

PRESERVING YOUR PRIVACY IN WINDOWS 10

MAKING SURE YOUR PRIVACY
OPTIONS ARE ON BY DEFAULT



Copyright Notice

INTRODUCTION TO WINDOWS 10 SECURITY - BY ONUORA AMOBI

UPDATED SEPTEMBER 15TH, 2015

©2015 Nnigma Inc.

All rights reserved.

Any unauthorized use, sharing, reproduction or distribution of these materials by any means, electronic, mechanical, or otherwise is strictly prohibited.

No portion of these materials may be reproduced in any manner whatsoever, without the express written consent of the Publisher or Author.

Published under the Copyright Laws of The United States of America by:

Nnigma Inc.

3579 East Foothill Blvd, Suite #254

Pasadena, CA 91107

www.Nnigma.com

Legal Notice

While all attempts have been made to verify information provided in this publication, neither the author nor the publisher assumes any responsibility for errors, omissions or contradictory interpretation of the subject matter herein.

This publication is not intended to be used as a source of binding technical, technological, legal or accounting advice.

Please remember that the information contained may be subject to varying state and/or local laws or regulations that may apply to the user's particular practice.

The purchaser or reader of this publication assumes responsibility for the use of these materials and information.

Adherence to all applicable laws and regulations, both federal, state, and local, governing professional licensing, business practices, advertising and any other aspects of doing business in the US or any other jurisdiction is the sole responsibility of the purchaser or reader.

Nigma Inc. assumes no responsibility or liability whatsoever on behalf of any purchaser or reader of these materials.

Windows 10, Windows 9, Windows 8.1, Windows 8.1 Update 1, Windows 8, Windows 7, Windows Vista, Windows XP, Surface Hub, Windows Holographic and all other related terms are registered trademarks of the Microsoft Corporation.

All Rights Reserved.

All other trademarks are the property of their respective owners.

All trademarks and copyrights are freely acknowledged.

Table of Contents

Introduction.....	5
During the Windows 10 Install	6
Using a Local Account	8
After Windows 10 Has Been Installed.....	8
Installing Updates	11
Cortana Settings	14
Disabling Telemetry	15
Microsoft Edge Browser updates.....	17
Switching to a local account	19
In Summary.....	20

Introduction

On July 29th, 2015, Microsoft began rolling out Windows 10, their best operating system so far.

A lot of work has gone into Windows 10 and it contains some pretty smart features, like Cortana, a highly intelligent voice controlled virtual assistant.

With Windows 10, Microsoft faces an interesting dilemma – how to capture as much telemetry and personal data to be useful without crossing the line of being big brother creepy.

This is a very delicate line and the software company has been trying to balance those competing imperatives with mixed results.

The challenge then for you as a consumer is to make sure that you are informed about Microsoft's default privacy settings and do as much as possible to stay protected.

Did you know that many of the default features in Windows 10 send a lot of data back to Microsoft?

Let's say that you have Windows 10 set on all the default settings.

Every single time that you type in the taskbar search box, whether it's to look for a particular file or open up an application, the local search terms that you use are sent to Microsoft, along with your location.

Some of that may be used as a way of targeting certain ads at you – you know, those banner ads that pop up? Some of those will be based on search terms that you have used.

Knowledge is power so here are a few things you can do to keep your copy of Windows 10 data-secure.

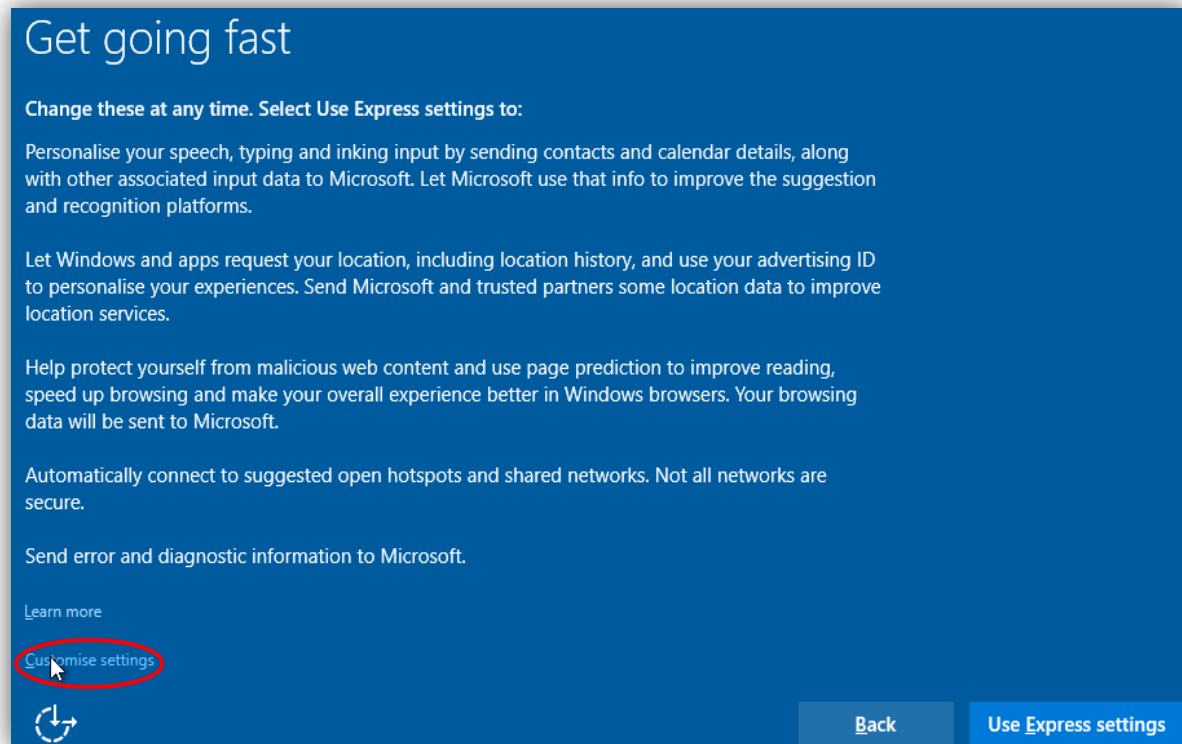
I hope these tips help you understand and feel a little more empowered about the amount of data that YOU decided to share in Windows 10.

During the Windows 10 Install

This is the bit that most people skim over, just clicking Yes to everything to get the installation moving.

First things first, make sure that you click on Customize Settings.

