# Microsoft Windows 10 and Your Privacy:

Synopsis of an article from Windows Secrets Newsletter,

“Making Windows 10 a bit more Private and Secure,”

by Susan Bradley, 8/06/2015.

(an article in the paid content section)

compiled by Gary Patrick

September 29, 2015

# Upon Installation, Windows 10 defaults to some pretty serious privacy invasions

Users can opt out of most of these, but as “opt out” suggests one has to take specific action to change these settings:

1) Windows 10 automatically assigns an advertising ID
- tied to the email address on file for the user
- tailors ads for web browsing and using certain applications

2) Much of users' personal data is synced with Microsoft servers –
- WiFi password, for example, for a feature called WiFi sense, shares it with your email contacts and social media “friends”

Advice: if you haven't already installed Win 10, when you do, select “Custom Installation,” not “Express.”

(Custom Installation walks you through the privacy choices)
refer to: http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/

The Dilemma with Windows 10 is many users want personalized services but it's difficult to draw the line at what data should not be collected.

- A better approach would have been “opt-in” rather than “opt-out.”
- Opt-in is the practice in Europe, for example
- Precedent, though, in the U.S. is for opt-out, as for Google, etc.
- Google admits to caching every search done.

Once Windows 10 is installed (assuming Express), here are three recommended changes to make soon:

Enable System Restore:

- Win 10 doesn't create restore points unless you do this.

Review account synchronization settings.

- By default, Win10 synchronizes your custom settings among your various devices.
- For various reasons, you might prefer to limit synching or turn it off altogether.

Review and control WiFi credentials sharing:

- Win10 inherited this feature from Windows 8 phone.
- It allows people on your Facebook friends list or Outlook, Hotmail, and Skype contact lists to be signed in automatically to your Wi-Fi router when they’re within range.

## Privacy implications for use of Microsoft's Cortana (electronic search assistant):

The End User License Agreement (EULA) for Windows 10 clearly states Cortana has the ability to collect and use various types of personal information, including

- your location and location history,
- contacts,
- voice input,
- searching history,
- calendar details,
- content and communication history from messages and apps.
- In the MS Edge browser Cortana collects your browsing history.

## Probable examples of this data collection:

- your choice of music,
- alarm settings,
- what you view and purchase online,
- your Bing search history,
- your use of other Microsoft services, and more.

- What can you do about it?
- tinker with what Cortana remembers in the Notebook,
- disable Cortana in the Edge Browser,
- or turn Cortana off completely.

- The next slides show Cortana Setup and Settings dialogs:

Part of the "Cortana" Search Assistant setup dialog:

