
MUO
THE COMPLETE GUIDE TO
WINDOWS 10
PRIVACY SETTINGS
by Gavin Phillips

The Complete Guide to Windows 10 Privacy Settings

Written by Gavin Phillips

Published October 2016.

Read the original article here: http://www.makeuseof.com/tag/complete-guide-windows-10-privacy-settings/

Table of contents

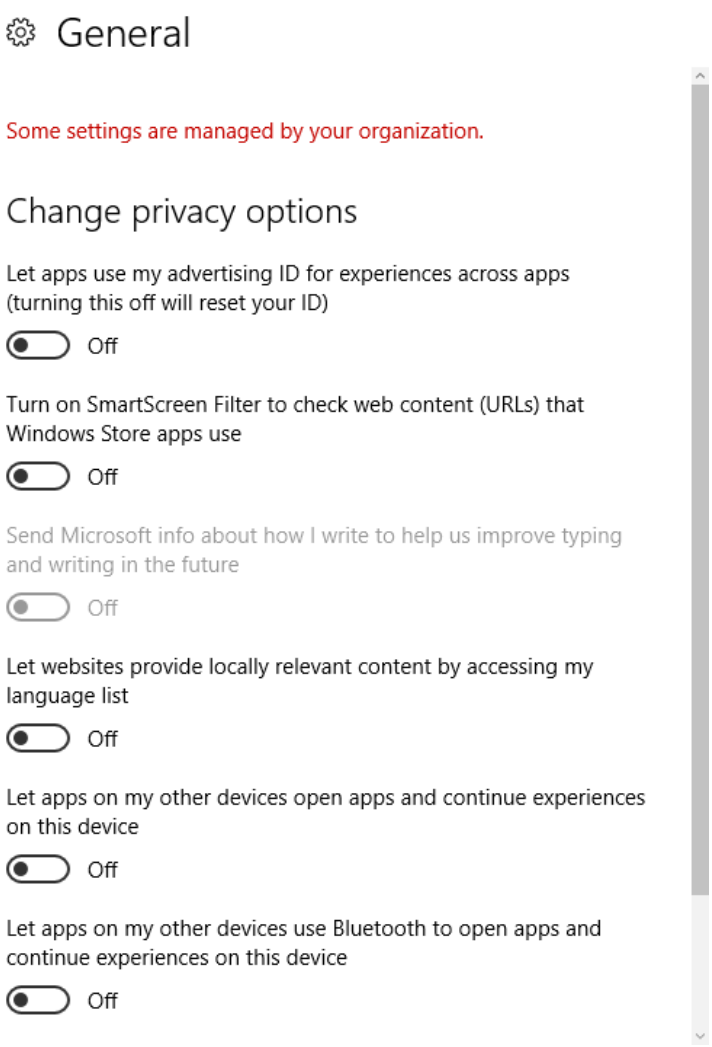
The Windows 10 Anniversary Update brought forth an almost staggering number of changes. The update arrived in the first week of August, 2016, and its worldwide roll-out is expected to complete this month. This is a good time to explore the changes to all the **Windows 10 privacy settings** we're still learning to live with.

What follows is a page-by-page guide of Windows 10 Anniversary Update (referred to as AU forthwith) privacy settings, **so you know exactly what to toggle, when to toggle it**, and why you'd want to toggle it.

To access Windows 10 Settings, press the keyboard shortcut **Windows key + I**, then head to **Privacy** or go to **Start > Settings > Privacy**.

General

This page contains your general privacy settings, including options for SmartScreen Settings.



Advertising ID

Your advertising ID is linked to your Microsoft account, acting much like the trackers that follow you around the internet to deliver personalized adverts. This is a matter of personal preference. You're likely to see adverts if you use the internet: do you want those ads to be personalized to your viewing and purchasing decisions?

To create a more customized online experience, some of the ads you may receive on Microsoft websites and apps are tailored to your previous activities, searches and site visits.

These refer to the adverts displayed throughout Microsoft services, such as your Start menu or Universal Apps. **Read more about opting-out right here.**

SmartScreen Filter

The SmartScreen Filter is an integrated Windows 10 feature, as it has been for several previous versions. The SmartScreen Filter actively scans Windows Store and Microsoft Edge / internet Explorer browser URLs and content **for any malicious activity**:

- As you browse the web, it analyzes pages and determines if they might be suspicious. If it finds suspicious pages, SmartScreen will display a warning page, giving you an opportunity to provide feedback and advising you to continue with caution.
- SmartScreen checks the sites you visit against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen will show you a warning letting you know that the site has been blocked for your safety.
- SmartScreen checks files that you download from the web against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen will warn you that the download has been blocked for your safety. SmartScreen also checks the files that you download against a list of files that are well known and downloaded by many people who use internet Explorer. If the file that you're downloading isn't on that list, SmartScreen will warn you.

If you use Microsoft Edge or internet Explorer, or indeed, regularly use Windows Store Universal Apps, the SmartScreen Filter can be a handy additional layer of security, filtering malicious content from your system. If you use none of those tools, you can likely turn this off.

Send Info About Writing

Only applicable to those using mobile or tablets (or novel input methods on a regular system). It'll improve autocomplete, spelling corrections, and so on. It is automatically grayed-out on laptops and desktops, and I would personally turn it off if I were using a tablet or mobile.

Access My Language

Microsoft and Windows can use your language settings to ensure locally served content matches up. If you're English, this really isn't much of a problem, given that the internet defaults to English. However, if you're not, this can be handy in ensuring site content matches your language of choice. If you'd prefer not to broadcast a list of languages installed on your system, turn it off.

Let Other Devices Open Apps

This new option allows your mobile experience to continue onto your laptop or desktop in a relatively seamless transition. This is the full evolution of Project Rome, and will allow you to send your active app and content to the same app installed on your Windows 10 desktop or laptop. In a show of good form from Microsoft, this feature isn't limited to Windows devices, meaning you'll be able to **transition from iOS and Android devices**, too.

This also ties nicely into another new feature that we'll take a look at a little further down the article.

Let Other Devices Open Apps Using Bluetooth

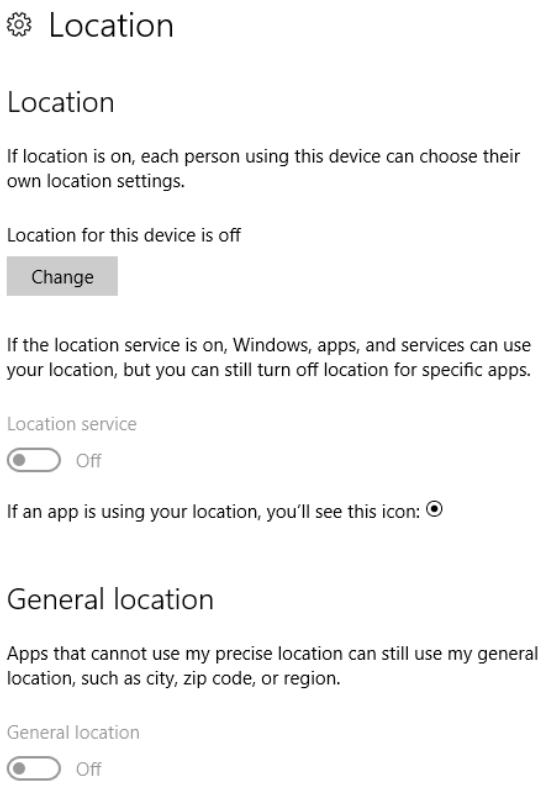
This is a new option, and functions similarly to the above feature, albeit using your local Bluetooth connection instead of an internet connection.

Change Privacy Options Roundup

With two new options focusing on functionality, workflow, and the transition between our various devices, Microsoft has implemented a useful tool that I'm sure many make excellent use of.

Location

This page contains your location-based privacy settings.



Location

When the location service is turned on “Windows, apps, and services can use your location, but you can still turn location off for specific apps.” Meaning you’ll receive more accurate localized information. In certain apps, especially for those using mobile versions of Windows 10, this can be handy e.g. if you search for something general, search returns localized results.

