Windows 10 violates your privacy by default, here's how you can protect yourself

Upon installation, Windows 10 defaults to some pretty serious privacy invasions. Here are some steps you can take to keep your personal data private.

By Conner Forrest

Since the July 29 release of Windows 10, the tech world has been talking about the latest OS update from Microsoft. A mere 24 hours after its release, more than 14 million users had downloaded Windows 10.

The quick ramp up was due, in part, to Microsoft releasing the update as a free download for existing Windows users. Windows 10 also came with a new service model as Windows will be releasing service packs every few months to users.

The model itself got some backlash, especially from organizations that don't want to upgrade their system that frequently. More recently, though, some criticism has arisen over privacy concerns brought on by the new OS.

The first issue is that Windows 10 automatically assigns an advertising ID to each user on a device tied to the email address that's on file. Using that ID, the company can tailor ads for web-browsing and using certain applications.

The next concern is that much of users' personal data is synced with Microsoft's servers. Some of this information, like your Wi-Fi password, can then be encrypted and shared with your contacts, using a feature called Wi-Fi sense. Although, some have argued that this isn't a security risk, because the user must choose to share the network.

Additionally, Microsoft's personal assistant, Cortana, must collect data as well to provide the kind of service it does, but it is likely not better or worse than its Apple and Google contemporaries.

One of the biggest worries, though, is Microsoft's policy on disclosing or sharing your personal information. The following is an excerpt from the privacy policy:

"We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to protect our customers or enforce the terms governing the use of the services."

The problem is that many users want personalized services, but it's difficult to draw the line at what data should be collected. Forrester's Tyler Shields said that instead of making these features default, Microsoft could have allowed users to opt-in later if they wanted to enable them.

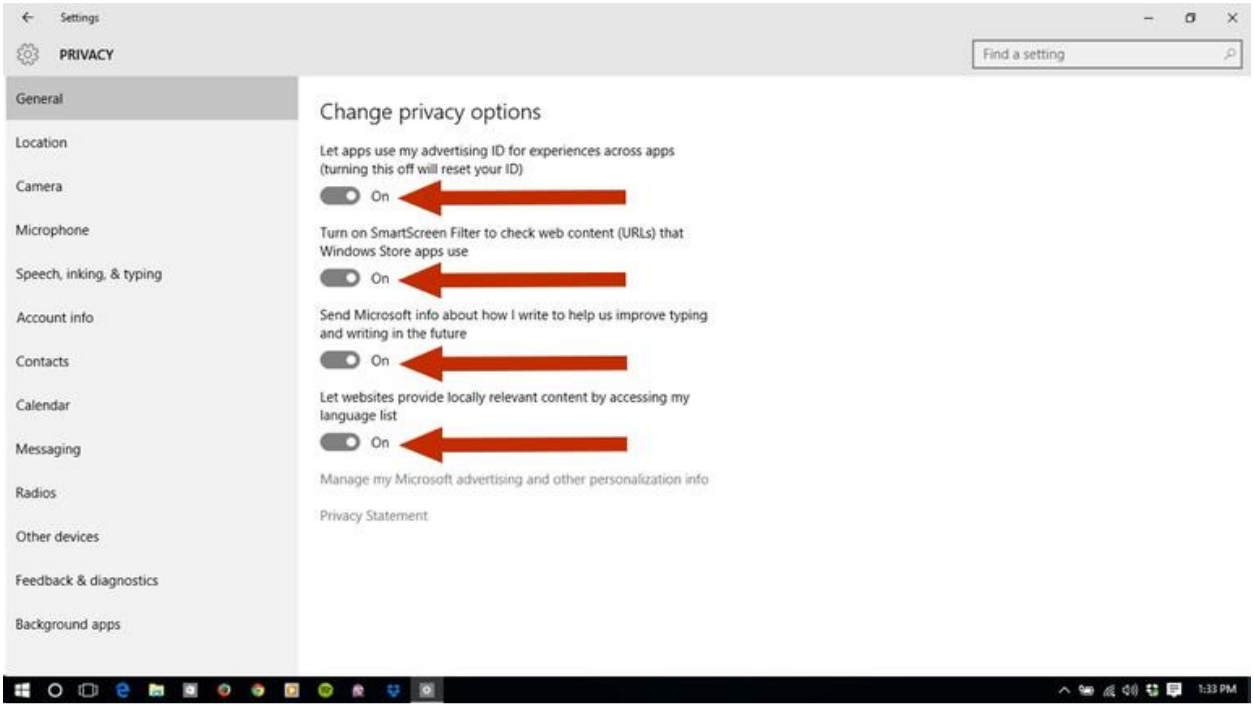
"This is more of a privacy-friendly stance that may have been palatable to the general public," Shields said. "However, Microsoft would have had less adoption to its value added services had it made them opt-in, thus lessening the potential success of the Windows 10 launch."

