

Windows 10 Wi-Fi Sense Explained: Actual Security Threat You Need to Know

To all;

If you have upgraded to windows 10 or about to do the upgrade you should be aware of the following Privacy issues in Microsoft windows 10. The information is available at this website:

<http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/?tag=nl.e101&cid=e101&ttag=e101&ftag=TRE684d531>

I will try to cover these issues at the upcoming Computer club presentation on Windows 10 on September 21. I still believe it is worthwhile upgrading to Microsoft Windows 10 as soon as possible (especially if you are on windows 7).

Bob Z

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."

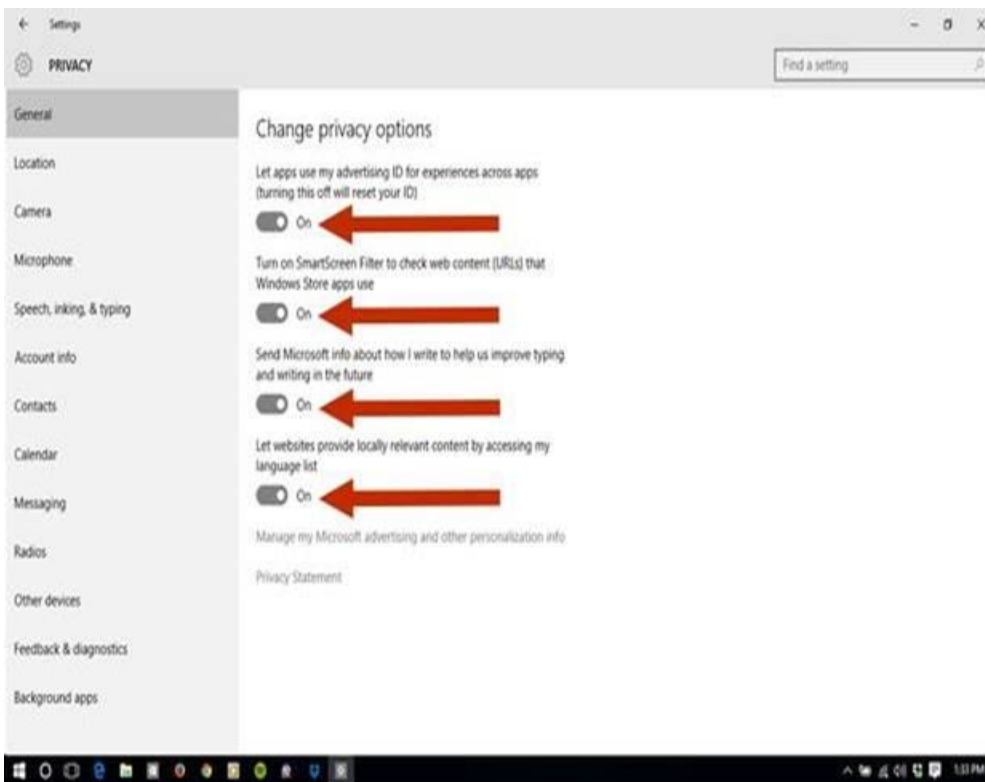
Solutions

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.

