How to protect your privacy in Windows 10

By Preston Gralla, Contributing Editor, Computerworld | APRIL 16, 2019

Worried about privacy issues in Windows 10? Here's what you can do.

There has been some concern that Windows 10 gathers too much private information from users. Whether you think Microsoft's operating system crosses the privacy line or just want to make sure you protect as much of your personal life as possible, we're here to help. Here's how to protect your privacy in just a few minutes. *Note: This story has been updated for the Windows 10 October 2018 Update, a.k.a. version 1809. If you have an earlier release of Windows 10, some things may be different.*

Turn off ad tracking

At the top of many people's privacy concerns is what data is being gathered about them as they browse the web. That information creates a profile of a person's interests that is used by a variety of companies to target ads. Windows 10 does this with the use of an advertising ID. The ID doesn't just gather information about you when you browse the web, but also when you use Windows 10 apps.

You can turn that advertising ID off if you want. Launch the Windows 10 Settings app (by clicking on the Start button at the lower left corner of your screen and then clicking the Settings icon, which looks like a gear) and go to Privacy > General. There you'll see a list of choices under the title "Change privacy options"; the first controls the advertising ID. Move the slider from On to Off. You'll still get ads delivered to you, but they'll be generic ones rather than targeted ones, and your interests won't be tracked.
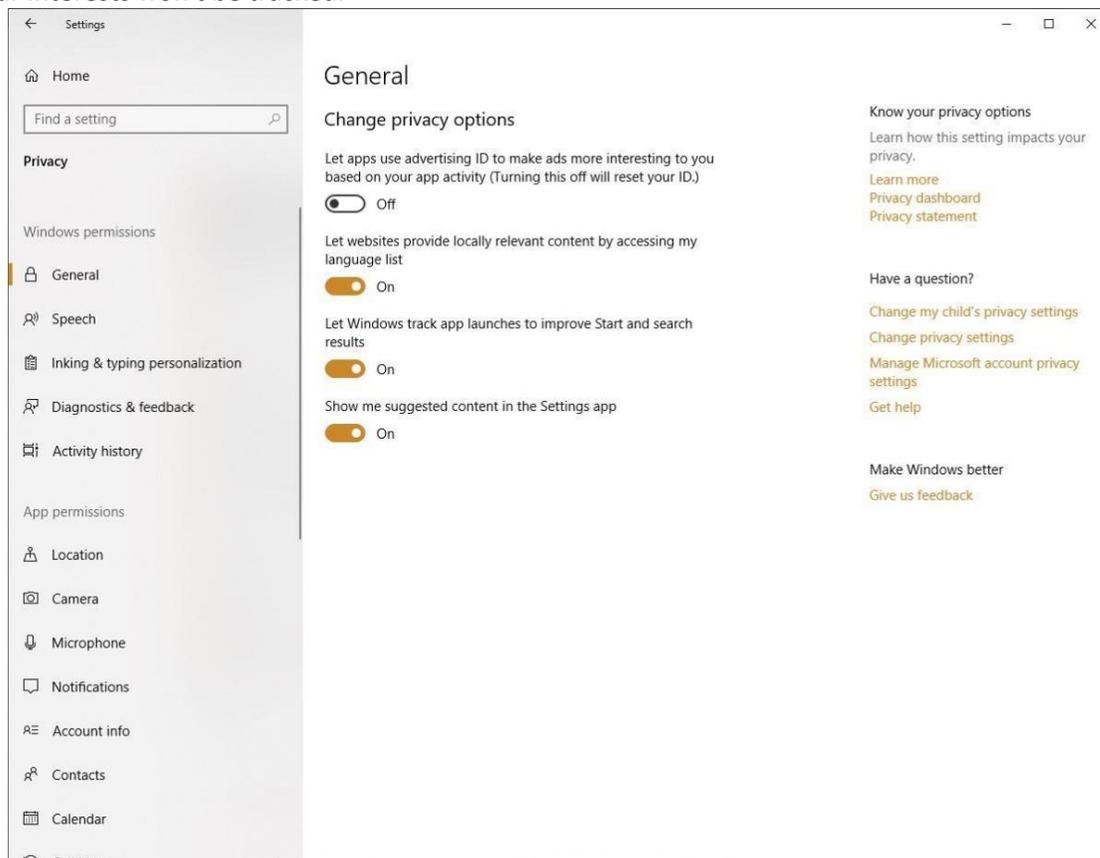