So, how do you protect yourself from these issues? Here are some steps you can take to opt-on or disable some of the problematic features.

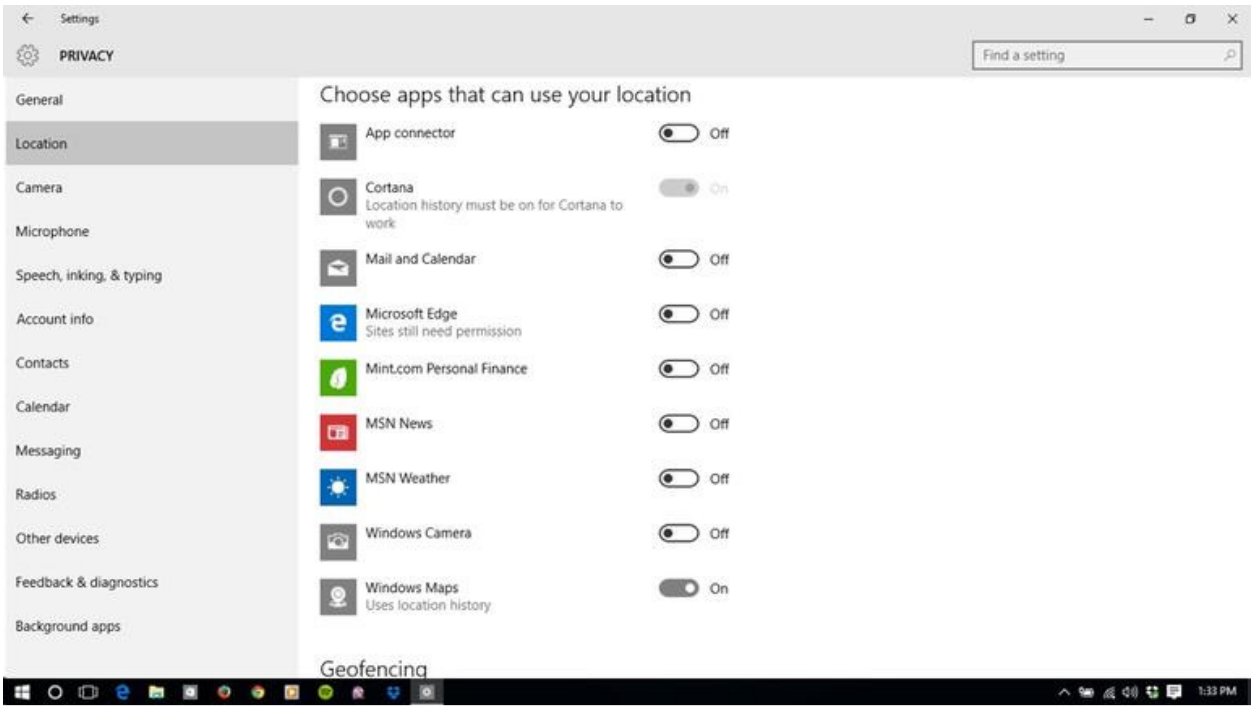
The first thing to note is that, if you haven't yet installed Windows 10 but you plan on doing so, make sure you that you do a custom install so you'll be able to pick and choose what is enabled at the onset. But, if you installed Windows 10 using Express settings, you can still disable some of the default privacy settings.

From the start button, click "Settings" and then click "Privacy" and click the "General" tab on the left sidebar. Under that tab you'll see a few sliders where you can toggle certain features on or off.

The top toggle button is the most important as it disables the advertising ID for each user. But, if you want to cover your bases, you should go ahead disable the rest of the options as well.