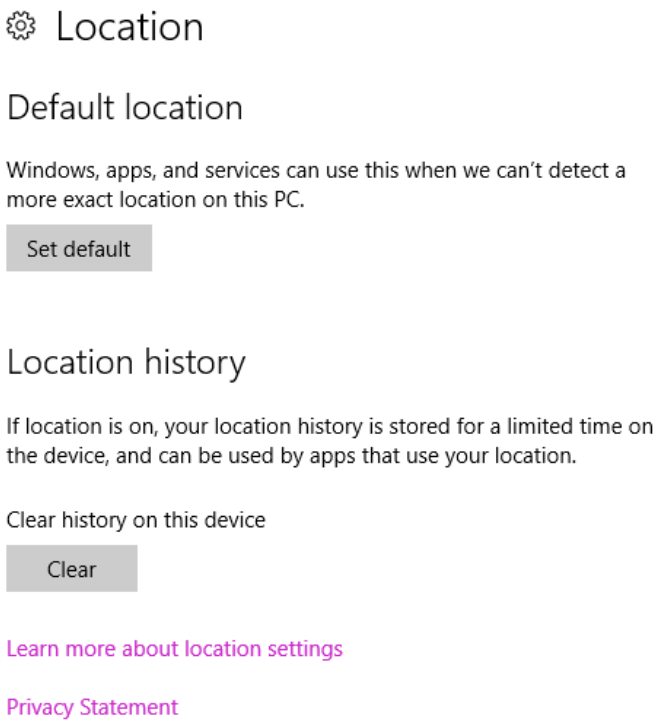
However, to do this, the location service may share your location results with “Trusted Partners”. I’m firmly in the off camp, but there are countless other apps and websites doing this otherwise, so it is up to you.

General Location

In an extension and “loophole” for the above location settings, Microsoft introduced the General Locations setting. This allows you to turn off location settings for the entire system, but still provide certain apps with “your general location, such as city, zip code, or region”. Handy if you move around a lot, as it’ll save you figuring out your zip or postcode every time you search for a specific local service.

Default Location

This is another handy extension to the location service. Enter your default location here, and Windows 10 will provide these criteria when requested by apps or other services. It saves constantly having to turn location services off, or updating your details when you move around, and ensures only one set of data is being broadcast.



Location History

If the location service is turned on, this option will maintain a short history of your recently visited places. During the limited period — "24 hours in Windows 10" — other apps installed on your system may be able to access this history. Those with access will be labelled **Uses location history** on your location settings page.

Geofencing

> *Some apps use geofencing, which can turn on or off particular services or show you information that might be useful when you're in an area defined (or "fenced") by the app.*

This means, if turned on, an app might use specific location information to turn on and provide you relevant information. Think along the lines of a weather report from a new location.

If any apps are using geofencing, you'll see **One or more of your apps are currently using geofencing** displayed on your locations settings page.

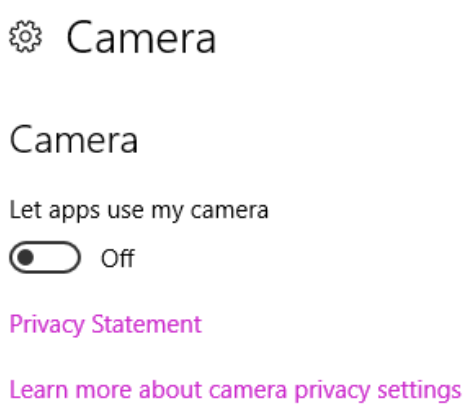
Location Options Roundup

There is **no single option for Cortana** in the location settings, but you'll note "she works best when she has access to your device location and location history." In fact, she won't work at all without your location, so bare that in mind if you want to make the most of the Windows 10 assistant.

Cortana drew a significant amount of ire when she appeared in Windows 10. If turned on, Cortana periodically checks your location and updates the range of search suggestions that could be returned. **If you don't want Cortana to have access to your device location, you'll need to turn her off completely.**

Camera

This page contains privacy settings for your camera.



Choose apps that can use your camera

Microsoft defines three camera types:

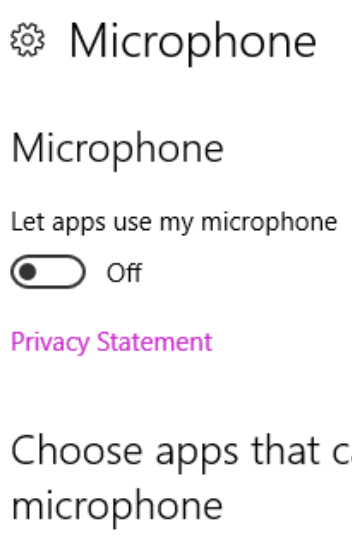
- **Color** — Used for taking traditional color photos and videos.
- **Infrared** — Takes a greyscale photo or video based upon infrared intensity.
- **Depth** — Can see the shapes of items in front of it, and how far they are from the device.

> *Some people worry about unknown apps, organizations, or malware using their camera. Whenever your camera is used, you should be in charge.*

And with that in mind, Microsoft gives you full control over the individual apps that might request access to your camera. I would advise managing access on an app-by-app basis, without forgetting those **other basic camera privacy strategies**, which everyone should be putting to use.

Microphone

This page contains privacy settings for your microphone. The settings are very similar to those offered for apps making use of a camera. You'll be able to decide which apps you want to grant access to on a case-by-case basis.

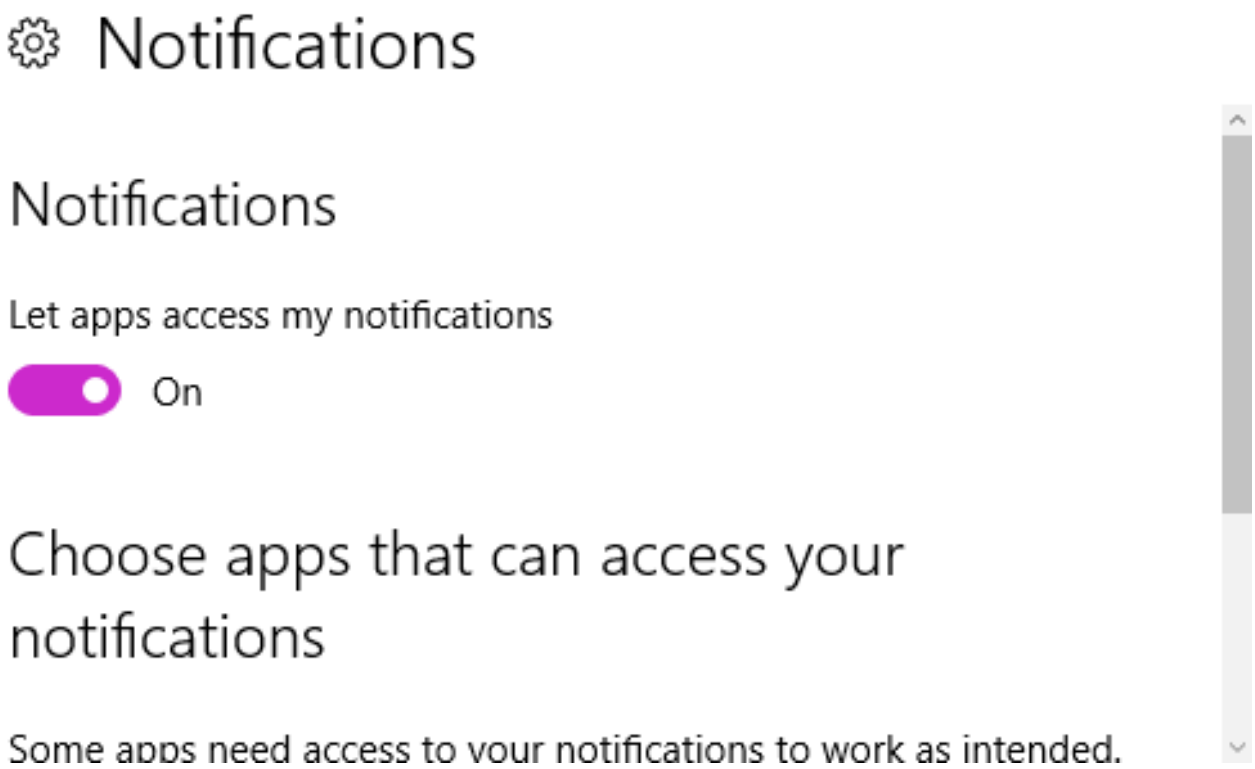


Some users consider microphones to be a security risk. On numerous occasions microphones have been turned on and used as a covert listening device. In this instance, Windows 10 users have raised concerns that their speech will be recorded without prior permission, or that their Cortana speech-searches will be recorded for longer than expected, or used against them at another time.