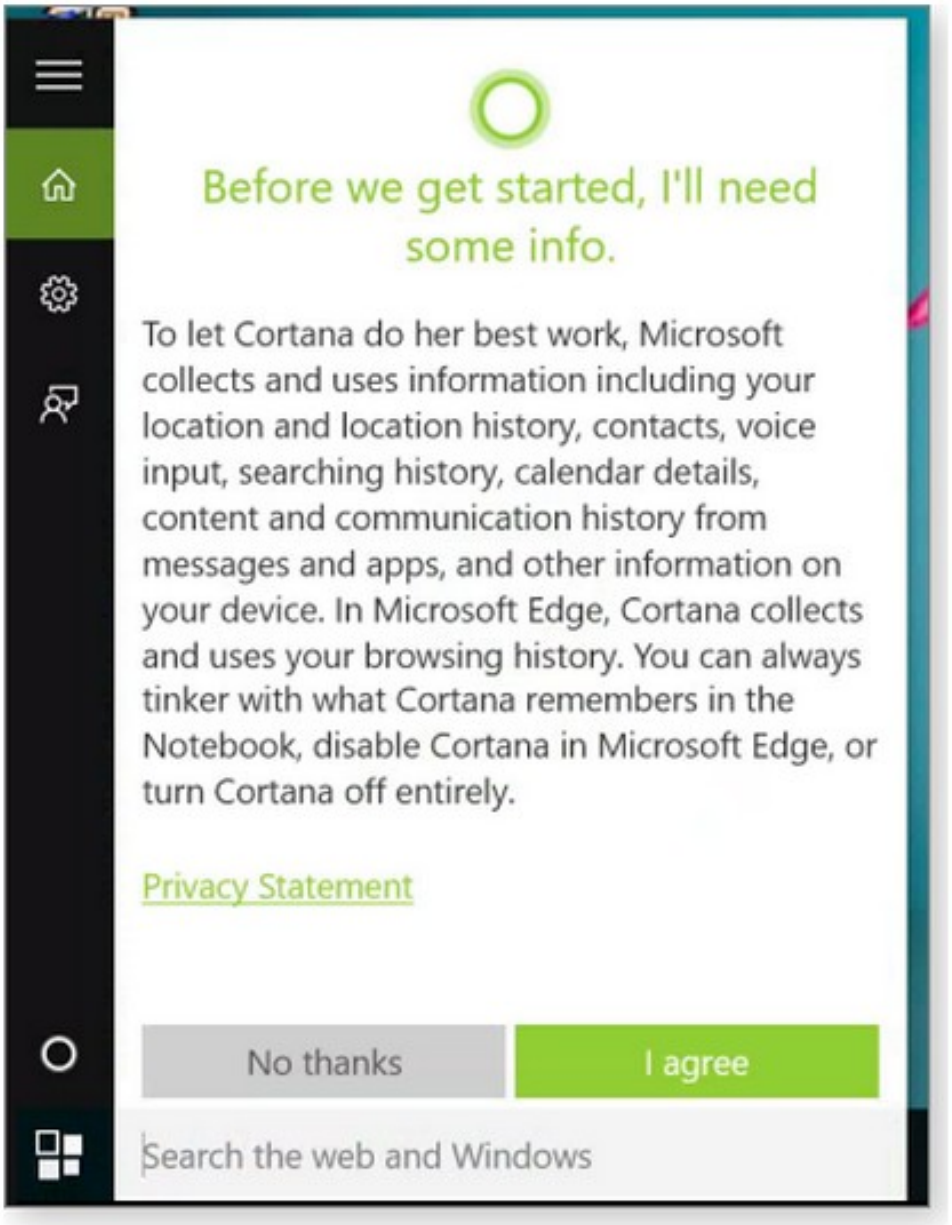



**Figure 3. Cortana collects a variety of personal information, as noted on first setup.**

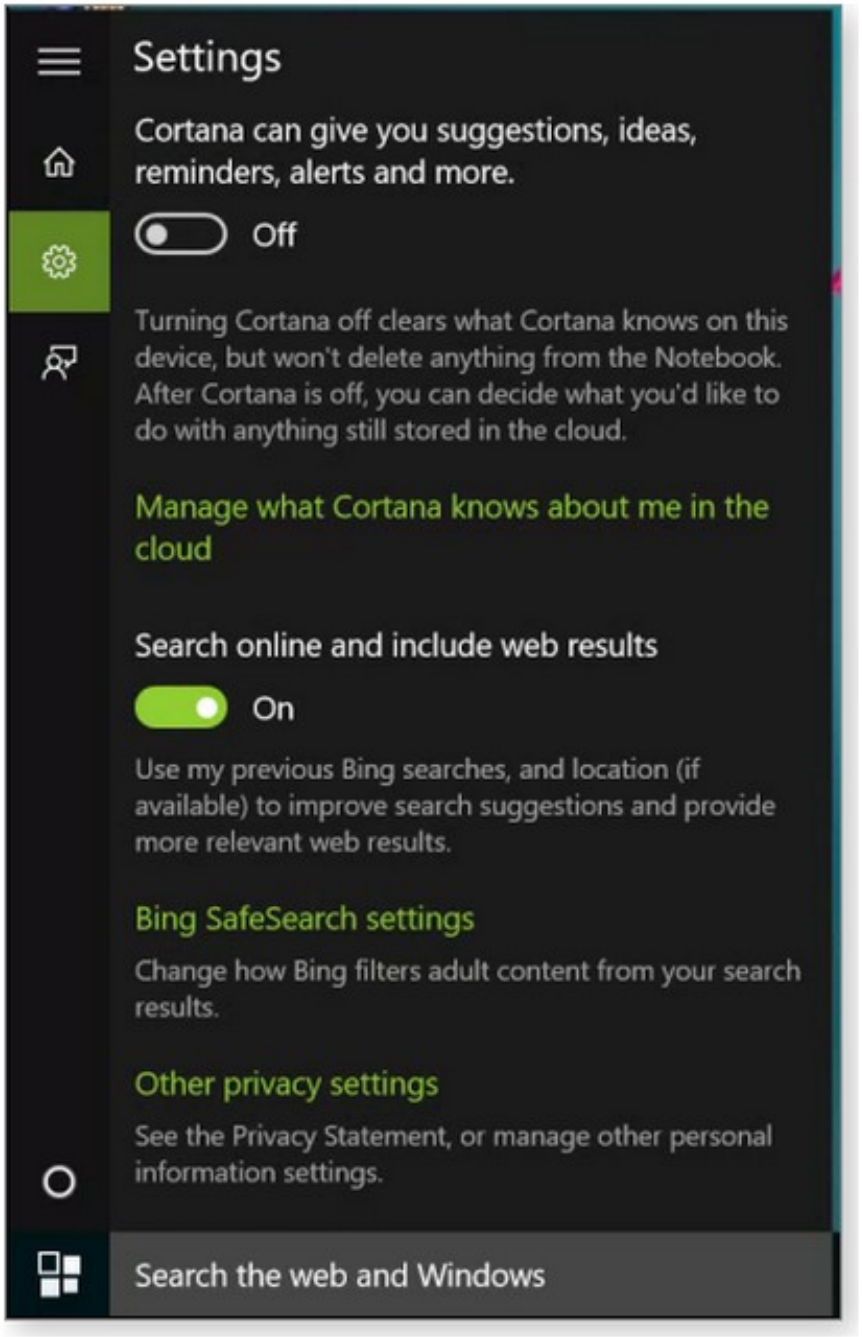



**Figure 4. Cortana can be disabled via its settings box.**

# Additional Windows 10 surprises:

The card game Solitaire includes advertising.

- To remove the ads, you have to pay a monthly subscription
- (reported in a Business Insider story).
- no workaround hack is known to get around this.

Each Win10 device generates a unique advertising ID

- can be used to target you with specific ads.
- This "feature" can be turned off in settings, or
- go online and opt out of personalized advertising.

(Go to Choice.microsoft.com to set how you want the Edge browser to behave).

If Win10 encryption is turned on, it uploads the encryption key to OneDrive.

- granted, this enables easy recovery or reset, through your Microsoft account.

Win10 also includes — again, turned "on" by default:

the option to share patches with, or obtain Windows updates from other computers on your local network, or the Internet.

- presumably to reduce updates traffic on Microsoft servers.
- hacking by a middleman conceivable, although not easy.
- one can reset this so updates come only from Microsoft servers.

## The ultimate way to exert control over Windows 10 is to purchase the Enterprise Edition.

- not easy for individuals, but neither is it impossible