Do NOT go ahead with the installation with Express Settings enabled – that is the fastest way to leave your computer exposed.



On the next screen, you will be able to customize the settings.

On this screen there are settings that control:

- SmartScreen
- Page Prediction
- Connectivity to open networks
- Connectivity to friendly networks
- Sending contact and calendar information back to Microsoft
- Sending typing and inking information back to Microsoft
- Sending advertising information back to Microsoft
- Sending your information back to Microsoft partners

You can make changes here to make sure Windows 10 is sending out the levels of data and information that YOU are choosing to.

This is not a right or wrong thing, ***just make sure you understand what you are giving Microsoft permission to do.***

Customise settings

Browser and protection

Use SmartScreen online services to help protect against malicious content and downloads in sites loaded by Windows browsers and Store apps.

Off ☐

Use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.

Off ☐

Connectivity and error reporting

Automatically connect to suggested open hotspots. Not all networks are secure.

Off ☐

Automatically connect to networks shared by your contacts.

Off ☐

Send error and diagnostic information to Microsoft.

Off ☐



Back

Next

Customise settings

Personalisation

Personalise your speech, typing and inking input by sending contacts and calendar details, along with other associated input data to Microsoft.

Off ☐

Send typing and inking data to Microsoft to improve the recognition and suggestion platform.

Off ☐

Let apps use your advertising ID for experiences across apps.

Off ☐

Location

Let Windows and apps request your location, including location history, and send Microsoft and trusted partners some location data to improve location services.

Off ☐



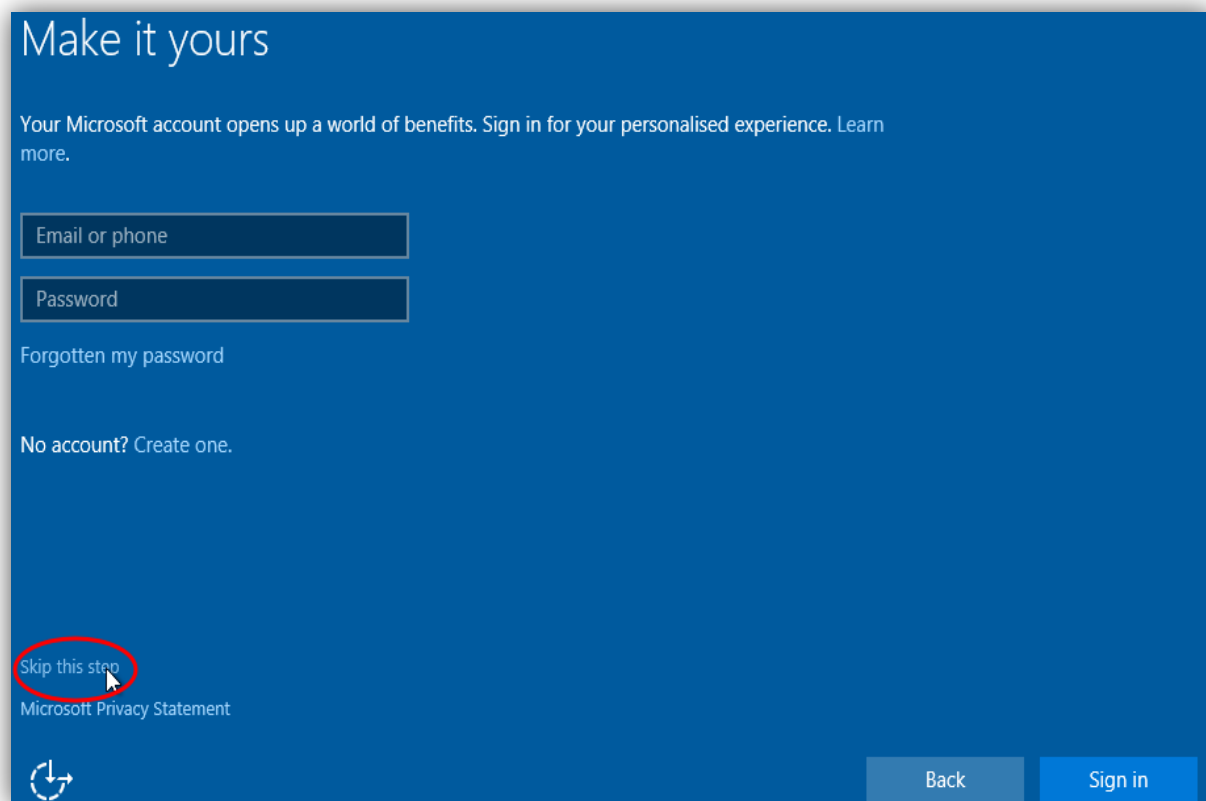
Back

Next

Using a Local Account

If data privacy is also of utmost importance to you, another thing you can do is use a local account.

In other words, when the Make it Yours screen appears, just click on ***Skip this Step***



After you have done that, you can continue to follow the installation instructions safely.

Keep in mind there is a trade-off between the ability to use cloud services and more personalized Microsoft features and the ability to keep your data local.

You have to decide at all times whether these trade-offs are worth it.