These concerns represent a core aspect of mistrust towards Microsoft. You can read more in the upcoming "Speech, Inking, and Typing" section.

Notifications

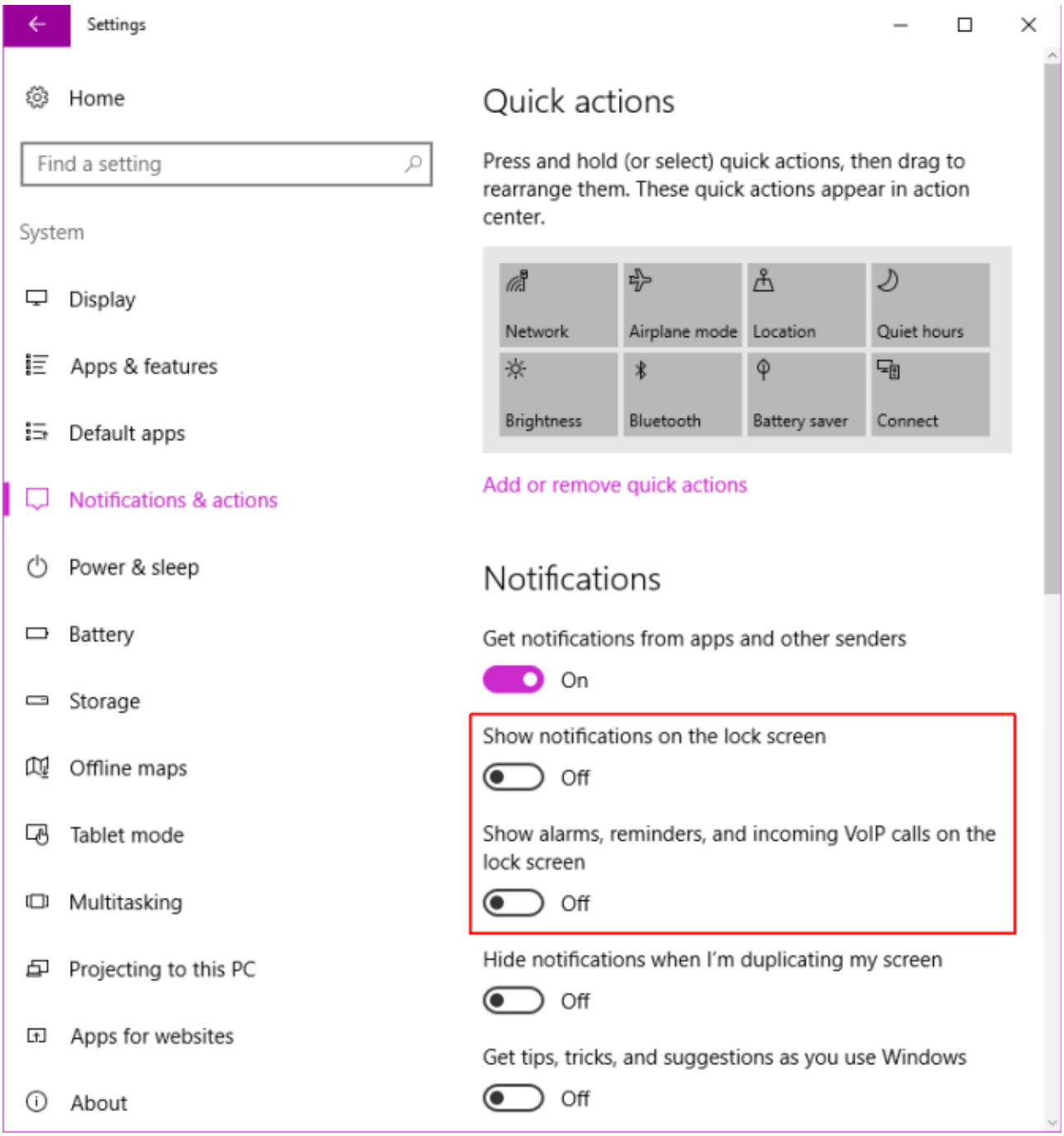
This page deals with your device notifications.



Apps that have access to notifications can post to your desktop notification bar. These notifications can come from a range of sources, such as email accounts and calendars, Cortana, Windows Defender, Windows Update messages, and so on.

Notifications within Windows 10 are, for me, an irritant to be turned off. However, I would be more vary with Windows Lock Screen notifications. These may display unwanted information in a public place without you realizing.

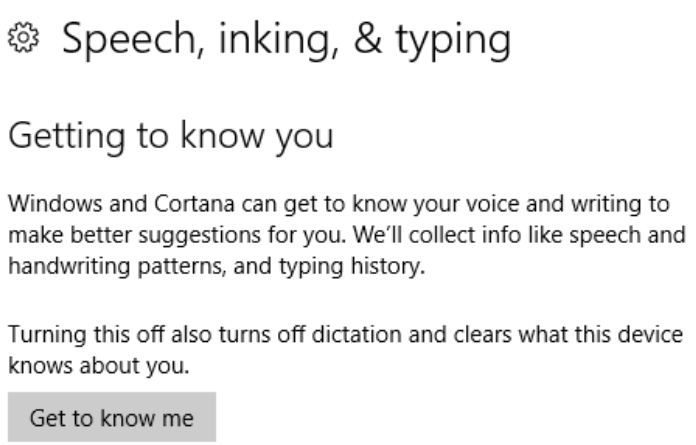
To turn these off, head to **Settings > System > Notifications & Actions**. Adjust the following settings:



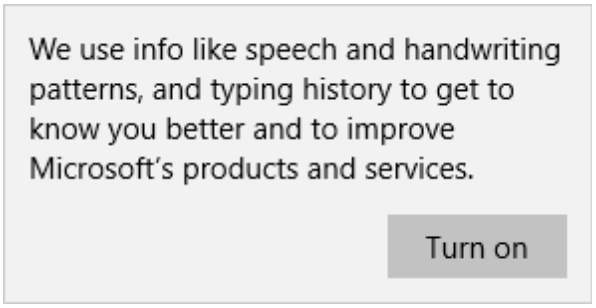
Notifications will no long display on your lock screen.

Speech, Inking, & Typing

This page contains settings concerning machine learning, and how you want the “getting to know you” process to transpire.



If you’re using Cortana, you might want to keep this turned on. Cortana will learn the specific pronunciation and tone of voice, or the nuances of your handwriting style to allow for faster results when using the service. To further streamline the service, Microsoft also collects and collates your calendar and contact list to **assist Cortana to** “better recognize people, events, places, and music when you dictate messages or documents”.