- you merely have to play the volume-license game.
- purchase Windows 8.1 with Windows Software Assurance
- plus 4 other Microsoft products to qualify for the Enterprise Edition.
- easiest is to use a vendor such as CDW or SoftwareOne to assist; gives rights to Windows 10 Enterprise or Enterprise 2015 LTSB. (LTSB — or Long-Term Servicing Branch version is meant to be placed on dedicated devices such as ATMs and industrial equipment).

## Advantages:

- The OS is locked down and rarely updated.
- Group Policy Control is Supergod in the Enterprise Edition, the only way to disable data telemetry to Microsoft completely.

# More on Group Policy Control:

- Home Edition doesn't even have Group Policy control.
- In Windows Professional, Group Policy Control can't disable telemetry.

(material for this presentation, from slide #2 through the next one is courtesy of Susan Bradley, “Making Windows 10 a bit more private and secure,” in Windows Secrets Newsletter, 8/06/2015 – a paid content article).

Slides after the next are screenshots from a TechRepublic online article, walking through Win10 settings changes step by step.

# Summary Observations and Final Advice:

Microsoft has clearly stated its intent to focus on a mobile-first strategy. That’s evident in some of the default settings included in Windows 10; they don’t make much sense on the desktop but appear to be more suited for use on phones or tablets.