To make absolutely sure you're not tracked online when you use Windows 10, and to turn off any other ways Microsoft will use information about you to target ads, head to the Ad Settings section of Microsoft's Privacy Dashboard. Sign into your Microsoft account at the top of the page. Then go to the "See ads that interest you" section at the top of the page and move the slider from On to Off. After that, scroll down to the "See personalized ads in your browser" section and move the slider from On to Off. Note that you need to go to every browser you use and make sure the slider for "See personalized ads in your browser" is set to Off.

Turn off location tracking

Wherever you go, Windows 10 knows you're there. Some people don't mind this, because it helps the operating system give you relevant information, such as your local weather, what restaurants are nearby and so on. But if you don't want Windows 10 to track your location, you can tell it to stop.

Launch the Settings app and go to Privacy > Location. Underneath "Allow access to location on this device," click Change and, on the screen that appears, move the slider from On to Off. Doing that turns off all location tracking for every user on the PC.
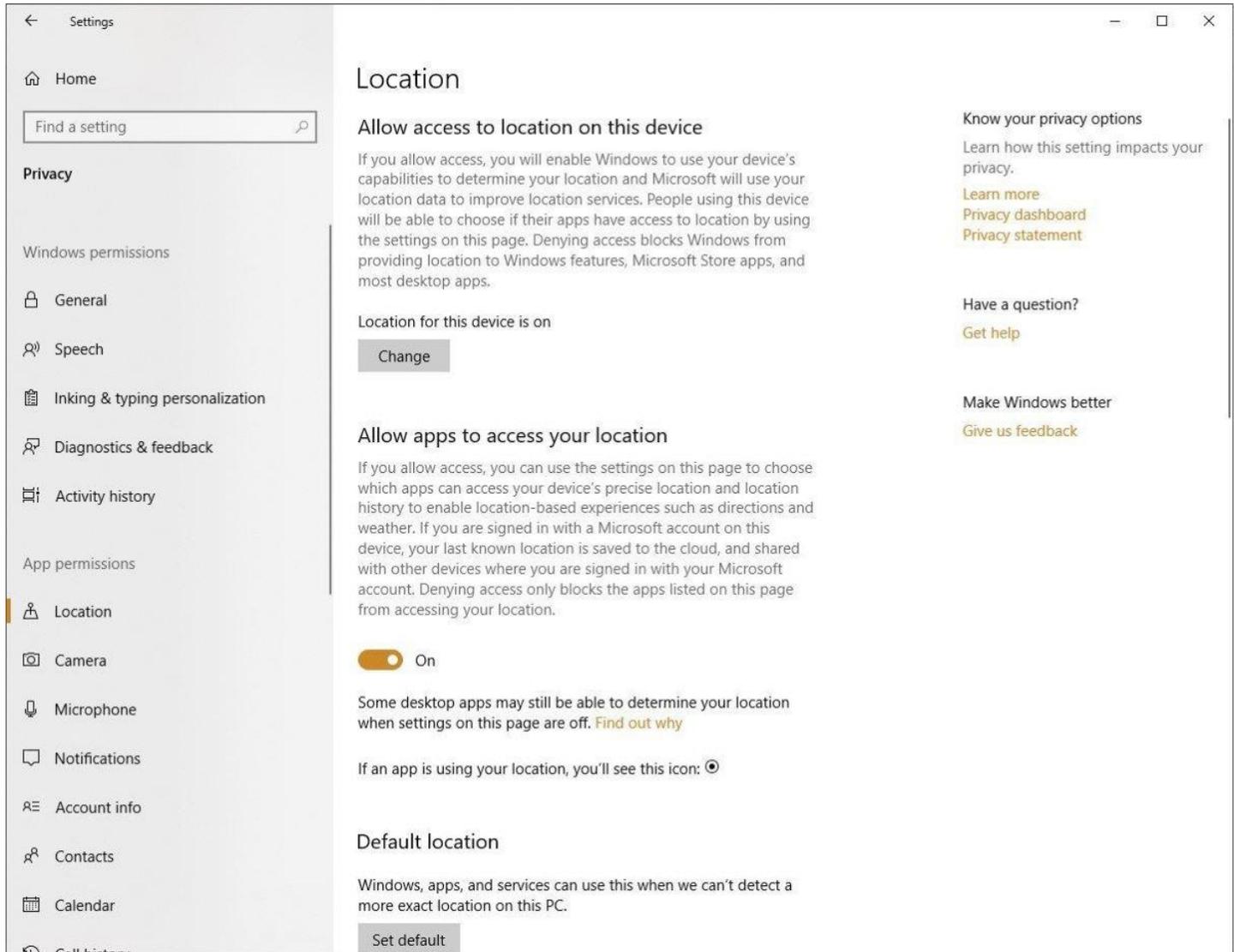