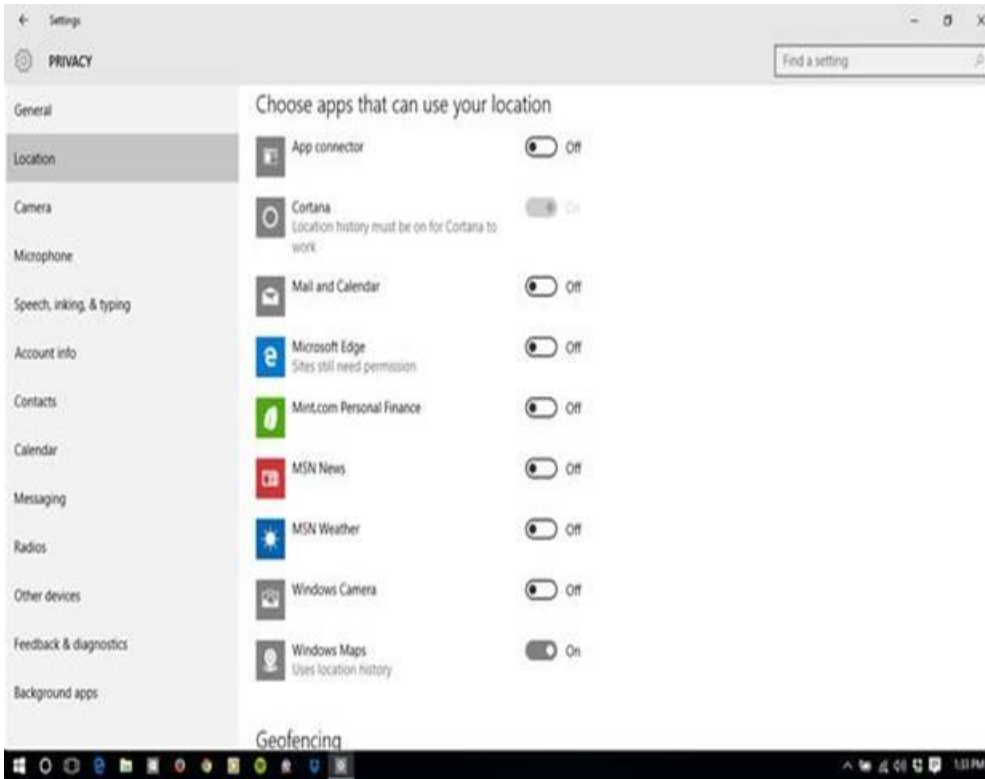
The first thing to note is that, if you haven't yet installed Windows 10 but you plan on doing so, make sure you that you do a custom install so you'll be able to pick and choose what is enabled at the onset. But, if you installed Windows 10 using Express settings, you can still disable some of the default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

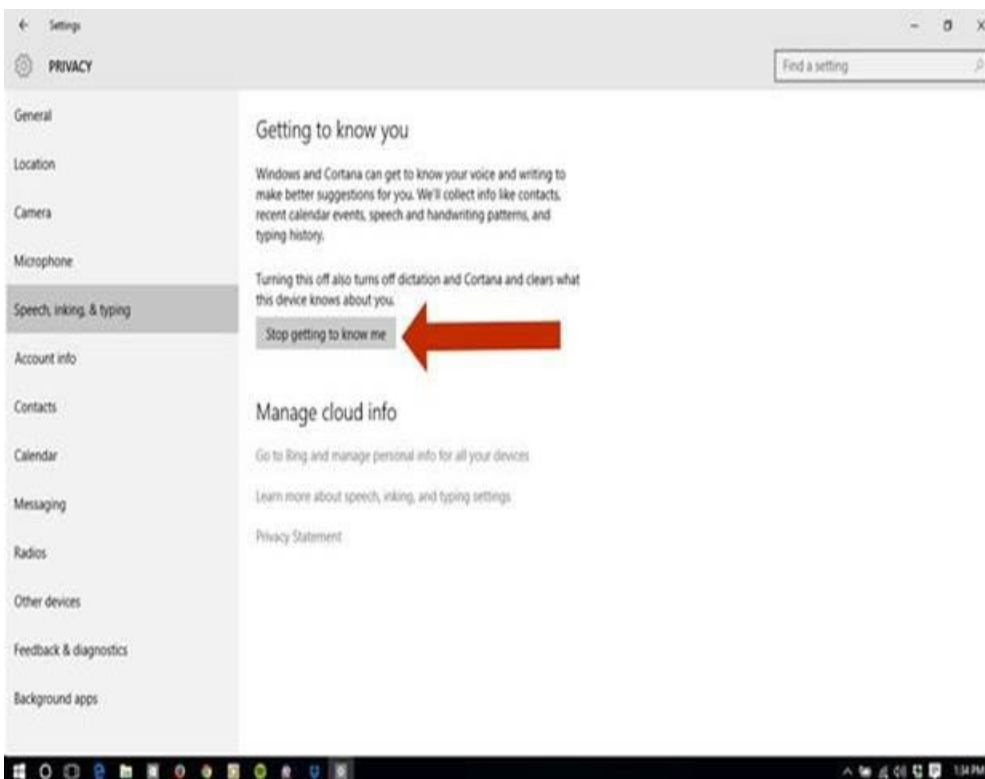


After turning off the options under the general tab, you can jump down to the next tab down, "Location," and turn off location data for all apps or specific ones. That's not necessarily new to Windows10, but it's something that many security-conscious folks like to do.