Users' privacy suffers from Microsoft's intent to make Windows 10 provide state-of-the-art user features on all devices: cell phones, tablets, laptops and desktops.

Express installation seems to enable everything.

Take some time to configure your preferred security before putting Win10 into heavy use!

One of the final security checks you can do is opt out of the personalized ads while browsing in Microsoft Edge:

1) Click the following link or paste it into your browser:
   https://choice.microsoft.com/en-gb/opt-out
2) Click the Xs next to the options to turn off
   "Personalized ads in this browser"  and
   "Personalized ads wherever I use my Microsoft account."

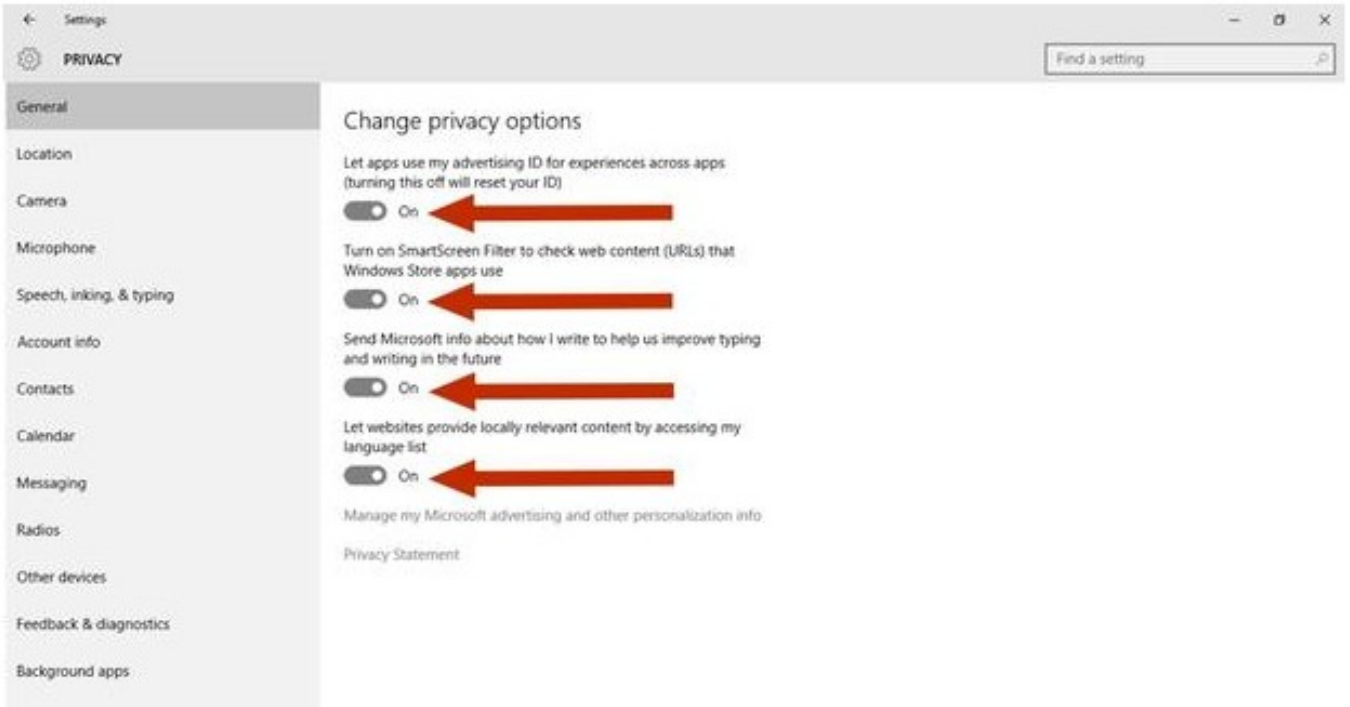
This isn't a comprehensive security checklist, but hopefully it will help you take care of some of the potential privacy issues in Windows 10.