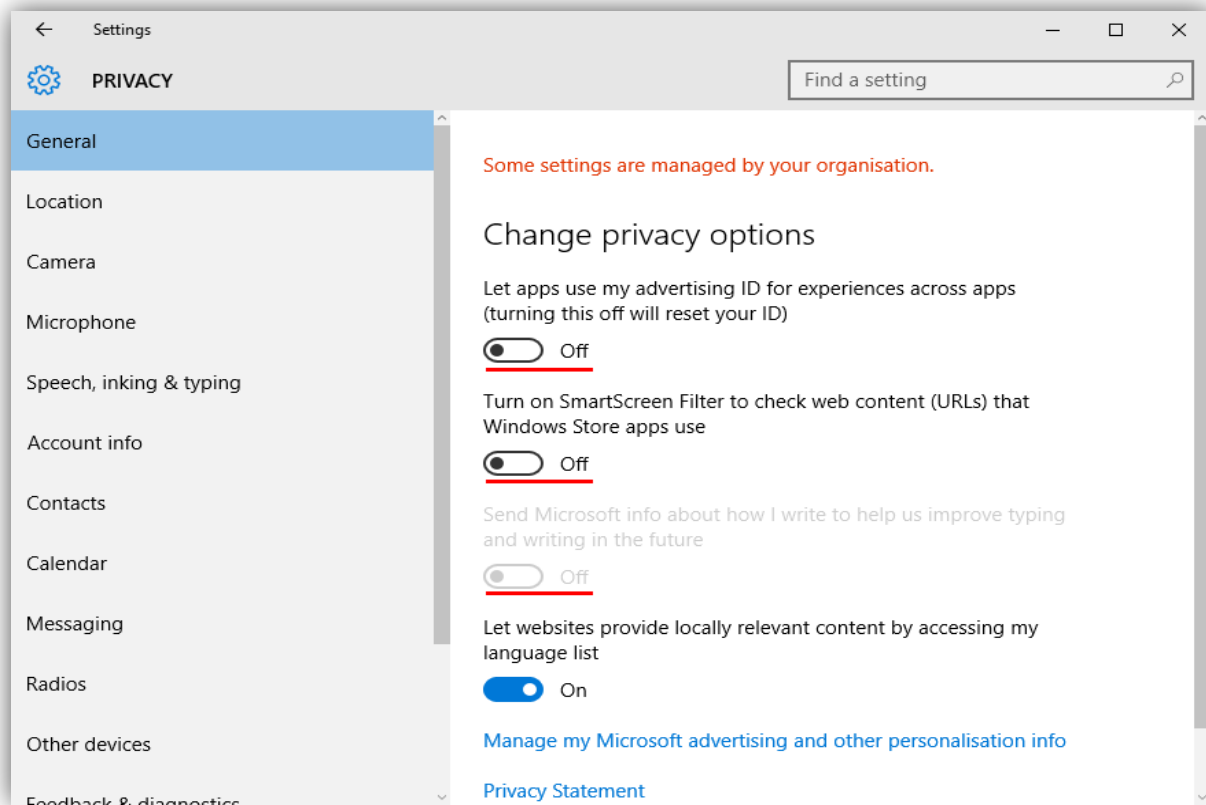
After Windows 10 Has Been Installed

Now that you have Windows 10 installed on your computer, its time to start disabling certain settings.

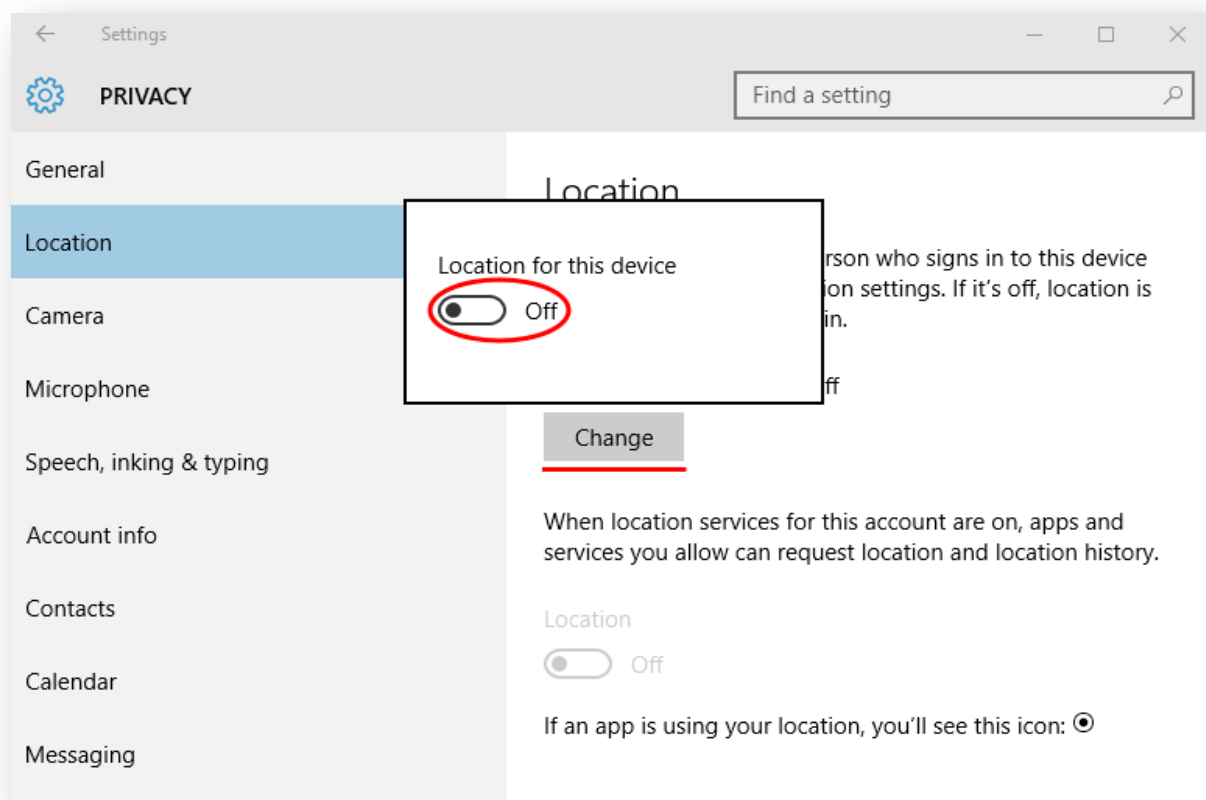
First, open up **Settings>Privacy** and then disable everything, unless there are any specific things that need to remain enabled, for example, letting certain websites have access to your language list.

If you do nothing else, pay special attention to the following tabs and pages:

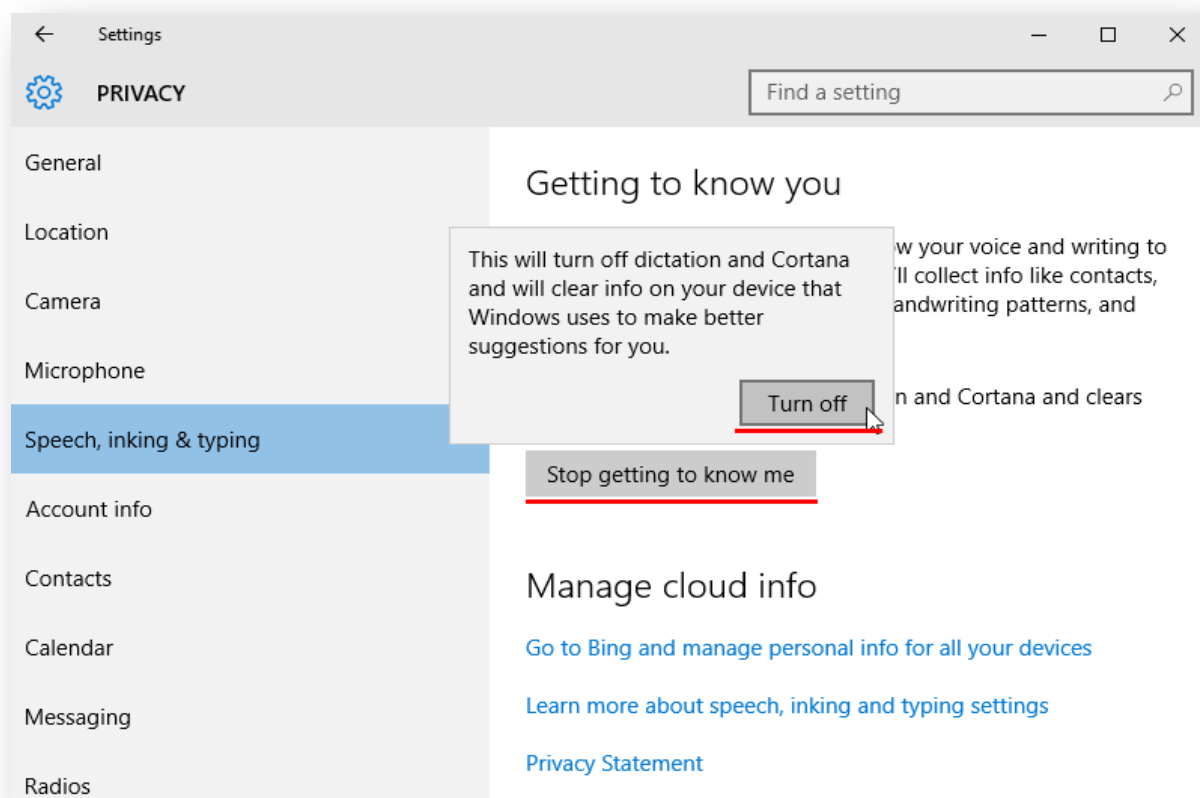
General



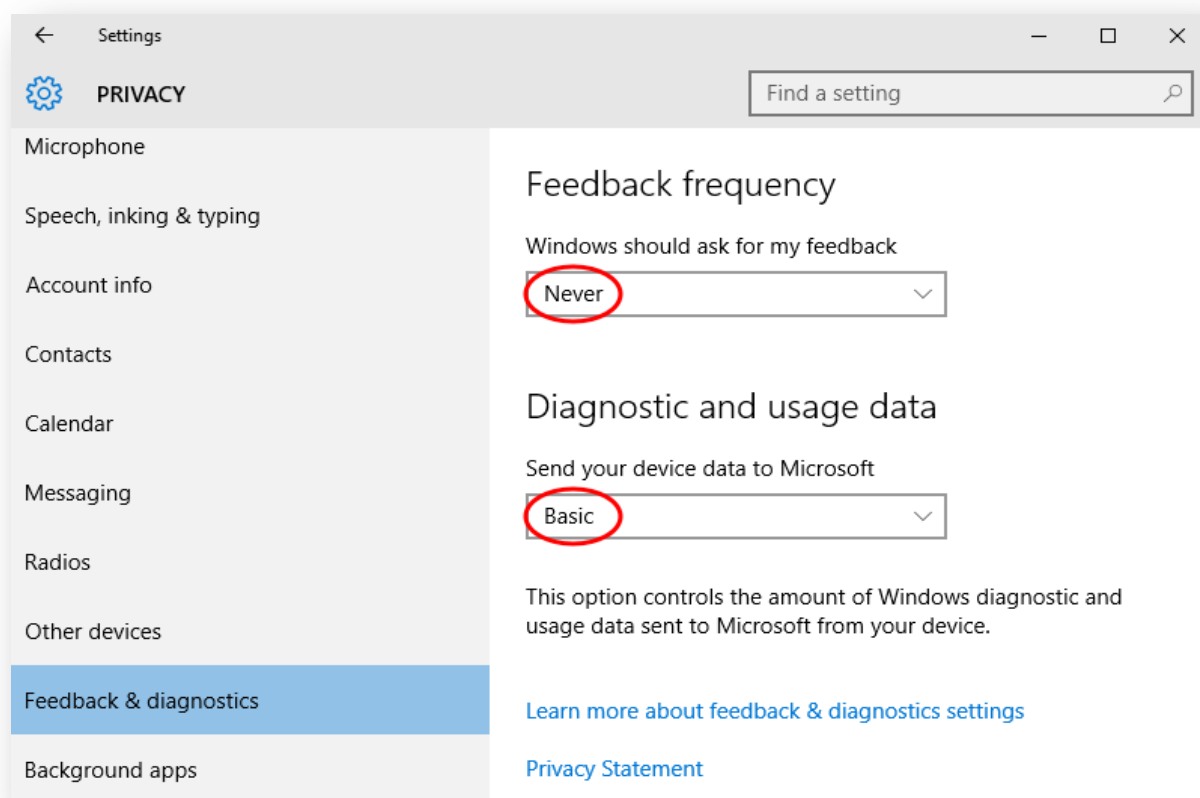
Location:



Speech, inking & typing:

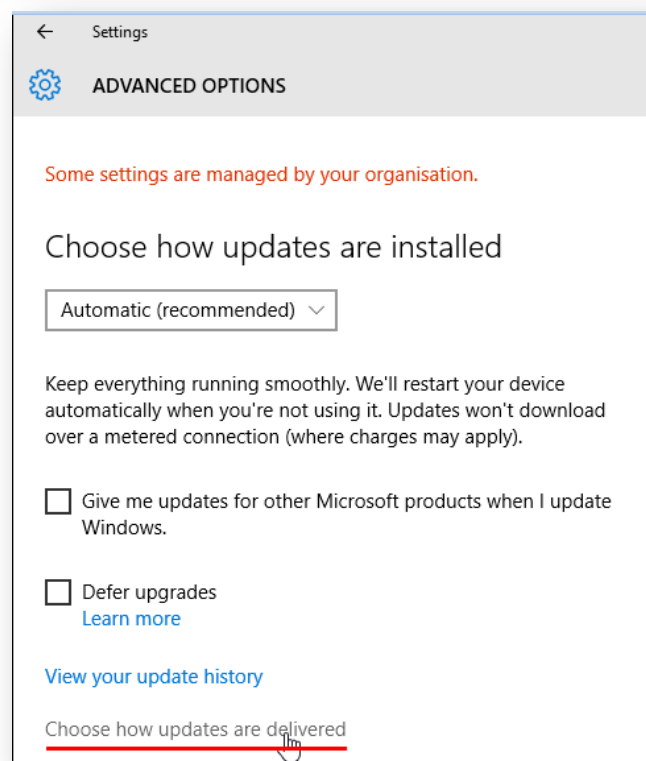
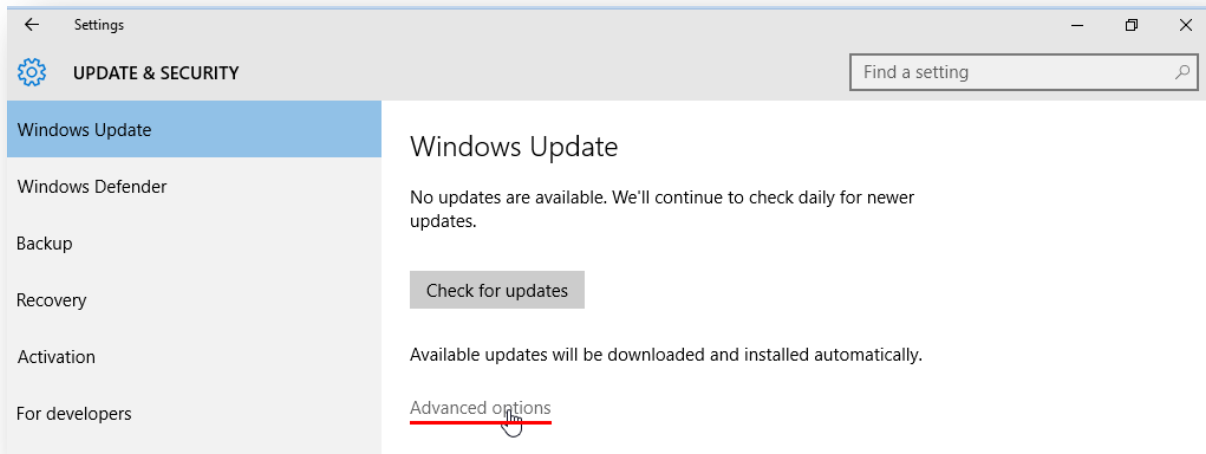


While you are in the Privacy settings, head on over to the Feedback & Diagnostics section. In the first box, select **Never** and in the second box select **Basic**.

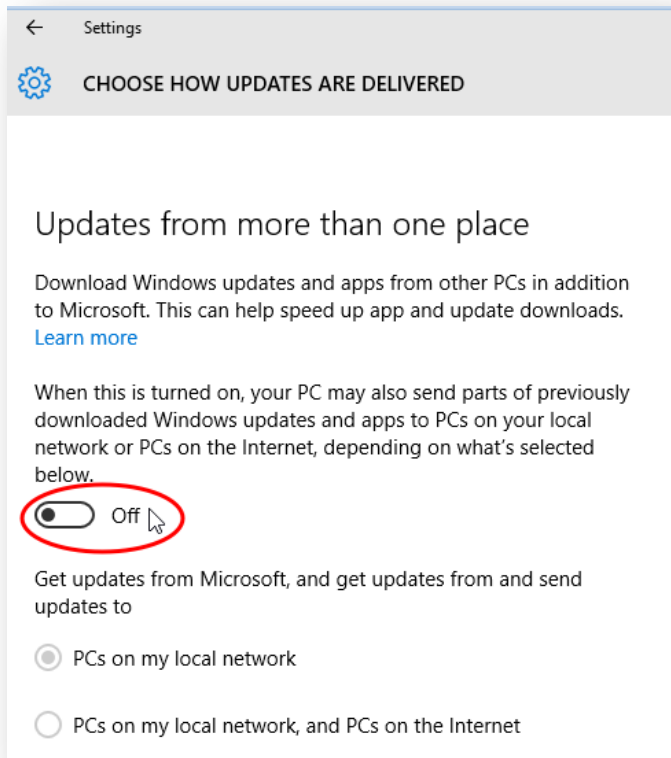


Installing Updates

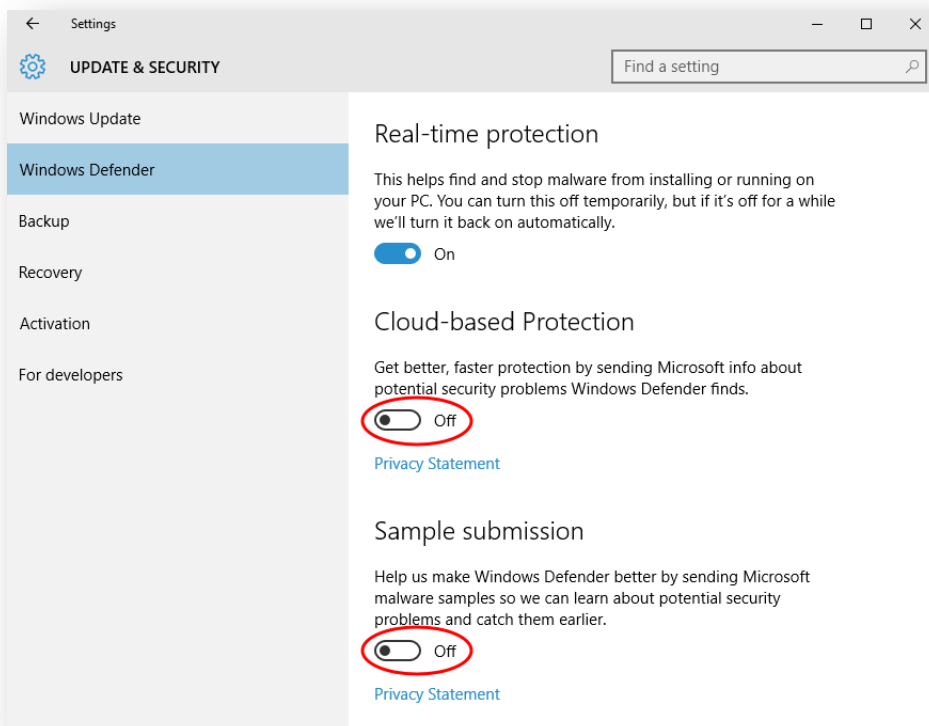
Now go to **Settings>Update & Security>Windows Update>Advanced Options>Choose How Updates Are delivered.**