This doesn't have to be all or nothing affair — you can turn off location tracking on an app-by-app basis. If you want your location to be used only for some apps and not others, make sure location tracking is turned on, then scroll down to the "Choose apps that can use your precise location" section. You'll see a list of every app that can use your location. Move the slider to On for the apps you want to allow to use your location — for example, Weather or News — and to Off for the apps you don't.

When you turn off location tracking, Windows 10 will still keep a record of your past location history. To clear your location history, scroll to "Location History" and click Clear. Even if you use location tracking, you might want to clear your history regularly; there's no automated way to have it cleared.

Turn off Timeline

The Windows 10 April 2018 Update introduced a new feature called Timeline that lets you review and then resume activities and open files you've started on your Windows 10 PC, as well as any other Windows PCs and devices you have. So, for example, you'll be able to switch between a desktop and laptop and from each machine resume activities you've started on either PC.

In order to do that, Windows needs to gather information about all your activities on each of your machines. If that worries you, it's easy to turn Timeline off. To do it, go to Settings > Privacy > Activity History and uncheck the boxes next to "Store my activity history on this device" and "Send my activity history to Microsoft."
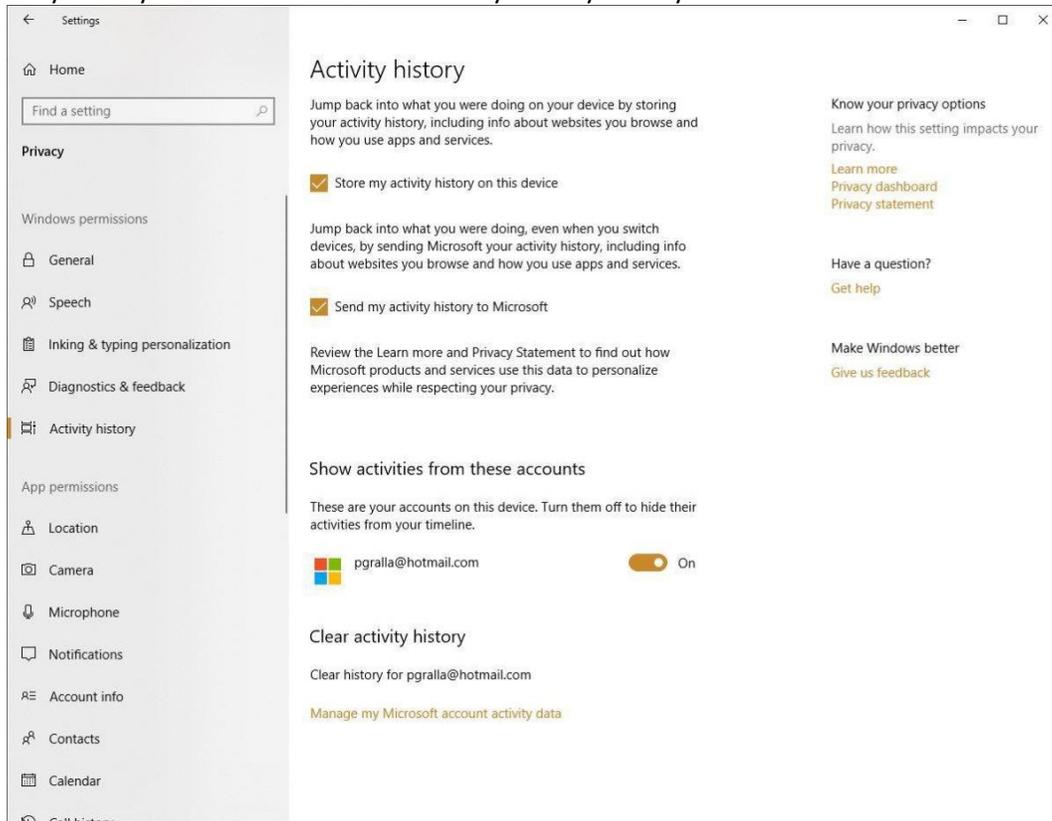
At that point, Windows 10 no longer gathers information about your activities. However, it still keeps information about your old activities and shows them in your Timeline on all your PCs. To get rid of that old information, in the "Clear activity history" section of the screen, click "Manage my Microsoft account activity data." You'll be sent to Microsoft's Privacy Dashboard, where you can clear your data. See the section later in this article on how to use the privacy dashboard to do that.

