



THE COMPLETE GUIDE TO

WINDOWS 10

PRIVACY SETTINGS

by Gavin Phillips

The Complete Guide to Windows 10 Privacy Settings

Written by Gavin Philips

Published June 2018.

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

This ebook is the intellectual property of MakeUseOf. It must only be published in its original form. Using parts or republishing altered parts of this ebook is prohibited without permission from **MakeUseOf.com**.

Table of contents

Overview of Windows 10 Privacy Issues	5
Windows 10 Update and Privacy Settings	5
6 Quick and Easy Fixes to Windows 10 Privacy	6
1. Change Windows 10 Privacy Settings	6
2. Opt Out During Windows 10 Installation	6
3. Turn Off Delivery Optimization	6
4. Completely Disable Cortana	7
5. Consider Using a Local Account	7
6. Check Your Microsoft Privacy Dashboard	7
3 Useful Tools for Managing Windows 10 Privacy	8
1. W10Privacy	8
2. O&O ShutUp10	9
3. AntiSpy for Windows 10	9
Windows 10 Privacy Settings: General	10
Advertising ID	10
Access My Language	10
Track App Launches	10
Suggest Settings Content	11
Windows 10 Privacy Settings: Speech, Inking & Typing	11
Windows 10 Privacy Settings: Diagnostics & Feedback	12
Diagnostic Data	12
Improve Inking & Typing Recognition	14
Tailored Experiences	14
Diagnostic Data Viewer	14
Delete Diagnostic Data	15
Feedback Frequency	15
Windows 10 1803 Feedback Frequency Setting Bug	15
Windows 10 Privacy Settings: Activity History	16
Windows 10 Privacy Settings: Location	16
Location	17
Default Location	17
Location History	17
Geofencing	17
Location Privacy Options Roundup	17
Windows 10 Privacy Settings: Camera	18
Windows 10 Privacy Settings: Microphone	18

Windows 10 Privacy Settings: Notifications	19
Windows 10 Privacy Settings: Account Info	20
Windows 10 Privacy Settings: Contacts	21
Windows 10 Privacy Settings: Calendar	22
Windows 10 Privacy Settings: Call History	23
Windows 10 Privacy Settings: Email	24
Windows 10 Privacy Settings: Tasks	24
Windows 10 Privacy Settings: Messaging	25
Windows 10 Privacy Settings: Radios	26
Windows 10 Privacy Settings: Other Devices	26
Communicate With Unpaired Devices	27
Windows 10 Privacy Settings: Background Apps	27
Windows 10 Privacy Settings: App Diagnostics	28
Windows 10 Privacy Settings: Automatic File Downloads	29
Windows 10 Privacy Settings: Documents, Pictures, Videos	30
Windows 10 Privacy Settings: File System	30
Is Windows 10 Still a Privacy Nightmare?	31



The Windows 10 April 2018 update brought forth a new smattering of privacy settings. The update landed in the final week of April 2018. Its worldwide roll-out is expected to complete during the coming months, so now is a good time to explore any changes to Windows 10 privacy settings and how they affect you.

What follows is a page-by-page guide to Windows 10 April 2018 update privacy settings, so you know exactly which security settings to configure, 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**.

You will note that Microsoft has split the privacy menu into two sections: **Windows Permissions** and **App Permissions**. The former deals with how Microsoft collects and uses your data to streamline your Windows 10 experience. The latter deals with how individual Windows 10 apps use identification, data collection, and other privacy-related app permissions.

Overview of Windows 10 Privacy Issues

Windows 10 has long come under attack for its approach to user privacy. When Windows 10 hit the shelves back in 2015, numerous features came under immediate attack from privacy advocates and Microsoft critics alike. However, Microsoft stuck to its guns in regard to alleged privacy infringements, adding greater control over individual elements but not completely removing any of the perceived privacy infringing features.

The major issue leveled at Windows 10 concerns data collection. Is Microsoft overstepping the boundaries of operating system data collection? Misleading stories regarding integrated keyloggers and spyware certainly do not help. However, nor does Microsoft's addition of advertising within File Explorer (this is easily turned off) and **vaguely worded EULAs that worry users** about constant system scanning (the EULA in question is not permitting this behavior).