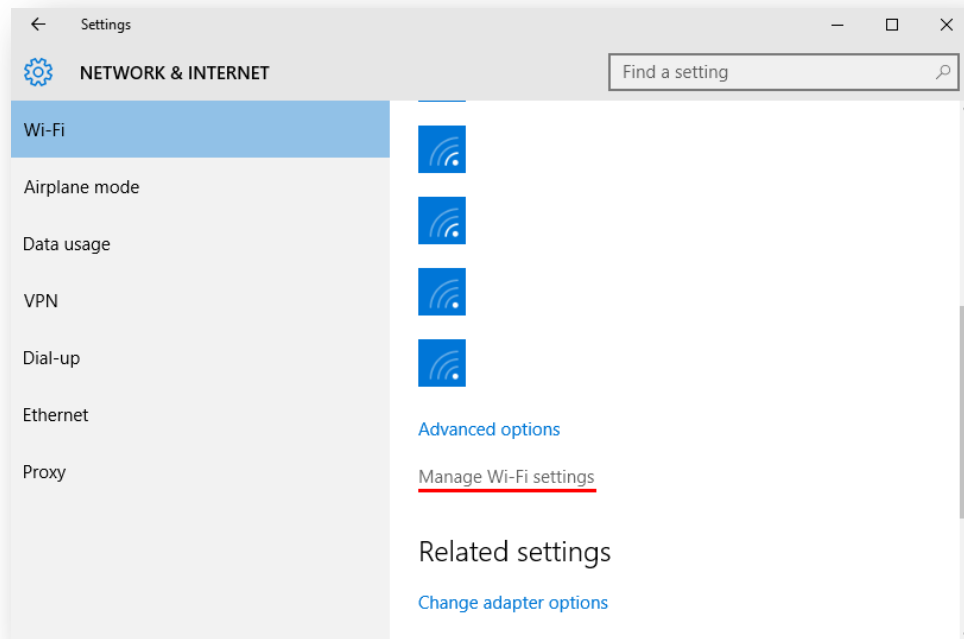
Turn off the first switch



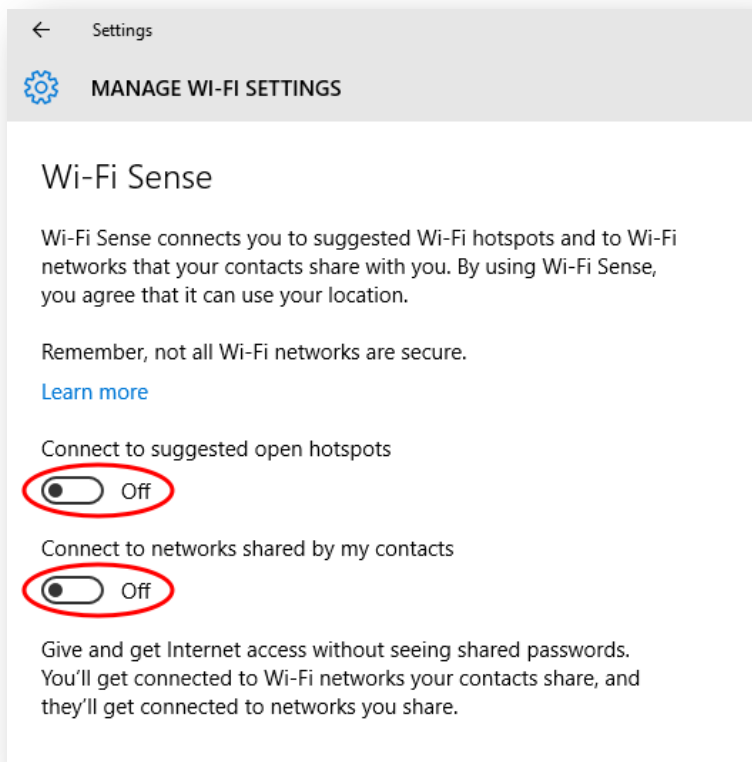
While you are in the Update & Security settings, click on **Windows Defender** and disable Cloud based Protection and Sample Submission.



Now go to **Settings>Network & Internet>Wi-Fi>Manage Wi-Fi Settings**.