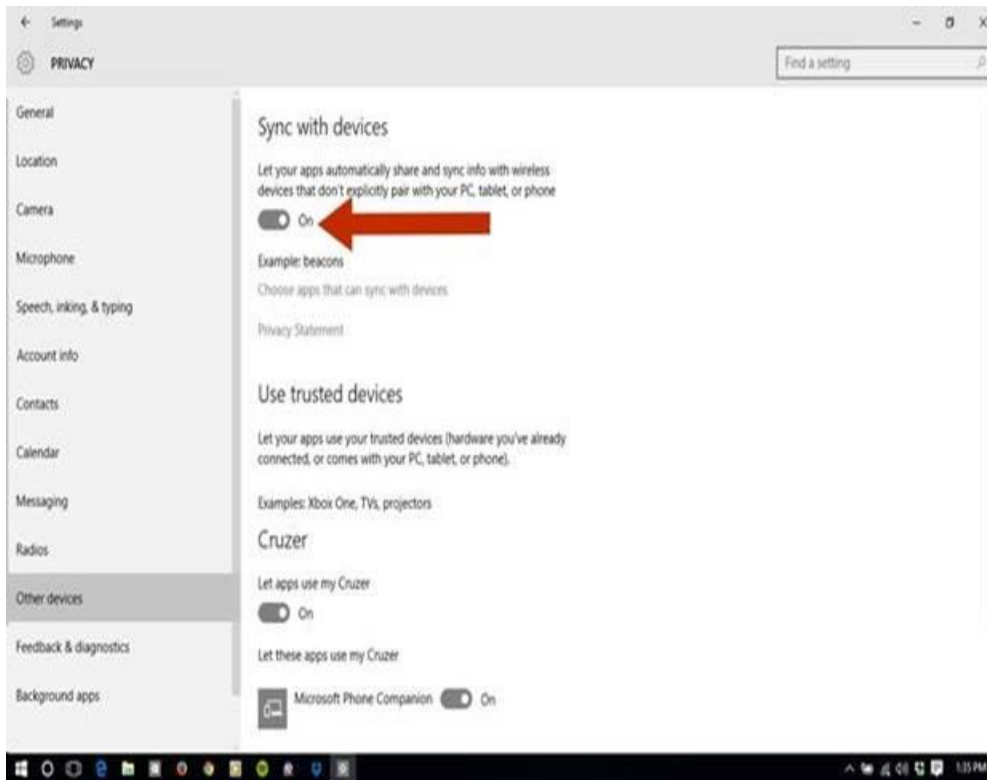
Next, you'll want to head down to the tab labeled "Speech, inking, and typing." Here you can disable Cortana from gathering information about you by clicking the "Stop getting to know me" button towards the middle of the screen.