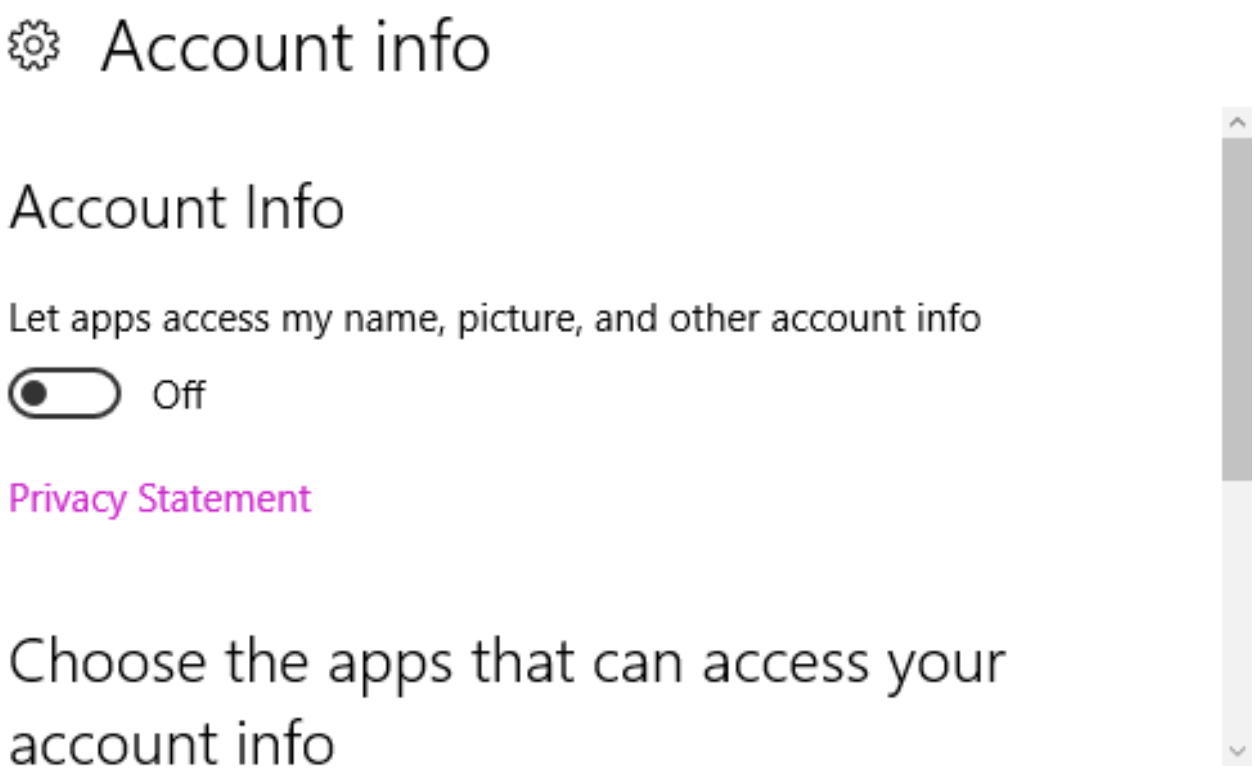
The collection of data relating to Speech, Inking, and Typing, along with the “Send Microsoft info about how I write” setting, provoked a massive amount of backlash **when Windows 10 arrived in 2015**. Microsoft purposefully uses extremely vague language to keep their service options open. When coupled with the equally vague language used in the Microsoft EULA (which also drew considerable ire), a proportion of users developed a strong belief Windows 10 had been developed primarily as a spying tool.

> *To use voice input in Cortana, **Getting to know you** (the privacy setting for Speech, inking, and typing) must be turned on. This is because Cortana and speech services exist both in the cloud and on your device. And the info Microsoft collects from these services in turn helps to improve them. Speech services that don’t rely on the cloud and only live on your device, like Narrator and Windows Speech Recognition, will still work when this setting is turned off; but Microsoft won’t collect any speech data without your consent.*

Were they wrong? I’ll elaborate on this question at the end of the article, so read on!

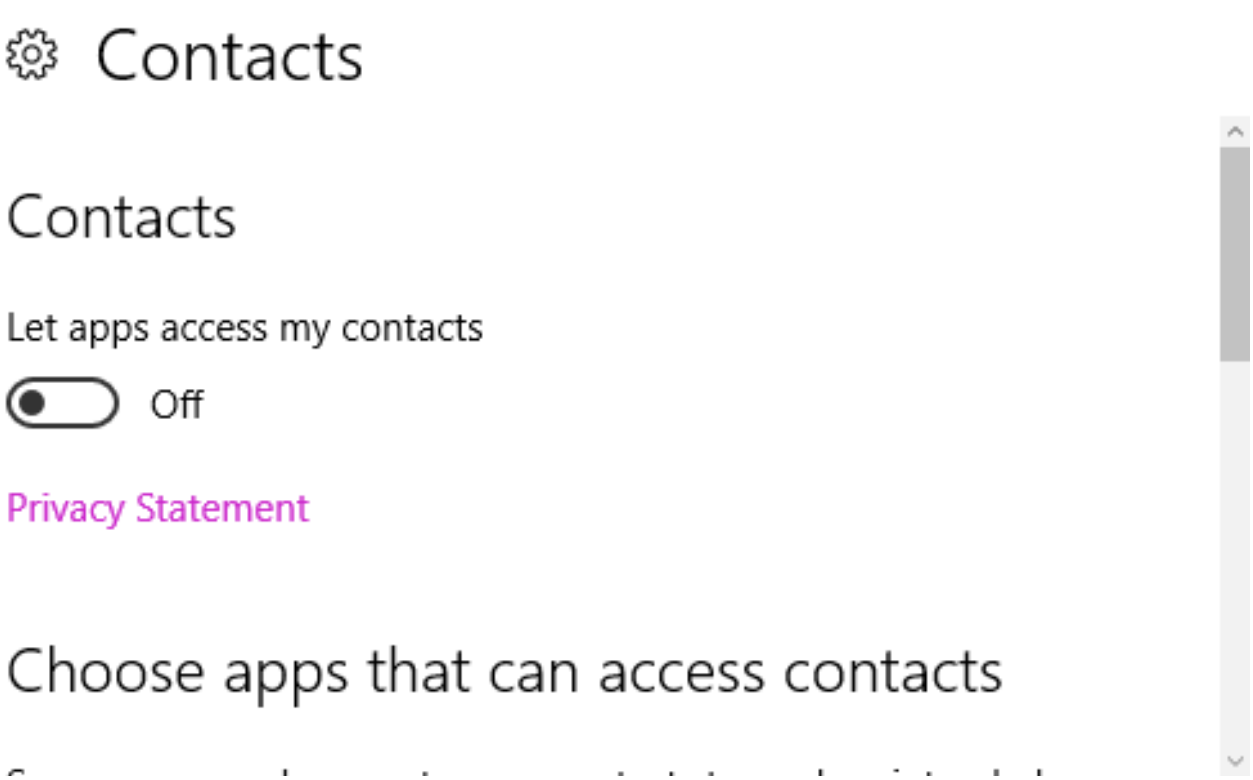
Account Info

This page **contains information relating to your Microsoft account**, specifically affecting how your email address, name, and account image is used with your installed apps.



It will also access other account information, depending on your Microsoft account settings. This could be your location, phone number, billing details, and so.