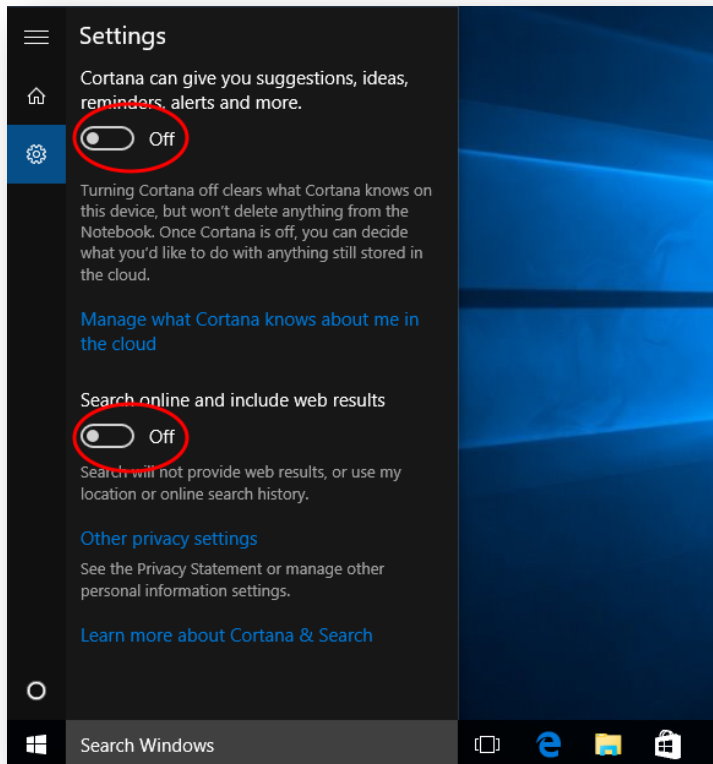


You can disable **Wi-Fi Sense** by turning off both of the switches



Cortana Settings

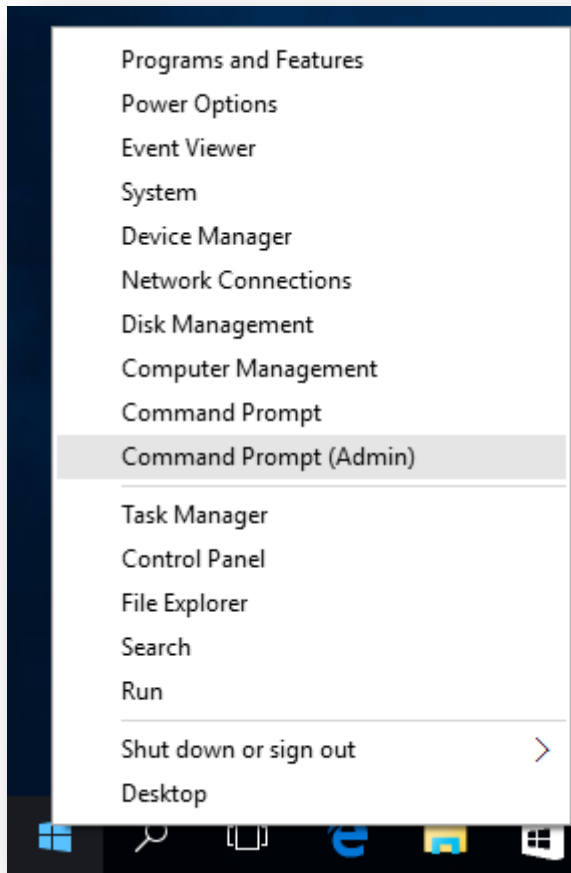
Turn off **Cortana** and web search in “**search bar**” by clicking it, clicking the cog icon to go into **Settings** and then turning off both of the switches



Disabling Telemetry

To turn off Telemetry, open the command prompt as an administrator.

Do this by right-clicking on the Start button or by using the shortcut Win+X



And then typing in this:

- `sc delete DiagTrack`
- `sc delete dmwappushservice`
- `echo "" > C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-Diagtrack-Listener.etl`
- `reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection" /v AllowTelemetry /t REG_DWORD /d 0 /f`

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc delete DiagTrack
[SC] DeleteService SUCCESS

C:\Windows\system32>sc delete dmwappushservice
[SC] DeleteService SUCCESS

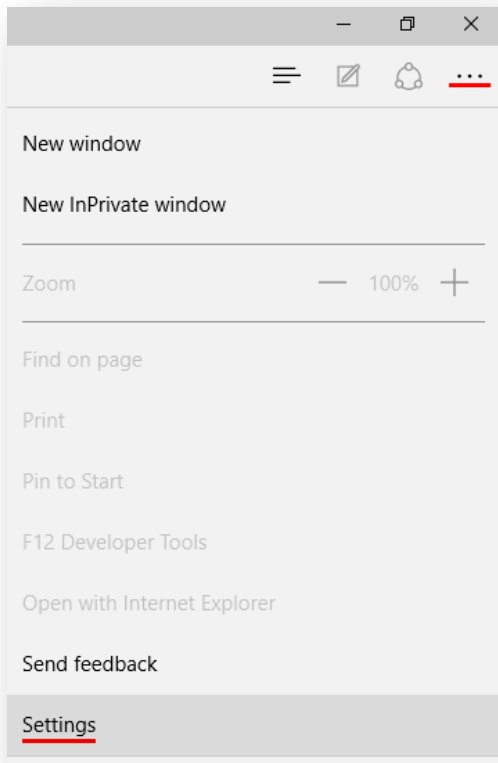
C:\Windows\system32>echo "" > C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-Diagtrack-Listener.etl

C:\Windows\system32>reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection" /v AllowTelemetry /t REG_DWORD /d
0 /f
The operation completed successfully.