Material on this slide and following is taken from:
http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/

# If you installed Windows 10 using Express settings, you can still disable some of the default privacy settings.

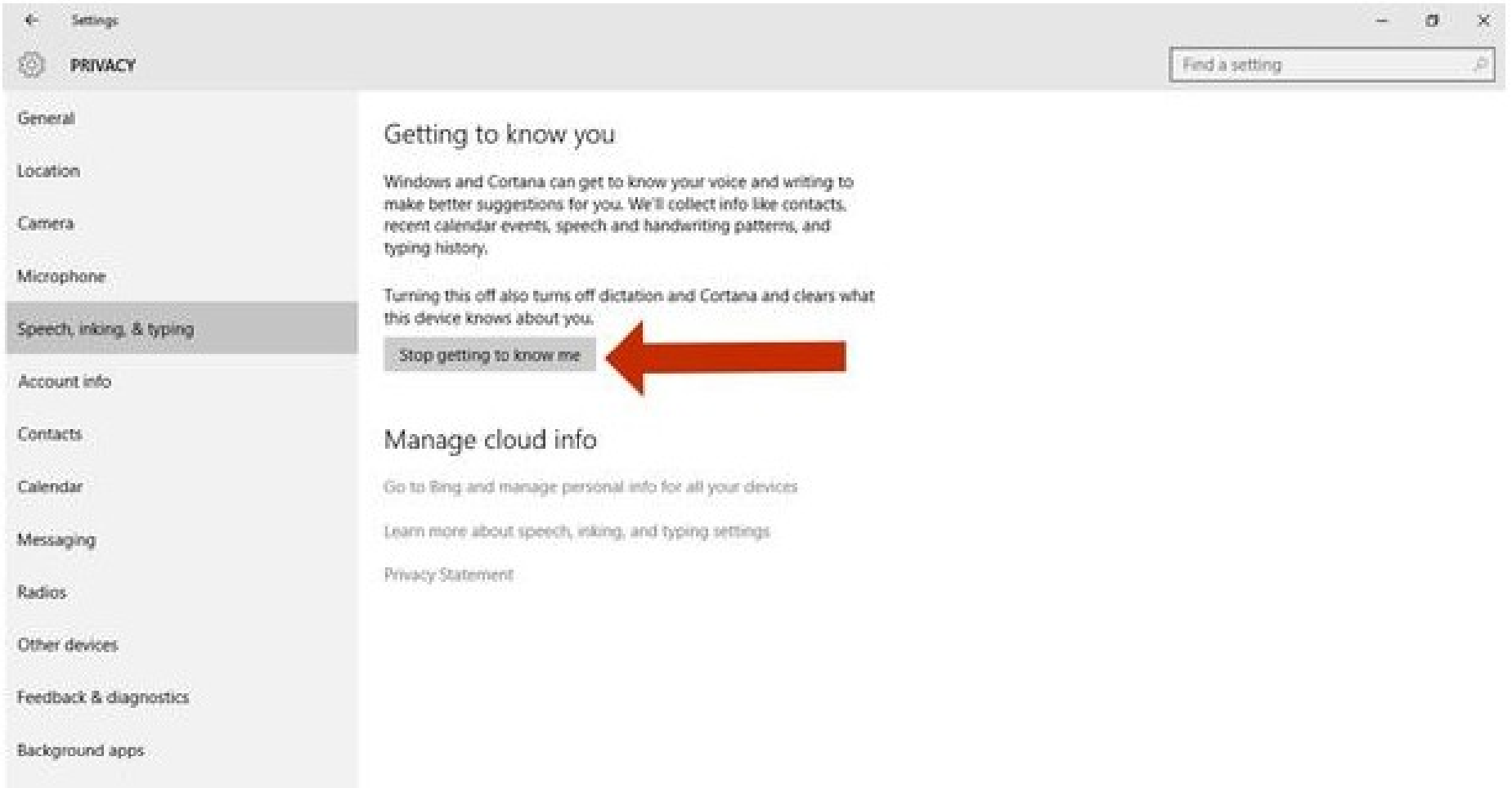
From the start button, click "Settings" and then click "Privacy" and click the "General" tab on the left sidebar. Under that tab you'll see a few sliders where you can toggle certain features on or off.

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.