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

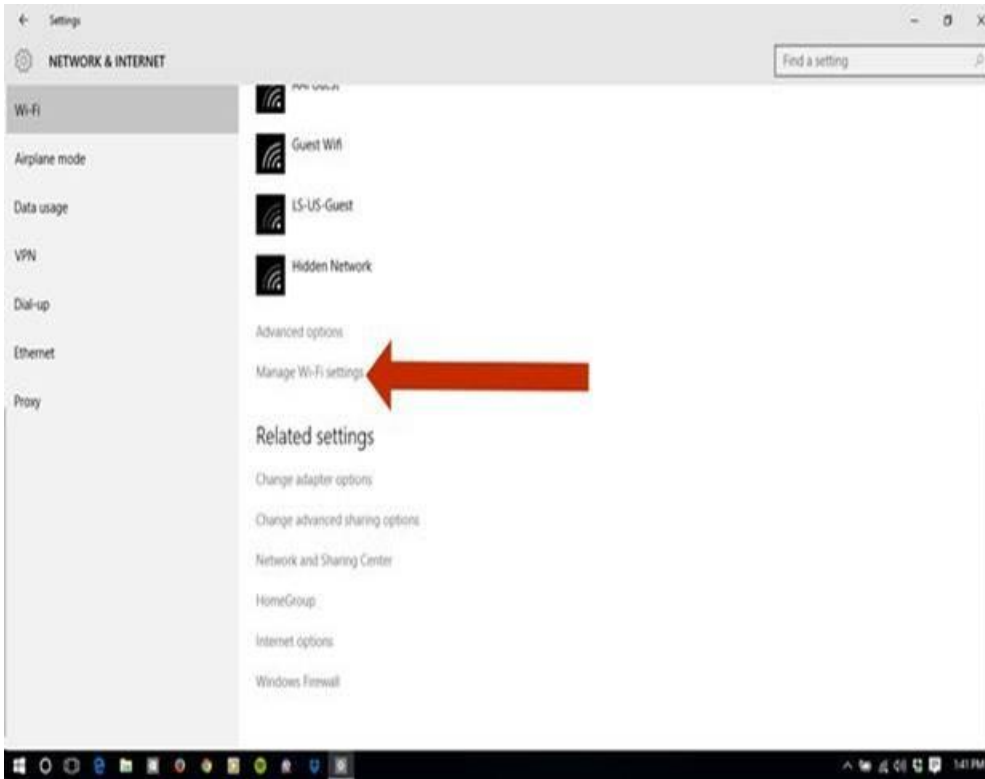


Moving on, click the "Other devices" tab at the bottom of the list. Under this tab you'll be able to turn off the "Sync with devices" feature. In the example given by Microsoft, this could be used for connecting with beacons, which are typically used for advertising purposes.

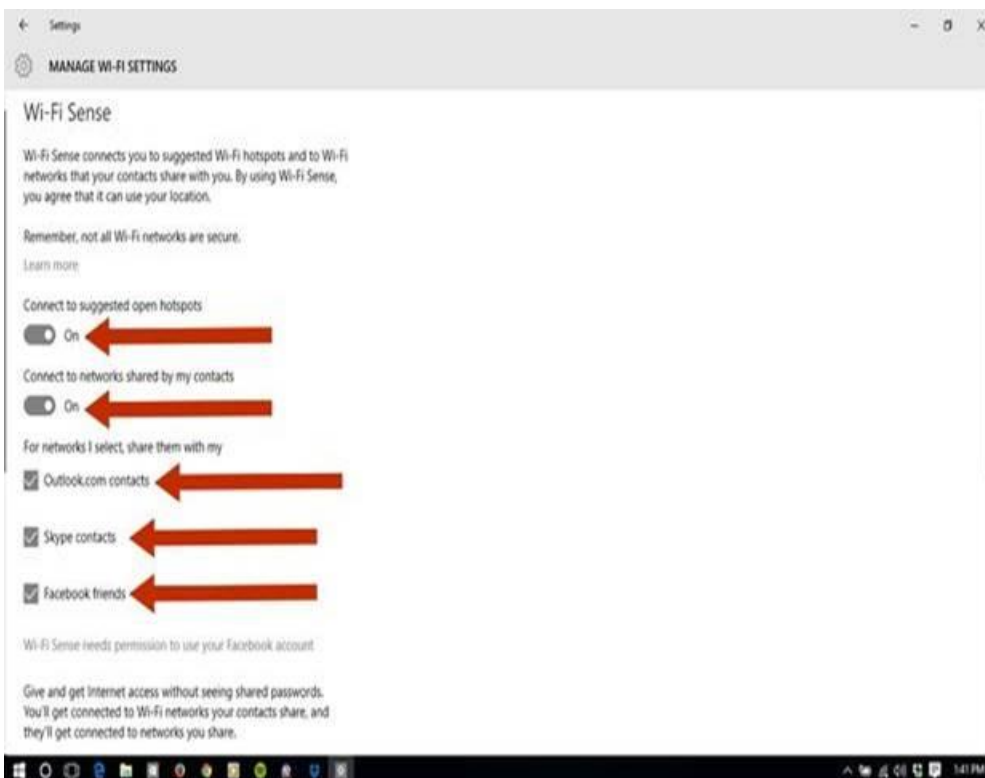
If you want to kill this feature, slide the first button to the off position. If you want, you can also turn off syncing for trusted devices as well.



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 they 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 X.s next to the options to turn off "Personalized ads in this browser" and "Personalized 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.