Note that you'll have to take these steps on all of your PCs to turn off the tracking of your activities.

Curb Cortana

Cortana is a very useful digital assistant, but there's a tradeoff in using it: To do its job well, it needs to know things about you such as your home location, place of work and the times and route you take to commute there. If you're worried it will invade your privacy by doing that, there are a number of things you can do to limit the information Cortana gathers about you.

Start by opening Cortana settings: place your cursor in the Windows search box and click the Cortana settings icon (it looks like a gear) that appears in the left pane. On the screen that appears, select Permissions & History. Click "Manage the information Cortana can access from this device," and on the screen that appears, turn off Location so that Cortana won't track and store your location.

Then turn off "Contacts, email, calendar & communication history." That will stop the assistant from gathering information about your meetings, travel plans, contacts and more. But it will also turn off Cortana's ability to do things such as remind you about meetings and upcoming flights. Towards the bottom of the screen, turn off "Browsing history" so that Cortana won't keep your browsing history.

To stop Cortana from gathering other types of information, head to the Cortana's Notebook section of Microsoft's Privacy Dashboard. You'll see a variety of personal content, ranging from finance to flights, news, sports, and much more. Click the content you want Cortana to stop tracking, then follow the instructions for deleting it.

If you want to delete all the data Cortana has gathered about you, click "Clear Cortana data" on the right side of the screen.
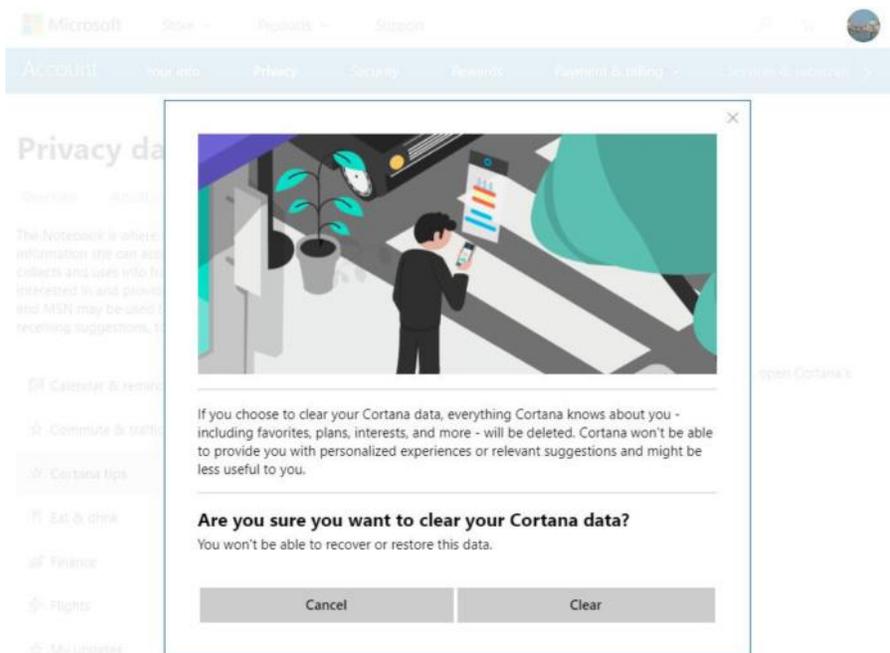
There's some bad news for those who want to ditch Cortana completely: Back when the Windows 10 Anniversary Update was released in August 2016, the easy On/Off setting for turning it off was taken away. However, that doesn't mean you can't turn Cortana off — it just takes more work.