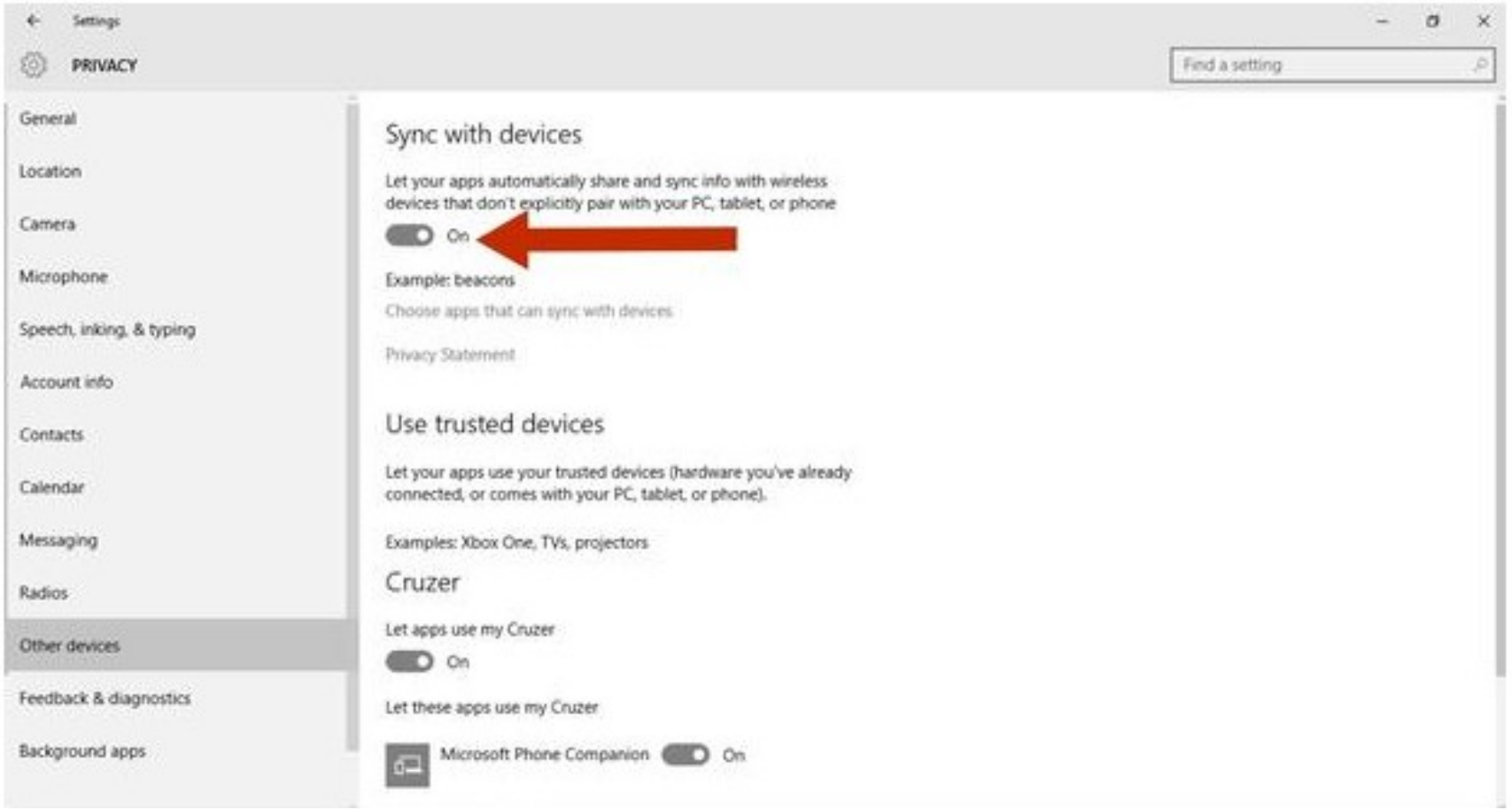
Next, you'll want to head down to the tab labeled "Speech, inking, and typing." Here you can disable Cortana from gathering information about you by clicking the "Stop getting to know me" button towards the middle of the screen.