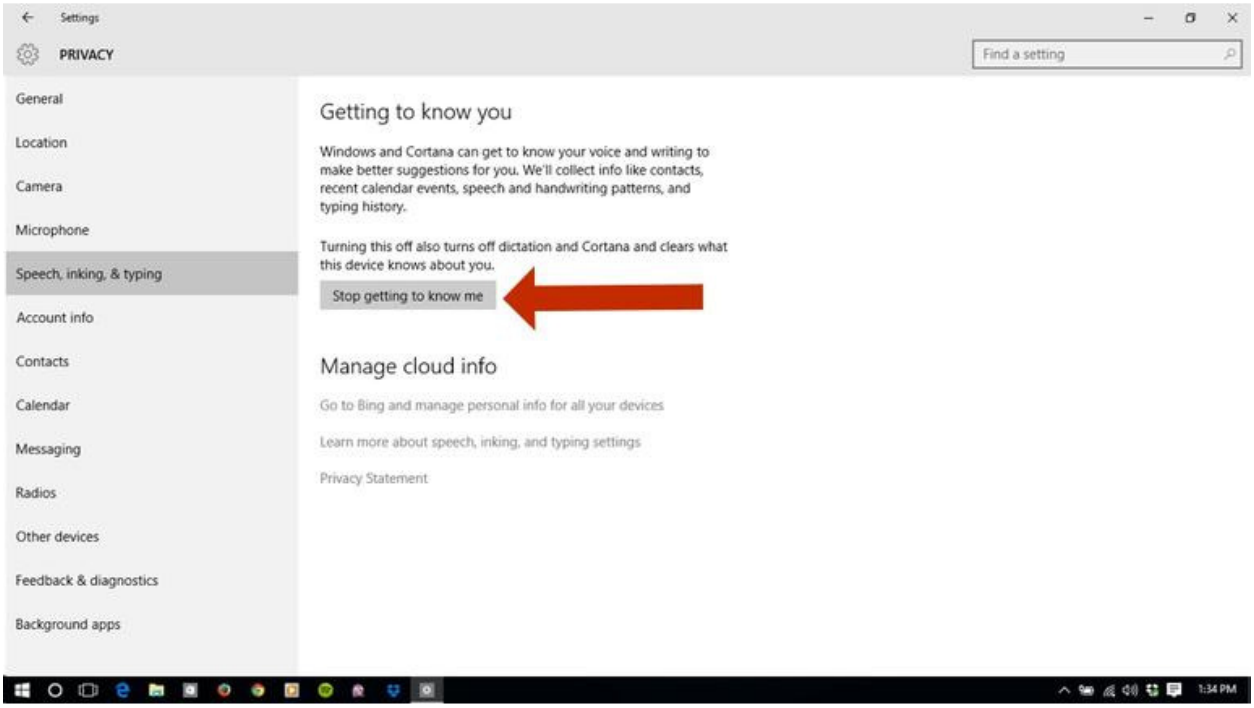


After turning off the options under the general tab, you can jump down to the next tab down, "Location," and turn off location data for all apps or specific ones. That's not necessarily new to WIndows 10, but it's something that many security-conscious folks like to do.