If you use any version of Windows 10 other than the Home version, you can use the Group Policy Editor to turn it off. Launch the Group Policy Editor by typing **gpedit.msc** into the search box. Then navigate to Computer Configuration > Administrative Templates > Windows Components > Search > Allow Cortana. Set it to "disabled."

If you have the Home version, you'll have to muck around in the Registry. Before doing that, though, create a Restore Point, so that you can recover if anything goes wrong. Once you've done that:

1. Type **regedit** into the search box and press Enter to run the Registry Editor.

2. Go to the key *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Windows Search*.

(If the Windows Search key doesn't appear in the Registry Editor, go to *HKEY _LOCAL_MACHINE\Software\Policies\Microsoft\Windows*. Right-click the key and select New > Key. It will be given a name such as New Key #1. Right-click it, select Rename, and then type **Windows Search** into the box.)

3. Create the DWORD value AllowCortana by right-clicking Windows Search and selecting New > DWORD (32-bit) Value. Type **AllowCortana** in the Name field.

4. Double-click the AllowCortana value. Type **0** in the Value data box.

5. Click OK. You'll have to sign out of your Windows account and sign back in again (or restart Windows) to make the setting take effect.

Ditch a Microsoft account for a local account

When you use your Microsoft account to log into Windows 10, you're able to sync your settings with all Windows devices. So, for example, when you make changes to your settings on a desktop PC, those changes will also be made on your laptop the next time you log in.

But maybe you don't want Microsoft to store that information about you. And maybe you want to cut your ties as much as possible to anything Microsoft stores about you. If that's the case, your best bet is to stop using your Microsoft account and instead use a local account.

It's simple to do. Go to Settings > Accounts and select "Sign in with a local account instead." A wizard launches. Follow its instructions to create and use a local account. Keep in mind that when you do this, you won't be able to use Microsoft's OneDrive storage or download and install for-pay apps from the Windows Store. You can, however, download and install free apps from the Windows Store.

Change your app permissions

Windows apps have the potential to invade your privacy — they can have access to your camera, microphone, location, pictures and videos.

But you can decide, in a very granular way, what kind of access each app can have.

To do this, go to Settings > Apps. Below "Apps & features" you'll see a list of your installed apps. Click the app whose permissions you want to control, then click Advanced options and set the app's permissions by toggling them either on or off.
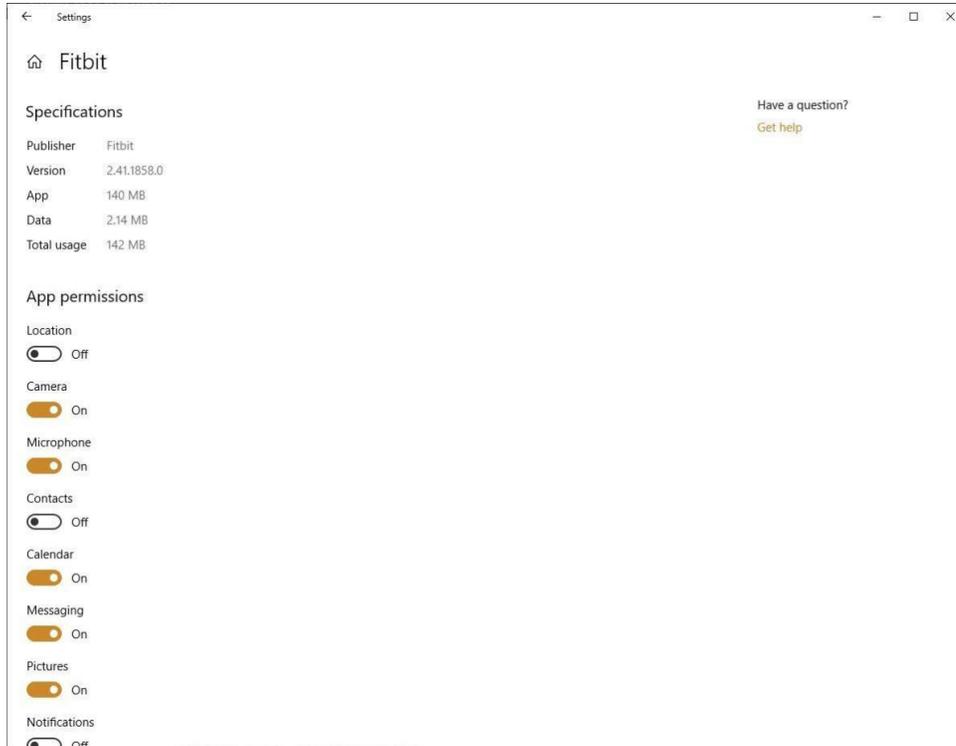
Note, though, that very few apps have an "Advanced options" link. And of those that do, not all let you customize your app permissions.