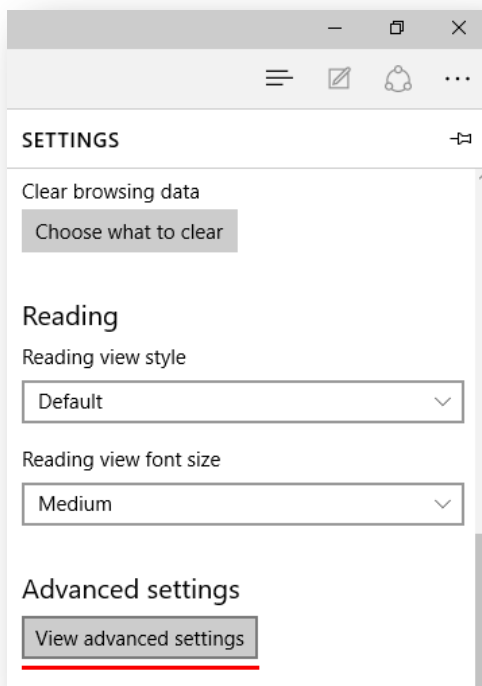
C:\Windows\system32>
```


Microsoft Edge Browser updates

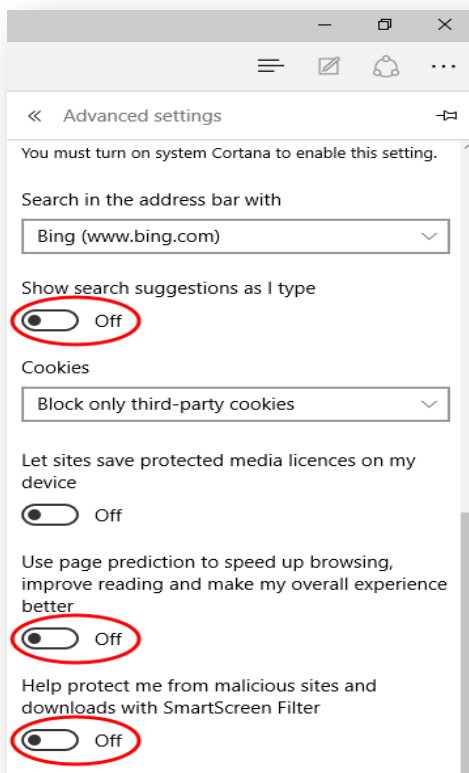
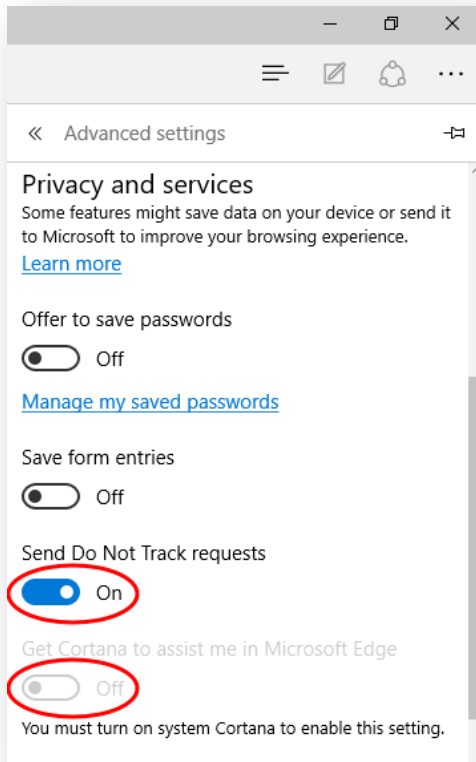
To set up the new Edge browser to protect your privacy, first open it. Then click on More Actions followed by Settings



Then click on **View Advanced Settings**



Now enable **Do Not Track Requests** and disable the search suggestions, the SmartScreen filter and page predictions. Also ensure that Cortana is off as well.

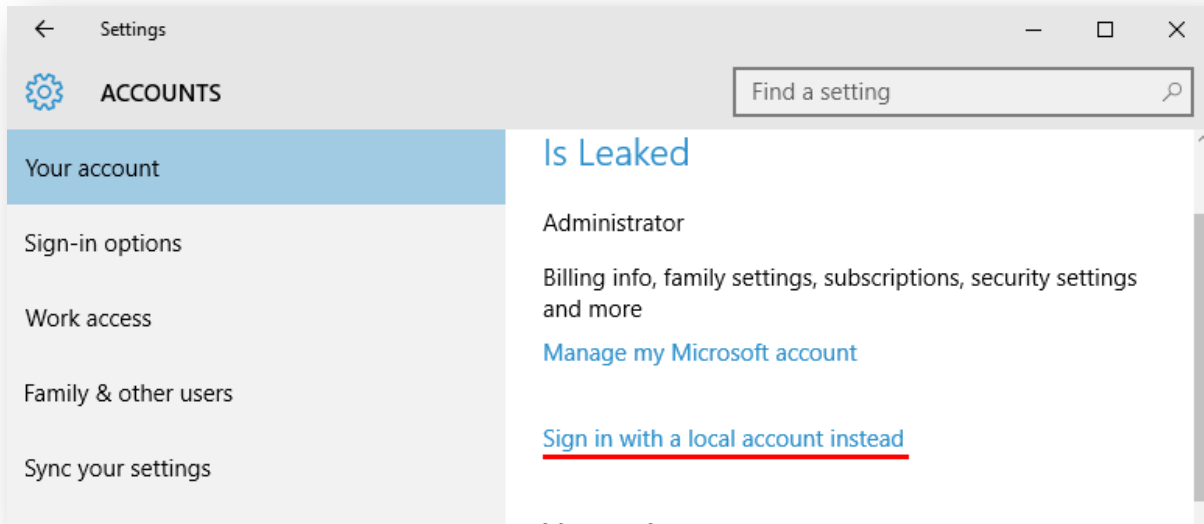


You should now find that the ad banners show ads that are not based on any of your search requests and interests.

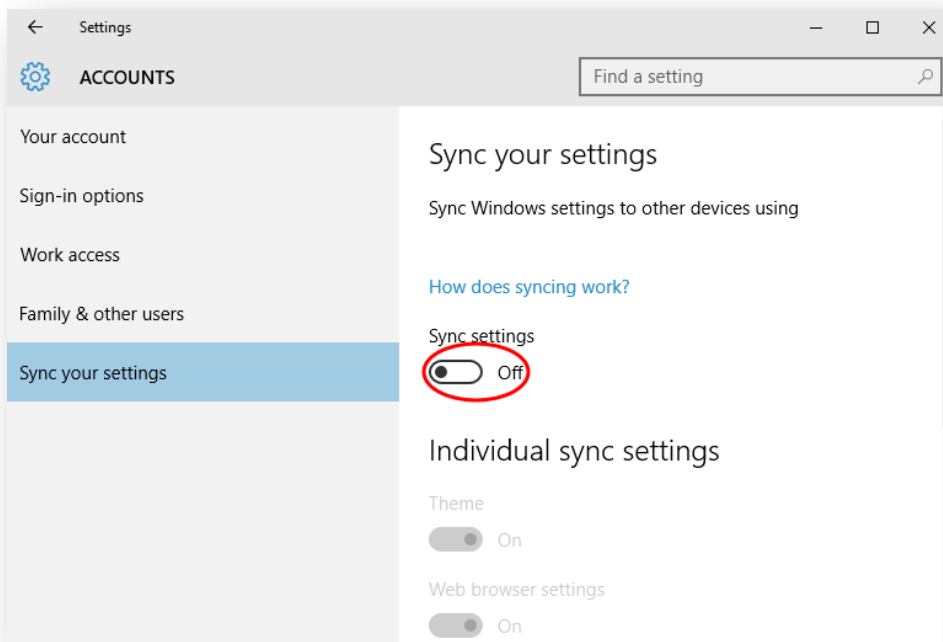
Switching to a local account

Finally, if you are using a Microsoft account, you should change over to a local account. You can do this by going to **Settings>Accounts>Your Accounts**.

Click Sign In With a Local Account Instead and then follow the instructions on the screen



If you are unable to do this, instead you can disable Sync Settings. Open **Settings>Accounts>Sync Your Settings** and disable it



In Summary

Windows 10 is hands down the most powerful and effective Operating System that Microsoft has ever put together.

As someone who covered the Windows 10 development process from day one at <http://www.windows10update.com>, I can tell you that the Operating System was built largely based on feedback from users just like you.

There is no right or wrong here, users just need to understand how to use the options in the software they are installing. Facebook, Google and all the large companies want to understand a lot more about you so they can help you AND sell you goods and services.

Microsoft is no different.

As I said earlier, the tension between Operating System effectiveness and privacy intrusion is something that will be with all of us for a while.

Hopefully the steps outlined in this book will help you take the first steps toward creating the level of privacy in Windows 10 that you want.

I would love to hear back from you with your questions and comments.

You can send me emails to privacy@windows10update.com

Thanks for reading and I hope you had as much fun reading this as I had writing it.

Regards,

Onuora Amobi

P.S. You can also find additional Windows 10 training resources on our **Windows 10 training page** here.

<http://www.windows10update.com/windows-10-training/>

Also check out our new training classes including:

Introduction to Windows 10

<https://www.udemy.com/introduction-to-windows-10/>

Setting up Windows 10 for a small business

<https://www.udemy.com/setting-up-windows-10-for-small-business/>