It boils down to one question: does Microsoft violate your privacy by default? Unfortunately, there is no clear answer as your relationship with Windows 10 privacy varies from your neighbors, friends, family, and so on. The Electronic Frontier Foundation strongly asserts that Windows 10 violates your privacy. The French government agrees, too, as does the European Union's data protection watchdog and the Netherlands' Data Protection Authority.

But data gathering within your Windows operating system isn't a startling new revelation. Microsoft has been **gathering information in Windows since at least 2009**, and maybe even before that.

Windows 10 Update and Privacy Settings

'Each major Windows 10 update resets your privacy settings to default.'

If Windows 10 privacy settings do concern you, you're in for a long battle. **Microsoft is more open with its data collection** and privacy settings. Users now have more direct control over how apps and other services interact. You can spend time turning every privacy off or restricting access to your data. But in a serious slight against all users, each major Windows 10 update resets your privacy settings to default. At this point, it isn't just privacy advocates suffering; all Windows 10 users must sift through their privacy settings because Microsoft yearns for data.

6 Quick and Easy Fixes to Windows 10 Privacy

Luckily, all is not lost. You can take some direct action against Microsoft and Windows 10 to restrict how much data you hand over.

1. Change Windows 10 Privacy Settings

This guide details the range of privacy settings available in Windows 10. But one of the most basic things to do is switch everything off. As you have just read, a major Windows 10 update will reset your efforts, but it only takes a couple of minutes to toggle everything to “off” again.

2. Opt Out During Windows 10 Installation

During the Windows 10 installation, you have the option to turn off several privacy settings. If you are new to Windows 10 or completing a fresh installation, use that opportunity **to turn off any privacy settings**.

3. Turn Off Delivery Optimization

Windows 10 Delivery Optimization makes use of peer-to-peer technology to share updates with other computers. Now, if you want to share updates with other computers within your known network, that's fine. You can opt-in and alter settings accordingly. But the default setting is to share updates—using your bandwidth—without letting you know.

Delivery Optimisation

Windows Update Delivery Optimisation provides you with Windows and Store app updates and other Microsoft products quickly and reliably.

Allow downloads from other PCs

If you have an unreliable Internet connection or are updating multiple devices, allowing downloads from other PCs can help to speed up the process.

If you turn this on, your PC may send parts of previously downloaded Windows updates and apps to PCs on your local network or on the Internet. Your PC won't upload content to other PCs on the Internet when you're on a metered network.

[Learn more](#)

Allow downloads from other PCs

☐ Off



Head to **Settings > Update & Security > Windows Update > Advanced Options > Delivery Optimization**. In addition, you can control the amount of bandwidth you share using the Delivery Optimization Advanced Options. The Advanced Options menu also features sliders that control how much bandwidth Windows 10 uses to download updates.

4. Completely Disable Cortana

Disabling Cortana doesn't break Windows 10 search. So, if you would **rather do without the Windows 10 assistant altogether**, you can **safely disable it without worrying**. However, the **process differs between Windows 10 versions**.

5. Consider Using a Local Account

Okay, so this isn't entirely necessary, but a local account has numerous benefits over an always-connected Microsoft account. **Security and privacy are just two of the reasons**. Check out this short guide **if you want to switch to a local account**.

