Four Ways to Keep Your Phone from Spying on You

It felt like we had a spy in the office.

My two assistants chatted the other day about artificial sugar replacements. A few minutes later, one of their smartphones lit up. It was an ad from her Amazon app saying there was a sale on bags of erythritol sugar replacement.

It likely wasn't a coincidence. She'd never purchased any sugar replacement before.

If it sounds like her phone was listening to her... it was.

In a recent investigative piece from Vice, Dr. Peter Henway discussed why this happens. He's a cybersecurity expert who teaches at Edith Cowan University in Australia. According to him, your phone does record "snippets" of audio. This data only stays on your phone, instead of reaching the Internet... but there's a catch. Your apps access your phone's information, including any of this data. Think about all the applications you have on your phone – Facebook, Google, Amazon, Target... They're all convenient. But they all want your data, so they can target ads to you.

In other words, you could talk about wanting to go to Peru this fall and your Kayak app could start sending you ads for flights to Lima.

The scary part is that we don't know when or why our phones suddenly listen to our conversations. Since all the data become encrypted, it's difficult to pinpoint the "trigger." That could be anything from a word or phrase to your phone sensing your location (if you're close to Target, you could get ads for Target).

All of this Big Brother stuff put a sour taste in our mouths. Whatever happened to privacy?

That's why we spent some time looking into ways to secure our phones and take back some of our privacy. Here are four things you should do immediately if you have a smartphone...

1. **Turn off your microphone**. Many of the apps in your phone (including Amazon's shopping app) ask for permissions when you sign up. If you just blindly agree, you're giving them access to your microphone.

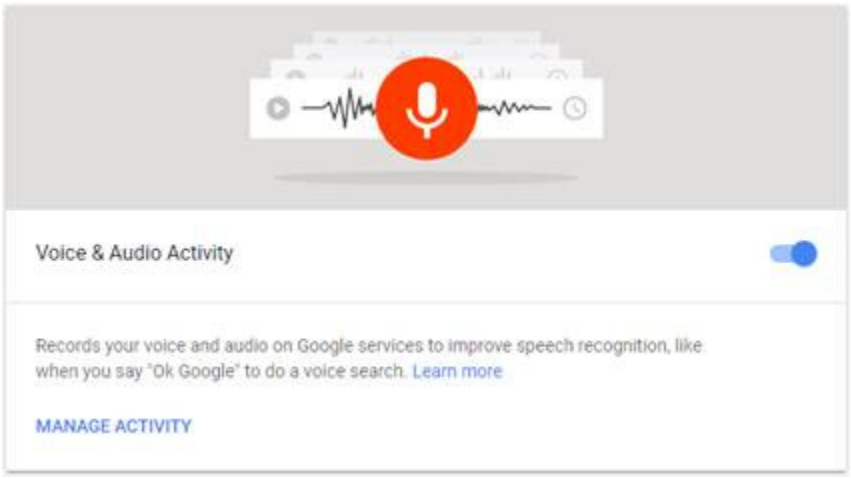
But it's easy to turn this off. If you have an Android, go to your Settings screen, then select Apps. You should see a menu where you can select App Permissions. Once there, tap on Microphone and you'll see all your apps with toggle buttons. These allow you to turn access on or off for each one. If you have trouble finding this screen, you can also search your phone for App Permissions and you should be able to find it.

For iPhones, you'll go to the Settings app and select Privacy. You can see the permissions by type, including microphone. From there you can see all the apps and control which ones have access. For a more detailed write-up, check out this how-to guide from *Popular Science*.

Remember, none of these are final. If you want to use your voice to search online for something, you can switch the microphone back on. But be careful, because all those searches stay recorded in your account...

2. **Delete your voice logs**. If you've ever used the voice commands on your smartphone (or on Google's Home Assistant), the device records and stores your voice. My researcher discovered this while writing this article. Not only did Google have a log of all her voice command searches (typically cooking questions asked while preparing dinner), it also had playable audio clips of her voice asking these questions.

To see what's stored about you, go to your Google Account, then click My Activity. On the left you should see Activity Controls. On this page you'll see Voice & Audio Activity. Go in and listen to everything Google's recorded and saved. Delete all or as much as you want. Go one step further and turn off all Voice and Audio Activity under the Activity Controls main page. It looks like this (just click that blue toggle button on the right to turn it off):



Siri on the iPhone also records your history, but it's a bit easier to clear. Simply go to Settings, select Safari, and Clear History. You can also deactivate Siri to avoid future recordings, but it's a bit more complicated. You can read more on how to do that right here.

3. **Stop your phone from tracking you**. If you have a smartphone, chances are that a store you visit is monitoring your every move via your phone's media access control (MAC) address. Some companies track this MAC address and use it to follow your movements within their stores... like which aisles you visit in the grocery store or how often you visit your favorite coffee shop. Stores use this information to study things like how many people stop at a sale display rack or how long customers wait in checkout lines.

The data do not include your personal ID or phone number. But if you don't want Big Brother knowing how often you stop for a latte, you can do a few things to protect yourself. First, always turn off the Wi-Fi and Bluetooth settings for your phone when out in public. That will keep your phone from broadcasting its MAC. You can also sign up for an "opt-out" list at smart-places.org. (This will only take you off the list for companies that have agreed to the opt-out policy.)

4. **Turn your phone off**. This sounds like common sense, but I've seen far too many folks glued to their phones at all hours of the day and night. Not only are you interfering with your natural circadian rhythm and sleep schedule, you're hurting your eyes. Plus, you're giving Big Brother more opportunities to track you.

Make a pledge to go phone-free for even just a few hours a day. Even better, try a whole weekend without your cellphone. Keep it off the table during meals and don't sleep with it in your bedroom. Both your physical and mental health will greatly improve the more you decide to unplug.

Here's to our health, wealth, and a great retirement,

Dr. David Eifrig and the *Health & Wealth Bulletin* Research Team
August 30, 2018