However, there's another way to change app permissions. To do it, go to Settings > Privacy and look under the "App permissions" section on the left-hand side of the page. You'll see a list of all of Windows' hardware, capabilities and features that apps can access if they're given permission — location, camera, microphone, notifications, account info, contacts and so on.

Click any of the listed items — for example, Microphone. At the top of the page that appears, you can turn off access to the microphone for all apps. Below that you'll see a listing of all the apps with access to the microphone, where you can control access on an app-by-app basis. Any app with access has a slider that is On. To stop any app from having access, move the slider to Off.

Control and delete diagnostic data

As you use Windows 10, data is gathered about your hardware and what you do when you use Windows. Microsoft says that it collects this data as a way to continually improve Windows and to offer you customized advice on how to best use Windows.

That makes plenty of people uncomfortable. If you're one of them, you can to a certain extent control what kind of diagnostic data is gathered about you. To do it, head to Settings > Privacy > Diagnostics & Feedback. In the Diagnostic data section, you can choose between two levels of diagnostic data to be gathered. Note that there's no way to stop Microsoft from gathering diagnostic data entirely. Here are your two choices:

- **Basic:** This sends information to Microsoft "about your device, its settings and capabilities, and whether it is performing properly." If you're worried about your privacy, this is the setting to choose.
- **Full:** This sends the whole nine yards to Microsoft: "all Basic diagnostic data, along with info about the websites you browse and how you use apps and features, plus additional info about device health, device usage, and enhanced error reporting." If you're worried about your privacy, don't make this choice.
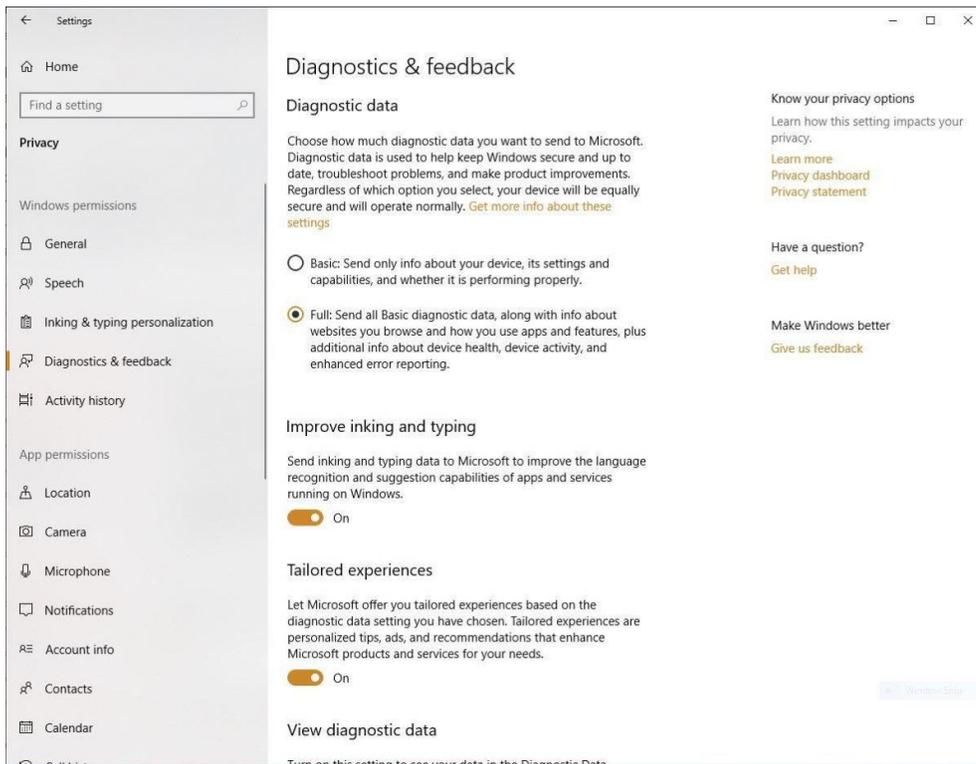
Next, scroll down to the "Tailored experiences" section and move the slider to Off. This won't affect the data Microsoft gathers, but it will turn off targeted ads and tips that are based on that information. So while it won't enhance your privacy, you'll at least cut down on the annoyance factor.

