worst default setting on Windows may have nothing to do with privacy. Whenever Kimber Streams, a Wirecutter editor, tests new laptops, one of their first steps is to open the sound menu and select No Sounds to mute the many annoying chimes that play whenever something goes wrong with Windows.