Contacts

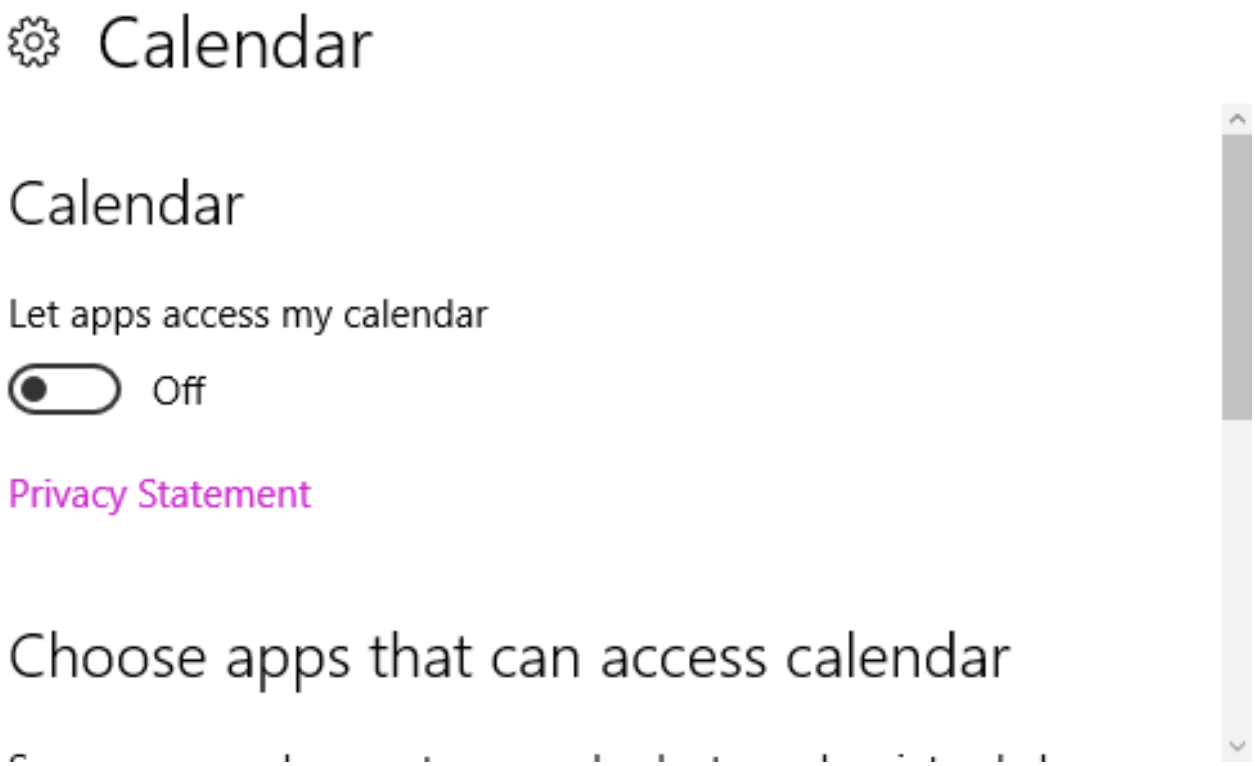


This page contains information relating to the Contacts you have stored on your Windows 10 device. As with other privacy settings, you can grant specific apps access if you so wish. Some apps may cease to function properly without access to your contact lists.

Contacts are also regularly shared between apps, including Cortana.

Calendar

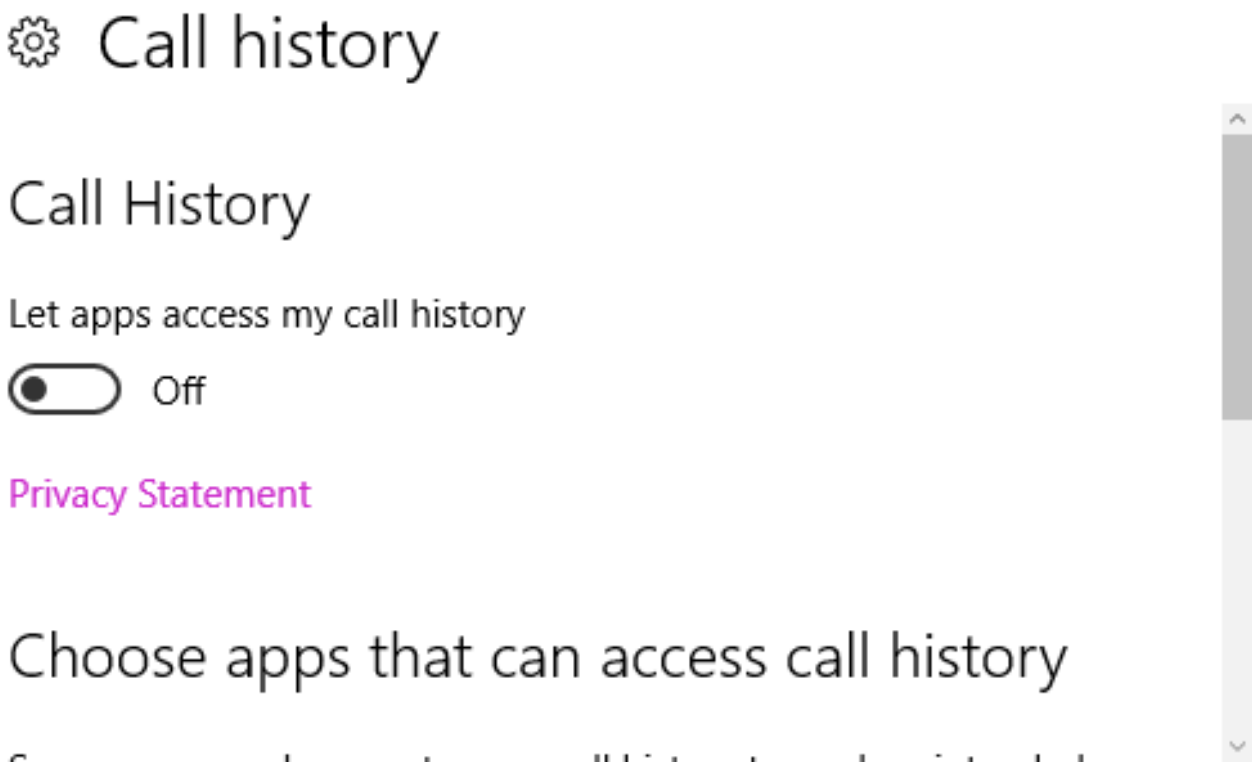
This page contains your calendar privacy settings.



As with your contacts, calendar information can be **shared between a number of apps, including Cortana**. You can specify access to your calendar information on an app-by-app basis.

Call History

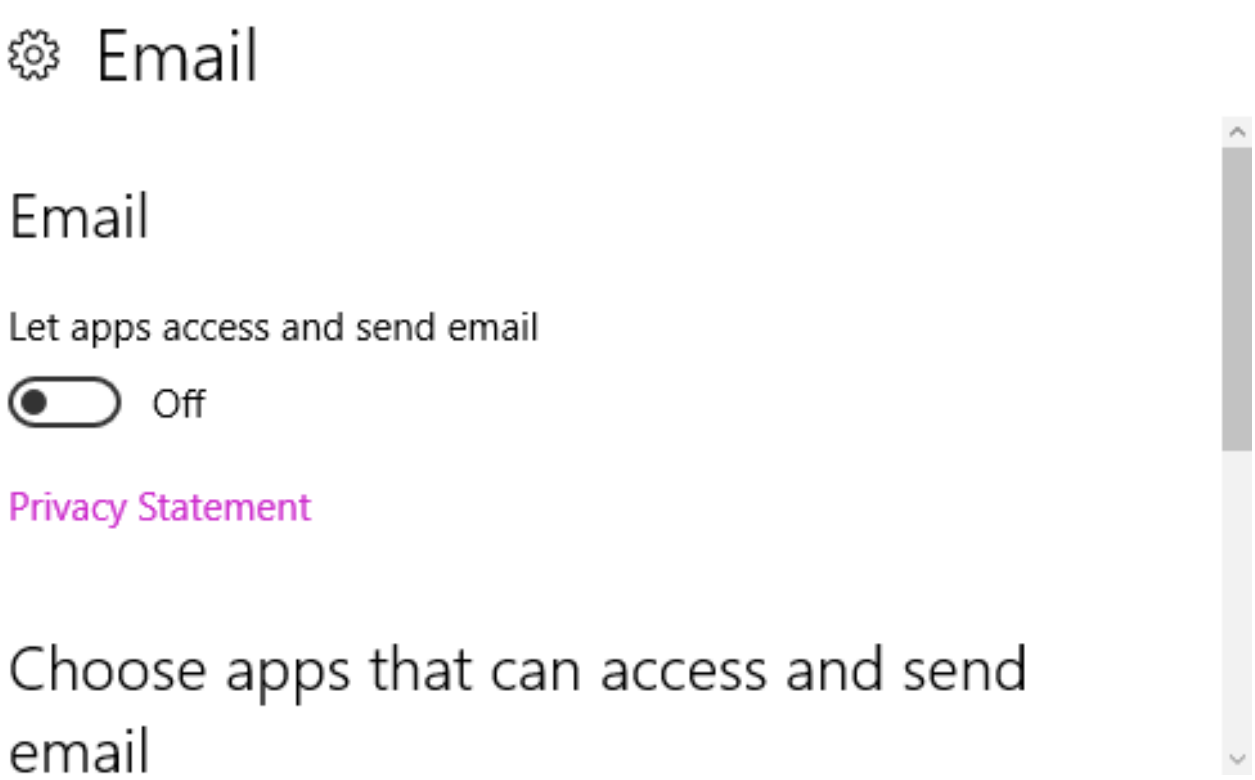
This page contains privacy settings for your Call History.