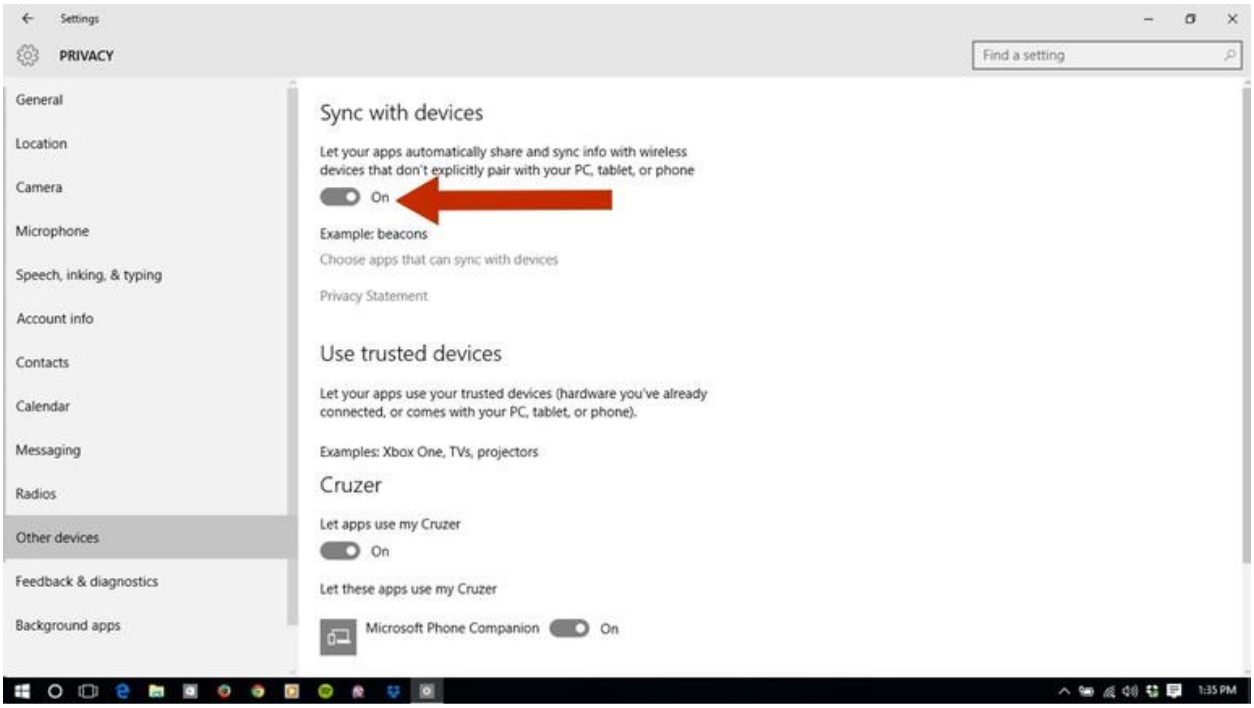
Next, you'll want to head down to the tab labeled "Speech, inking, and typing." Here you can disable Cortana from gathering information about you by clicking the "Stop getting to know me" button towards the middle of the screen.

Keep in mind, clicking this will also disable Cortana and dictation.

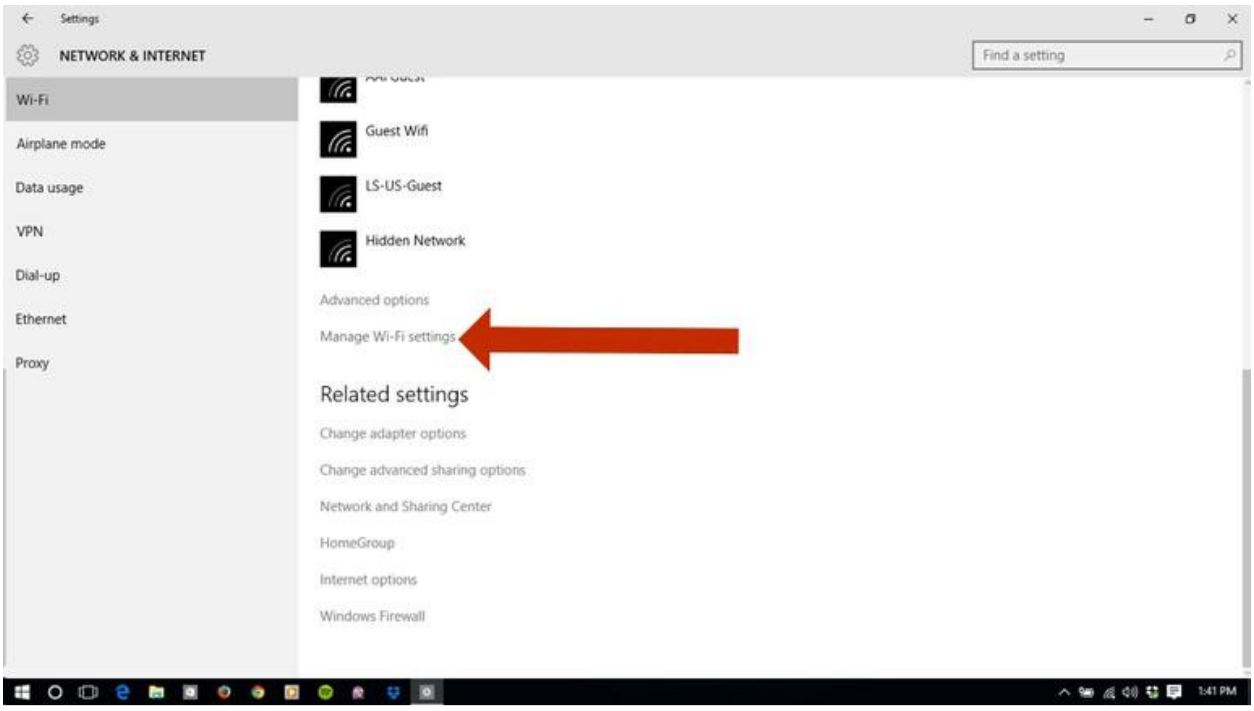


Moving on, click the "Other devices" tab at the bottom of the list. Under this tab you'll be able to turn off the "Sync with devices" feature. In the example given by Microsoft, this could be used for connecting with beacons, which are typically used for advertising purposes.