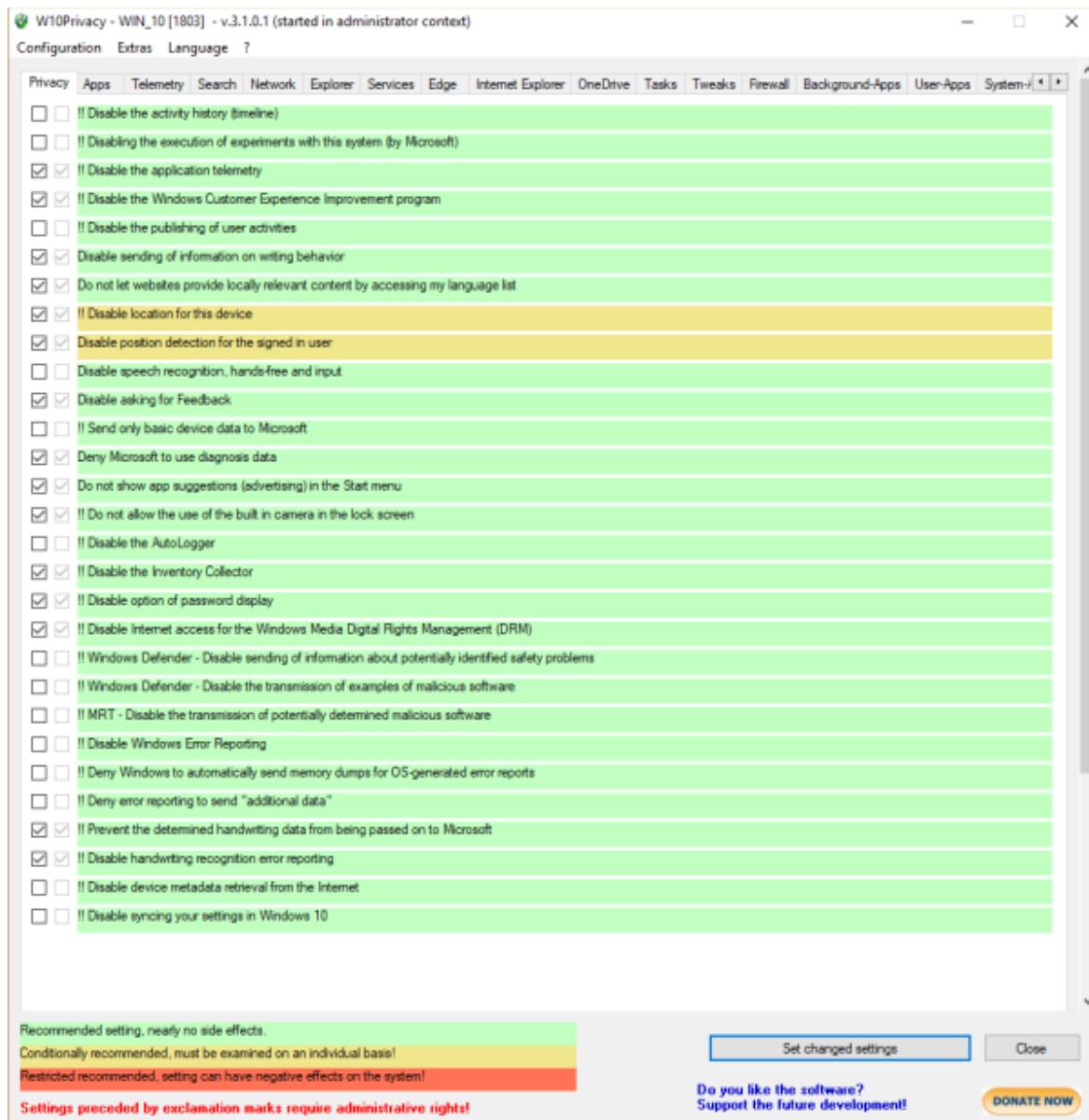
6. Check Your Microsoft Privacy Dashboard

The Microsoft privacy dashboard gives you a chance to see what information Microsoft is storing. The information you see "represents the most relevant personal data" saved to personalize your experience. You can download or delete your data at any time.

3 Useful Tools for Managing Windows 10 Privacy

Along with the quick fixes listed above, there are **several extremely useful Windows 10 privacy tools** you can use to make changes rapidly. Here are three of the best.