This relates directly to the Windows 10 Mobile operating system found across a number of smartphones, but can also affect those users making or receiving calls through a SIM-enabled tablet.

Unfortunately, I don't have experience with the Windows 10 Mobile operating system, or how this privacy setting affects other apps installed on the device. I have this turned off on my laptop and desktop, for obvious reasons. If you believe it is sharing unnecessary information across your device, turn it off, and gauge if any apps are directly affected by this.

Email



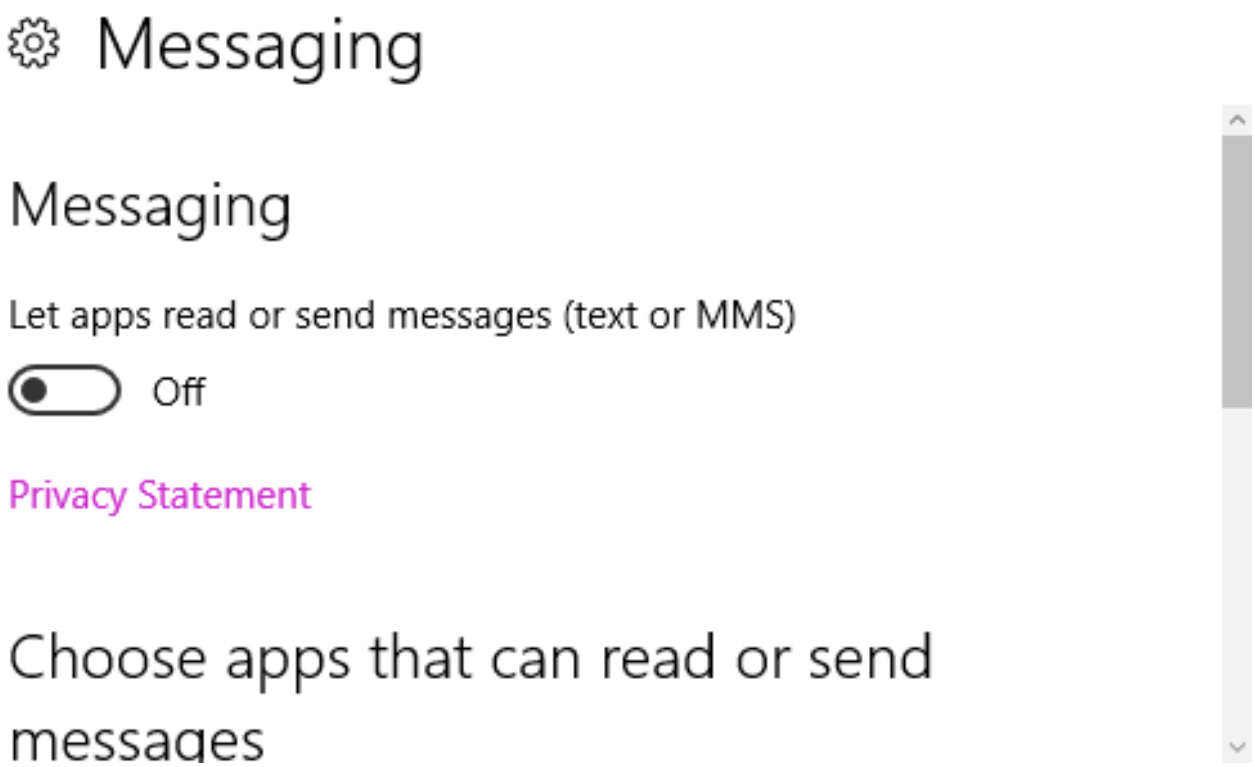
This setting defines which apps will be able to sign-in and send emails on your behalf.

You can specific permissions on an app-by-app basis, but you should note that “Classic Windows applications” will not show up on this list. This means Outlook and other email apps installed outside of the Windows Store will act according to their individual settings. In this case, please see your email client for further notification and privacy settings.

As with Call History, making alterations to this setting could cause some of your installed apps to behave differently.

Messaging

This page contains privacy settings for you Messaging services.

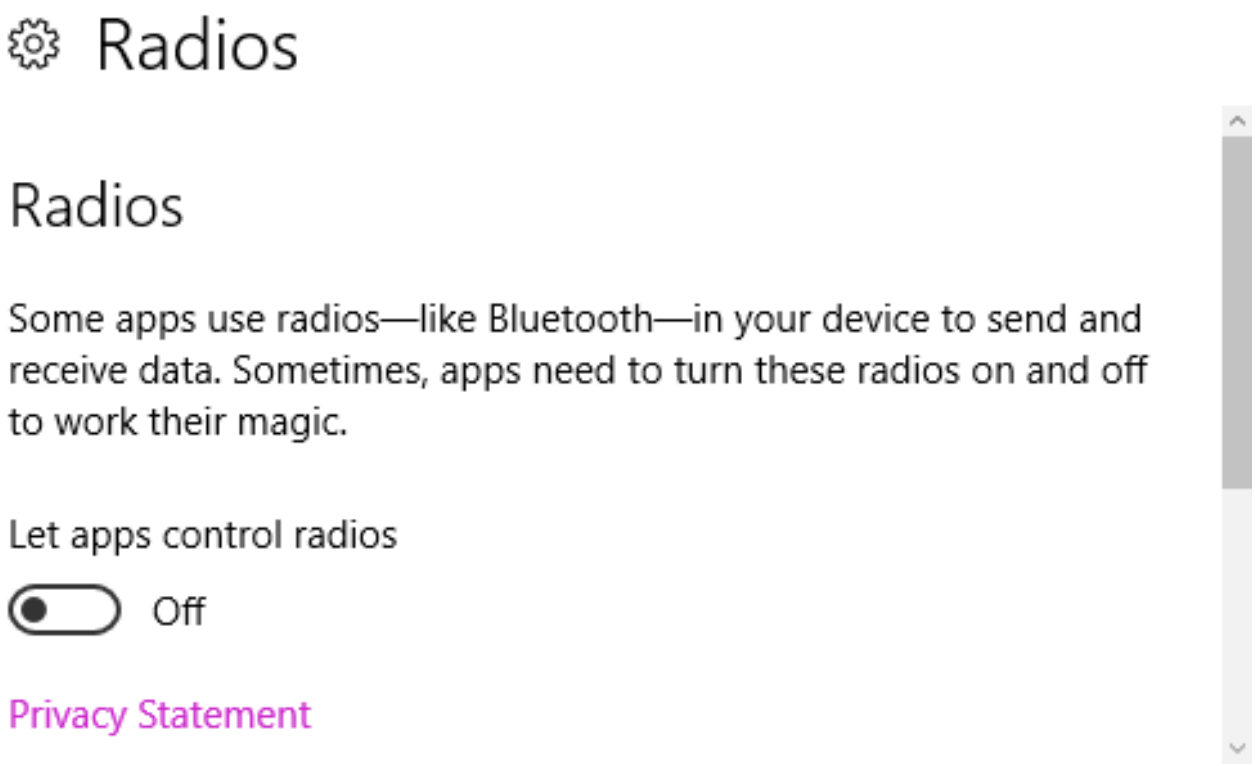


Some apps will require the ability to post as you, or post on your behalf. If you feel uncomfortable with this, by all means turn the feature off. However, as with the settings for Call History and Email, turning this off could cause some of your installed apps to behave differently, especially on Windows 10 Mobile devices.