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

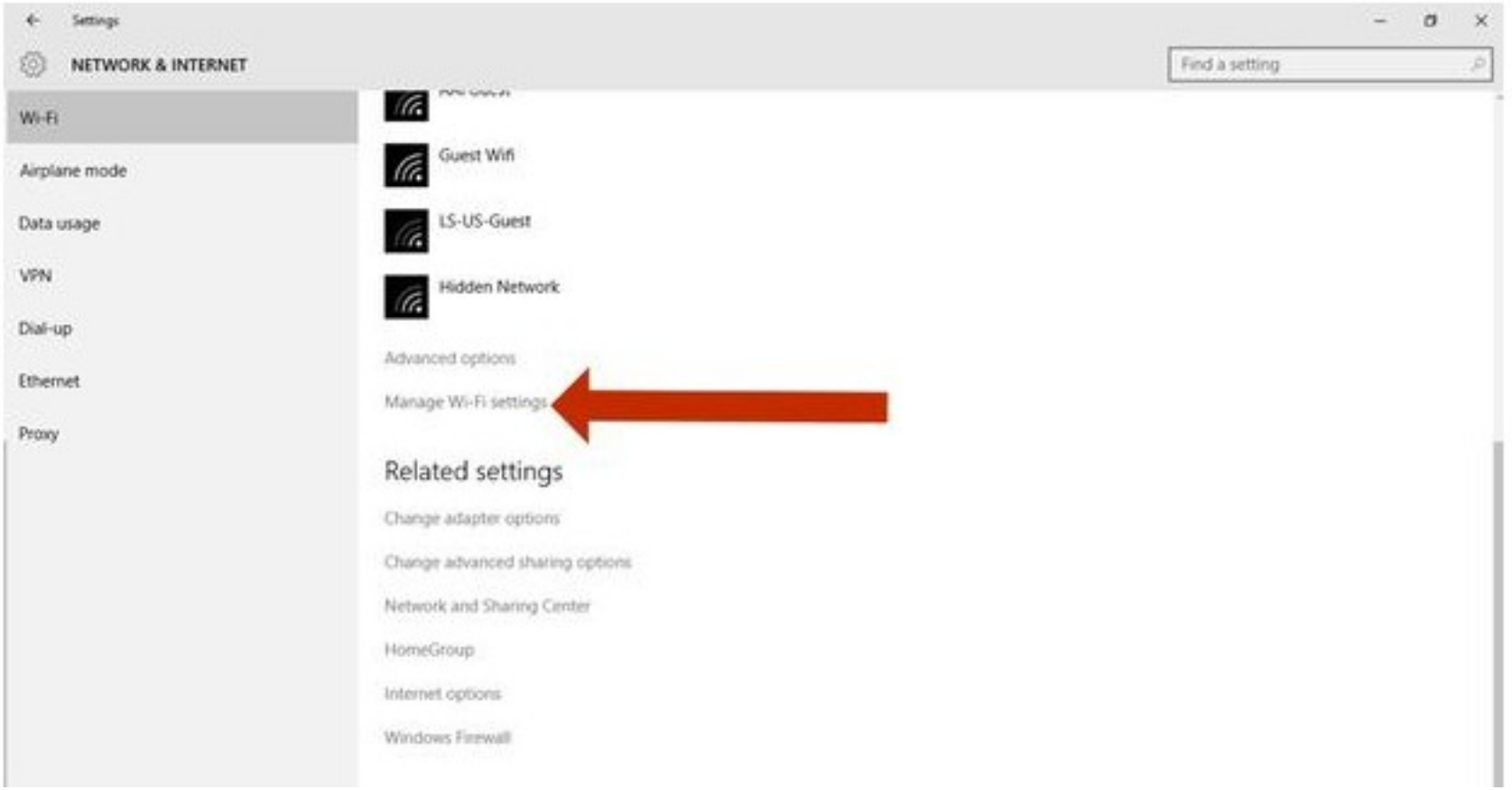


Moving on, click the "Other devices" tab at the bottom of the list. Under this tab you'll be able to turn off the "Sync with devices" feature. In the example given by Microsoft, this could be used for connecting with beacons, which are typically used for advertising purposes.

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.