1. W10Privacy



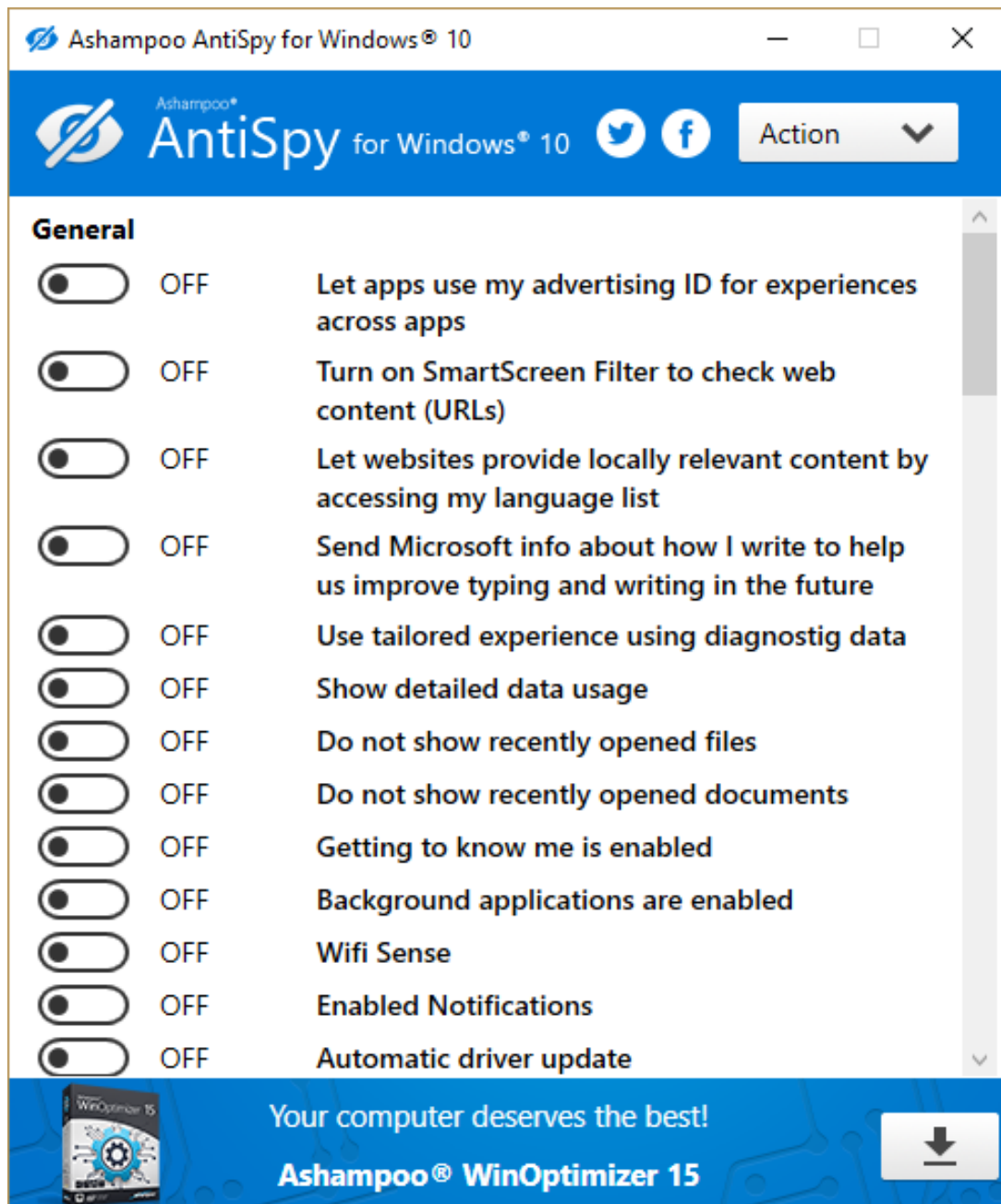
W10Privacy is one of the first ports of call for many Windows 10 privacy buffs. Simply put, it offers a vast range of privacy settings that you can use to claw-back some privacy from Microsoft. The app features 14 tabs relating to a different aspect of Windows 10 privacy.

All W10Privacy options are color-coded, too. Green indicates a recommended tweak, yellow indicates a case-by-case privacy setting, while red means you only proceed if you're confident in your selection.

2. **O&O ShutUp10**

O&O ShutUp10 is another well-respected third-party privacy tool for Windows 10. Like W10Privacy, you toggle privacy settings on or off depending on your requirements. You can scroll over each privacy setting for an outline of what it does, while the app offers a recommended setup for privacy seekers.

3. **AntiSpy for Windows 10**



Your final Windows 10 privacy tool to check out is AntiSpy for Windows 10. AntiSpy for Windows 10 features a comprehensive list of privacy settings you can easily toggle on and off. AntiSpy comes with a default setting that eliminates most privacy settings. You can still head through and turn any other settings off.

Windows 10 Privacy Settings: General

General

Change privacy options

Allow apps to use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)



Allow websites to provide locally relevant content by accessing my language list



Allow Windows to track app launches to improve Start and search results



Show me suggested content in the Settings app



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 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.**

Access My Language

Microsoft and Windows can use your language settings to ensure locally served content matches up. If you're English, this 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.

Track App Launches

Windows 10 can track the apps you launch to arrange your Start menu and search results better. Turning this feature on will streamline Start menu results and tile suggestions with your most frequent choices, with similar results for the Start menu search bar.