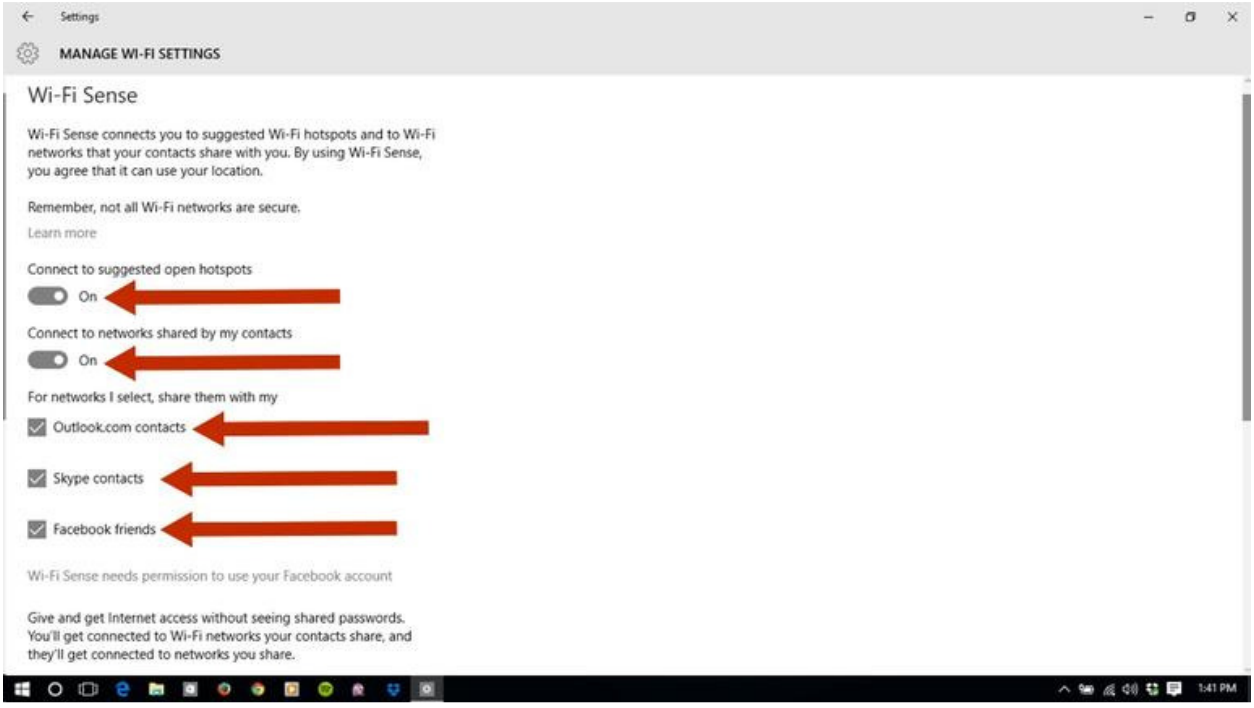
If you want to kill this feature, slide the first button to the off position. If you want, you can also turn off syncing for trusted devices as well.



Now, back out to the general settings and click "Network and internet." In that window click "Manage Wi-Fi settings" toward the middle of the screen.



Here you'll be able to customize your setting for the Wi-Fi Sense feature. If you want to keep everything private, click all the sliders until the read "off" and uncheck the boxes on the page. If not, you can select which features to turn off individually.



One of the final security checks you can do is to opt out of the personalized ads while browsing in Microsoft Edge. Click the following link or paste it into your browser: https://choice.microsoft.com/en-gb/opt-out

Click the Xs next to the options to turn off "Personalised ads in this browser" and "Personalised ads wherever I use my Microsoft account."

This isn't a comprehensive security checklist, but hopefully it helps you take care of some of the potential privacy issues in Windows 10