I would advise turning off individual apps one by one, and checking what is affected by the change.

Radios

Windows 10 Radio privacy settings concern apps which turn the radio in your device on to communicate with other devices as requested.

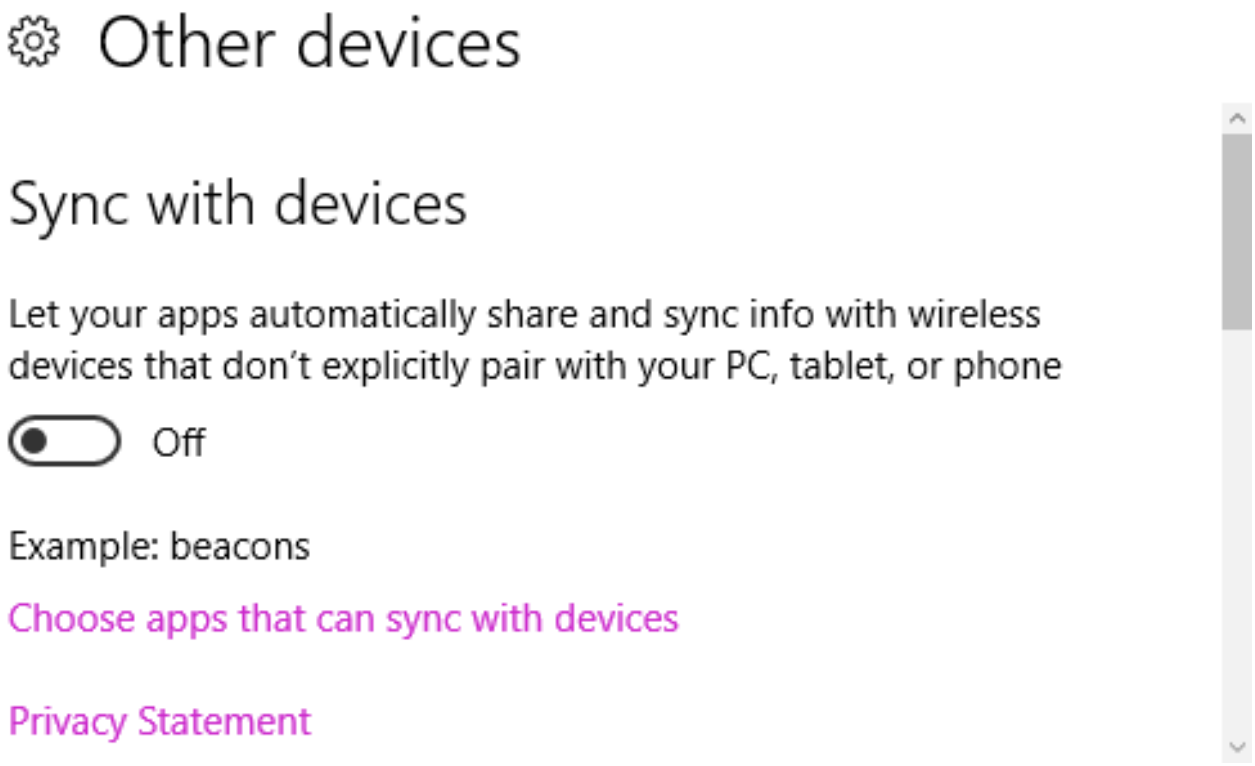


This could range from an app requiring specific access to your Bluetooth to allow direct communications — think smart watches and their companion apps — to turning on Wi-Fi adapters to create a network connection.

I would advise handling this on an app-by-app basis, with special consideration going to those Windows 10 Mobile users. You may find disabling the entire setting causes some apps to simply stop working as they do not have the access require to work.

Other Devices

This page contains privacy settings concerning how your device relates with others around it.



Sync With Devices

Your device will communicate with other devices around it. This setting allows apps installed on your device to "automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet, or phone".

This is a big "no" for me. The settings page references "beacons," which references the use of tracking and advertising beacons in heavily populated areas. For instance, you enter a busy shopping mall containing beacons, and your phone syncs up. The beacons can then track you around the building, using the stores you visit to build an advertising profile. Urm, no thank you.

Microsoft also uses "web beacons" to "help deliver cookies and gather usage and performance data. Our websites may include web beacons and cookies from third-party service providers."

Use Trusted Devices

Windows 10 can sync with other trusted devices, using your local network. This can be pretty handy, for example if you use some of Microsoft's cross-platform features, such as streaming your Xbox One to your Windows 10 PC.

Manage your trusted devices one-by-one, and you should be fine. If you have concerns about how much information is being transmitted between trusted devices and apps, Microsoft advise visiting "the apps' sites and explore the settings for your individual apps and devices". This isn't entirely helpful, so be wary of allowing any old device onto your trusted list.

Feedback & Diagnostics

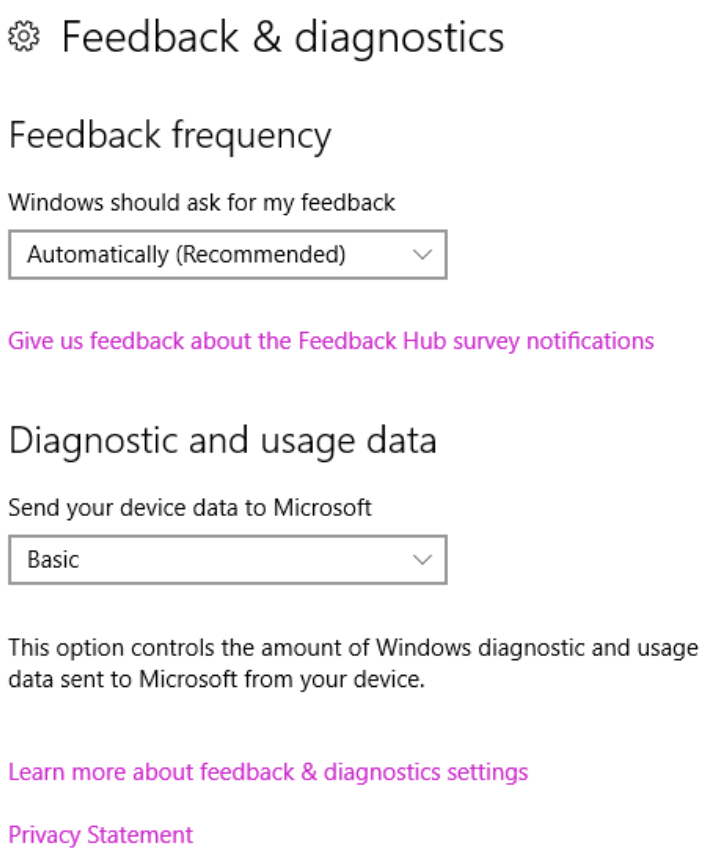
This page contains privacy settings for the feedback and diagnostic features of Windows 10. At the time of Windows 10 release in July 2015, Microsoft received some extremely negative feedback relating to these two features. Some of that negative sentiment continues to the current day. A core of Windows 10 users believe Microsoft consistently oversteps the boundaries of reasonable data collection. A major concern is what and how the company sets about collecting **that data**.

