Your Device is Listening: the Ultimate Fly on the Wall

Author : Cat

Date : May 25, 2017

My friend pulled me aside and, in a hushed voice, told me that he was worried his device was listening to him when he spoke to his wife at home. He said he had mentioned something in a live conversation, that he swears he had never typed, and then he started getting ads for it. The nervous question came "Is my device listening to me all the time?" The answer.. Probably.

From phones to smart TVs, most devices are equipped with a microphone. Initially this was for use as an actual phone, but now the microphone has multiple uses including voice commands, and the collection of voice data. If an app wants to collect your data all they need to do is ask for your permission to use the microphone, not stipulate what it is for. Snapchat, for example, records videos and does voice changing on the images. But do you know what else it records? Or how it handles it?

Think of your microphone like a young child who is in the same room. If that child is engaged with TV or a game, we often assume they are not listening when we are talking with other adults. Then, a week later, they parrot back something you didn't know they heard. When we want our devices to hear us, like kids, we address them with their names. But that doesn't mean they are not just sitting and listening in the background all of the time.

Virtual Assistants

No matter if you call her Siri (Apple), Bixby (Samsung), OK Google (Android), Alexa (Amazon), or Cortana (Microsoft), Virtual Assistants are popping up everywhere to help you operate your devices

by voice. They can do simple tasks like turning on a set of lights, or complicated ones like recommending a restaurant they think you will like. The more artificial intelligence the tasks require, the more background the assistants need on you.

Consider if you wanted to select an ice cream shop. If you ask a stranger what ice cream you should get then they will give you the shop they know, not a personalized answer. If you ask a friend, they will tell you the place that is closest to you as well as one they think you would enjoy, based on other information they have. When you enable Siri on an iPhone, it immediately takes your location and contact data. As you use the assistant, it stores data on the types of questions you ask and the answers you find adequate. All this additional data creates better and more accurate answers.

The terms and conditions become fuzzy on where data collection stops. It is unclear how much other audio data it takes, when it records your daily conversations, when it listens to your phone calls, or if it make notes on ambient noise. The small print will tell you that this is all to improve your experience. If you are talking about a trip to Vegas with friends, maybe it is helpful for you to find ads for Vegas next time you are online. Or maybe it is just creepy. You, as a consumer, need to decide how much value you get from the assistance versus the amount of data they are potentially taking.

If you use Google voice commands, you can check here for a full list of what you have searched by voice and what they have recorded.

Settings for Your Microphone

It is important that you control your permissions and settings. As we previously went through how to turn off Location Settings for your device, below are the instructions for finding and altering the access to your microphone. Only allow access when needed. For instance, a flashlight app or one with movie listings should not ever require access to record your voice.

iPhone

On iPhone, microphone access is found inside the *Settings* under the *Privacy* section.

This screen will list any apps that you have downloaded that have requested permission to access your microphone. Turn off any apps that do not need it. If you want to occasionally use a microphone, you can turn on access for a time window in which you want to make a call or a recording, and then turn it off again.

Android

Microphone permissions in Android can be found as a permission type or within each application. To find the entire list, select *Settings, Apps, Advanced*, and then *App Permissions*. You will find *Microphone* listed as one of the permission types. Same as iPhone, this screen will list any apps that you have downloaded that have requested permission to access your microphone. Turn off any apps that do not need it. If you want to occasionally use a microphone, you can turn on access for a time window in which you want to make a call or a recording, and then turn it off again.

Alternatively, you can select the specific application from the Apps screen. Here you can decide which permissions are actually needed and leave only those that make sense.

As with all things digital, there is a trade-off between what we give away and what we get. Decide how much data you are willing to share for the benefit of the app or assistant. Additionally, your microphone is an access point to your personal data (your voice). Be wary that software bugs, and hacks, do happen. If you leave the door open for access, that could be taken advantage of.