Now scroll a bit further down and in the "Delete diagnostic data" section, click Delete. That will delete all the diagnostic data Microsoft has gathered about you. However, after you delete it, Microsoft will start gathering the data again.

Finally on this screen, consider scrolling up to the "Improve inking & typing recognition" section and moving the slider to Off. That will stop Windows 10 from sending to Microsoft the words you input using the keyboard and inking.

One final note about diagnostic data. You may have heard about a tool Microsoft has been hyping, called the Diagnostic Data Viewer, which you can download from the Microsoft Store. Microsoft claims it lets you see exactly what kind of diagnostic data Microsoft gathers about you. Don't believe it. It's something only a programmer could love — or understand. You won't be able to use it to clearly see the diagnostic data Microsoft collects. Instead, you'll scroll or search through incomprehensible headings such as "TelClientSynthetic.PdcNetworkActivation_4" and "Microsoft.Windows.App.Browser.IEFrameProcessAttached" with no explanation of what it means. Click any heading, and you'll find even more incomprehensible data.

Use Microsoft's Privacy Dashboard

Microsoft has built an excellent, little-known web tool called the Privacy Dashboard that lets you track and delete a lot of information Microsoft gathers about you. To get to it, go to https://account.microsoft.com/privacy/.

As covered earlier in this story, here you can turn off ad targeting and limit the data gathered in Cortana's Notebook. You can also view and delete your browsing history, search history, location activity, voice activity, media activity, LinkedIn activity, and a lot more. (Note that for you browsing and search history, it only tracks your activity when you use Microsoft Edge or Internet Explorer. It doesn't track data when you use other browsers, like Chrome or Firefox. And it only tracks your location history when you're using Microsoft devices, not those that use iOS or Android.)

Browsing history

If browsing history in Cortana is turned on, your Microsoft Edge browsing history is sent to Microsoft so that Microsoft features and services may use this data to provide you with timely and intelligent answers, proactive personalized suggestions, or to complete tasks for you.

In addition to the browsing history saved here, Microsoft Edge also saves your browsing history on your device. To clear that data, on your device, go to **Microsoft Edge > More ··· > Settings.**

When you use InPrivate tabs or windows, your browsing data (like your history, temporary internet files, and cookies) isn't saved on your device once you're done. Learn more about InPrivate Browsing

VIEW AND CLEAR BROWSING HISTORY >

Search history

Like other search engines, Bing uses your search history to give you better results, including personalization and autosuggest. Cortana also uses that data to give you timely, intelligent answers, personalized suggestions, and complete other tasks for you.

View and change your search settings

Learn more about InPrivate Browsing

VIEW AND CLEAR SEARCH HISTORY >   Feedback

Using it is a breeze. Simply head to the information you want to view and clear, then click the "View and Clear…" button. You'll see all your activity in that category, and be able to delete individual instances (such as a single web search, for example), or all of it at once.

Get granular in the Settings app

All this shouldn't take that long and will do a great deal to protect your privacy. However, if you want to dig even deeper into privacy protections, there's something else you can do.

Launch the Settings app and click Privacy. On the left-hand side of the screen, you'll see the various areas where you can get even more granular about privacy — for example, in the Windows permissions section you can change your global privacy options for things such as speech recognition and inking. And here's where you'll get access to all app permissions, as outlined earlier in this article.

These steps can take you a long way towards making sure that Windows 10 doesn't cross the line into gathering data you'd prefer remain private.

This article was originally published in January 2016 and most recently updated in April 2019.