> *Together, feedback and diagnostics are how you and your Windows 10 device tell Microsoft what's really going on.*

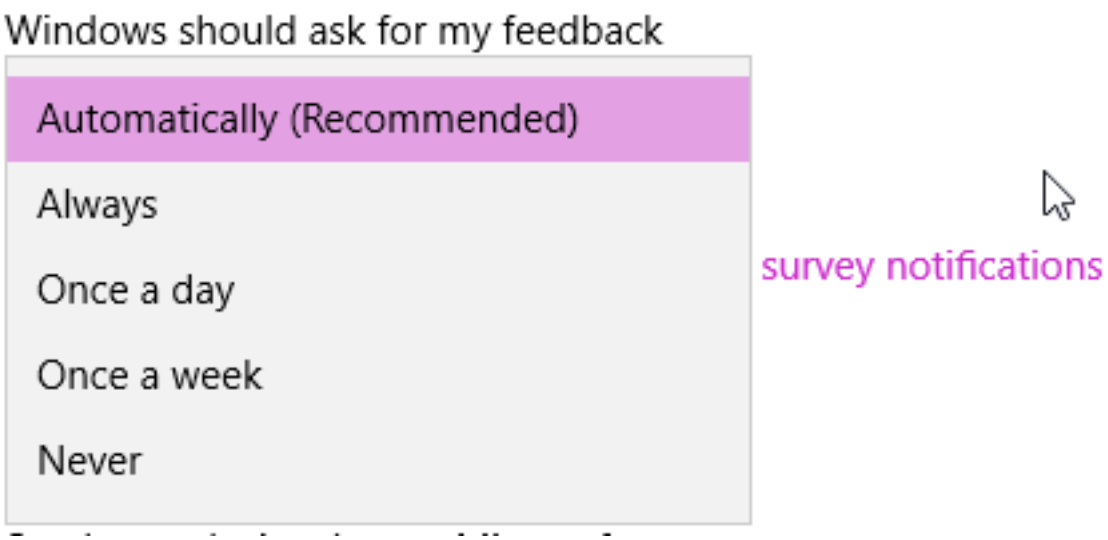
I'll expand on this toward the end of this article.

Feedback Frequency

The first option defines how often Microsoft should ask for feedback relating to Windows 10 features. Having signed up to the Insider Preview many moons ago, being asked for feedback doesn't irk me. However, some Windows 10 users do not want to be asked about their experiences with the operating system. If that is you, switch this option to **Never**. Otherwise, choose a level you're comfortable with.



The information you provide is used to streamline and improve Windows 10 services and features. This is how you're contributing to the development of the operating system for everyone.



Diagnostic and Usage Data

Perhaps the most controversial setting in all of Windows 10 (a fierce competition between this and forced Windows Updates!): "This option controls the amount of Windows diagnostic and usage data sent to Microsoft from your device." Microsoft provides three options to help you decide just how much data you'd like to share. The following information is taken directly from the Microsoft.com Feedback, diagnostics, and privacy in Windows 10 document, which can be found here.

- **Basic** sends data that is vital to the operation of Windows. It helps keep Windows and apps secure, up to date, and running properly by letting Microsoft know the capabilities of your device, what is installed, and whether Windows is operating correctly. Basic includes basic error reporting back to Microsoft. Basic data consists of:
    - Configuration data, including the manufacturer of your device, model, number of processors, display size and resolution, date, region and language settings, and other data about the capabilities of the device.
    - The software (including drivers and firmware supplied by device manufacturers), installed on the device.
    - Performance and reliability data, such as which programs are launched on a device, how long they run, how quickly they respond to input, how many problems are experienced with an app or device, and how quickly information is sent or received over a network connection.
    - Network and connection data, such as the device's IP address, number of network connections in use, and data about the networks you connect to, such as mobile networks, Bluetooth, and identifiers (BSSID and SSID), connection requirements and speed of Wi-Fi networks you connect to.
    - Other hardware devices connected to the device.
- **Enhanced** includes everything in Basic, plus data about how you use Windows, including Microsoft and third party software (apps, drivers, etc.) that run on Windows. This data includes which apps you use most often, how long you use certain features or apps, how

often you use Windows Help and Support, and which services you use to sign in to apps. Enhanced lets us collect diagnostic data related to system or app crashes. If you select this option, we'll also be able to provide you with an enhanced and more personalized Windows experience.

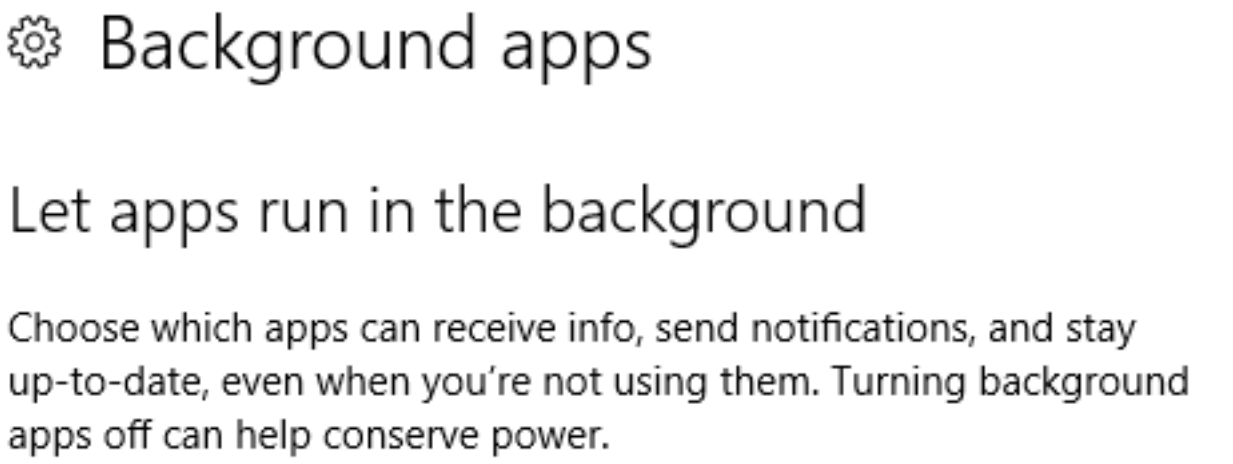
- **Full** includes everything in Basic and Enhanced levels, plus additional diagnostic data including the memory state of your device when a system or app crash occurs (which may unintentionally include parts of a document you were using when a problem occurred). It also turns on advanced diagnostic features that can collect additional data from your device, which helps us further troubleshoot and fix problems. When we learn that devices are experiencing problems that we have trouble diagnosing or replicating internally, we will randomly select a small number of devices from those at the Full level that are experiencing those problems from which to gather the data needed to diagnose and fix the problem (including user content that may have triggered the issue). If an error report contains personal data, we won't use that information to identify, contact, or target advertising to you. **Full is the recommended option for the best Windows experience and the most effective troubleshooting.**

Have you got all that?

I keep my telemetry level at **Basic**.

Background Apps

This privacy setting lets you decide which apps can receive and send information, even while you're not using them. The Windows 10 settings page confirms "turning background apps off may conserve power," but it can also save these apps unnecessarily communicating.



Head through the list and turn the apps off, one by one. If something stops working, you should consider turning it back on, or use an internet search to find a solution.

Is Windows 10 Still a Privacy Nightmare?

I think the answer to that question very much depends on who you ask. **This writer expressed some serious concerns** when Windows 10 was released. The language surrounding some of the seemingly invasive settings felt purposefully vague; Microsoft did little to allay the fears expressed by concerned users. Even with detailed (but not technical) explanations into the telemetry system, some Windows 10 users are understandably unhappy with their data being used to better services for their fellow users.

The unhappiness and mistrust comes from a poorly handled launch. Are the vast majority of people completely happy to share their information so freely with Microsoft, or are they just completely unaware it is taking place? Microsoft has done itself no favors, either. While increasing the control over other privacy areas, as we have covered in this article, in others, it is constantly stripped back. For instance, Cortana: **you accept everything, or you have nothing.**

Pro-Microsoft users point to the fact that no personal data has been liberated from Redmond since the release of Windows 10 (or even before that, with the release of the Insider Preview scheme). This, through multiple builds, bugs, and vulnerabilities, is excellent news. And it is true, **Windows 10 is a very secure operating system**.

But by **gathering information on users by default**, by logging keystrokes, by building profiles, by assuming we'd like to be part of a peer-to-peer system, and simply by removing direct user control from some operating system elements, Microsoft has regressed toward accommodating uniformed consumers while eroding customer trust.

In the age of data gathering and intelligence, Microsoft made a clear choice: **act first, never ask for forgiveness**.

Does the extensive list of privacy options let you control Windows 10, or is it just a smoke and mirrors act delivered by Microsoft? What else are you doing to protect your privacy in Windows 10?