Suggest Settings Content

Microsoft can suggest new settings and other content that you might find interesting. The new and interesting settings, content, and app suggestions can manifest in several ways. If you're an infrequent or new user, this isn't an entirely terrible way to learn about new features you might otherwise miss out on. However, if you are in any way familiar with Windows 10 and other Windows operating systems, you can toggle this off.

Windows 10 Privacy Settings: Speech, Inking & Typing

Speech, inking & typing

Getting to know you

Use your voice to do things like talk to Cortana or Store applications, and use your typing history and handwriting patterns to create a local user dictionary that makes better suggestions for you. Microsoft will use your voice input to make cloud-based speech services work even better.

When this is switched off, you can't speak to Cortana, and your typing and inking user dictionary will be cleared. Speech services that don't rely on the cloud, like Windows Speech Recognition, will still work. Typing suggestion and handwriting recognition using the system dictionary will also continue to work.

Turn on speech services and typing suggestions

[View user dictionary](#)

Speech, Inking & Typing maintains a database of your Cortana inputs to streamline how yours and other users' speech services work. When this option is turned on, Windows records your typing history (in the Cortana search box) and voice search requests. That data is then aggregated with other user data "to help improve our ability to recognize all users' speech correctly."

The Speech, Inking & Typing option has several knock-on privacy matters. For instance, because Cortana is turned on, Microsoft also collects information about your Calendar and People (your contacts) to further "personalize the speech experience." The setting also creates a user dictionary of frequent and unique terms to streamline the service further.

Unfortunately, Cortana will not work without turning this option on. However, you can turn off some Cortana features to limit the amount of data collection.

Windows 10 Privacy Settings: Diagnostics & Feedback

Diagnostics & feedback

Diagnostic data

Choose how much data you send to Microsoft. Select [Learn more](#) for information about this setting, how Windows Defender SmartScreen works and the related data transfers and uses.

- ☒ **Basic:** Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.
- ☐ **Full:** Send all Basic diagnostic data, along with info about the websites you browse and how you use apps and features, plus additional info about device health, device usage and enhanced error reporting. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.

The Diagnostics & Feedback section contains privacy settings for the wide range of feedback and diagnostic features of Windows 10. While the fierce criticism of Windows 10 data collection practices has somewhat ceased, there are still concerns about how far-reaching some practices are.

Diagnostics and feedback are how you and your Windows 10 device tell Microsoft what's really going on.

You can check out the **full range of diagnostic data collection categories right here**.

Diagnostic Data

In a previous update, Microsoft reduced the number of diagnostic data options to two, leaving just the Basic or Full options (Enhanced no longer exists). The two settings controls exactly how much data you send to Microsoft. The following information is taken directly from the Microsoft "Diagnostics, feedback, and privacy in Windows 10" document that **you can find here**.

Basic: Sends only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems and make product improvements. Basic sends:

- Device, connectivity, and configuration data:



- Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, and firmware and memory attributes.
- Network capabilities and connection data such as the device's IP address, mobile network (including IMEI and mobile operator), and whether the device is connected to a free or paid network.
- Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics level, and whether the device is part of the Windows Insider program.
- Data about connected peripherals such as model, manufacturer, driver, and compatibility information.
- Data about the applications installed on the device such as application name, version, and publisher.
- Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space, or connectivity through a paid network.
- Whether updates complete successfully or fail.
- Data about the reliability of the diagnostics collection system itself.
- Basic error reporting, which is health data about the operating system and applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

Full: Sends all Basic diagnostic data, along with info about the website you browse and how you use apps and features, plus additional info about device health, device usage, and enhanced error reporting. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems and make product improvements. In addition to Basic, Full sends:

- Additional data about the device, connectivity, and configuration beyond that collected at Basic.
- Status and logging information about the health of operating system and other system components (in addition to data about the update and diagnostics systems collected at Basic).
- App usage, such as which programs are launched on a device, how long they run, and how quickly they respond to input.
- Browser usage, also known as browsing history.
- Small samples of inking and typing input, which is processed to remove identifiers, sequencing information, and other data (such as names, email addresses, and numeric values) which could be used to reconstruct the original content or associate the input to the user. This data is never used for Tailored experiences as described below.
- Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

There isn't really a way of completely escaping Microsoft diagnostic data if you use Windows 10. Opt for the Basic setting if this is a concern.

Improve Inking & Typing Recognition

In relation to the previous section, this option further streamlines and improves inking and typing services for you and other users.

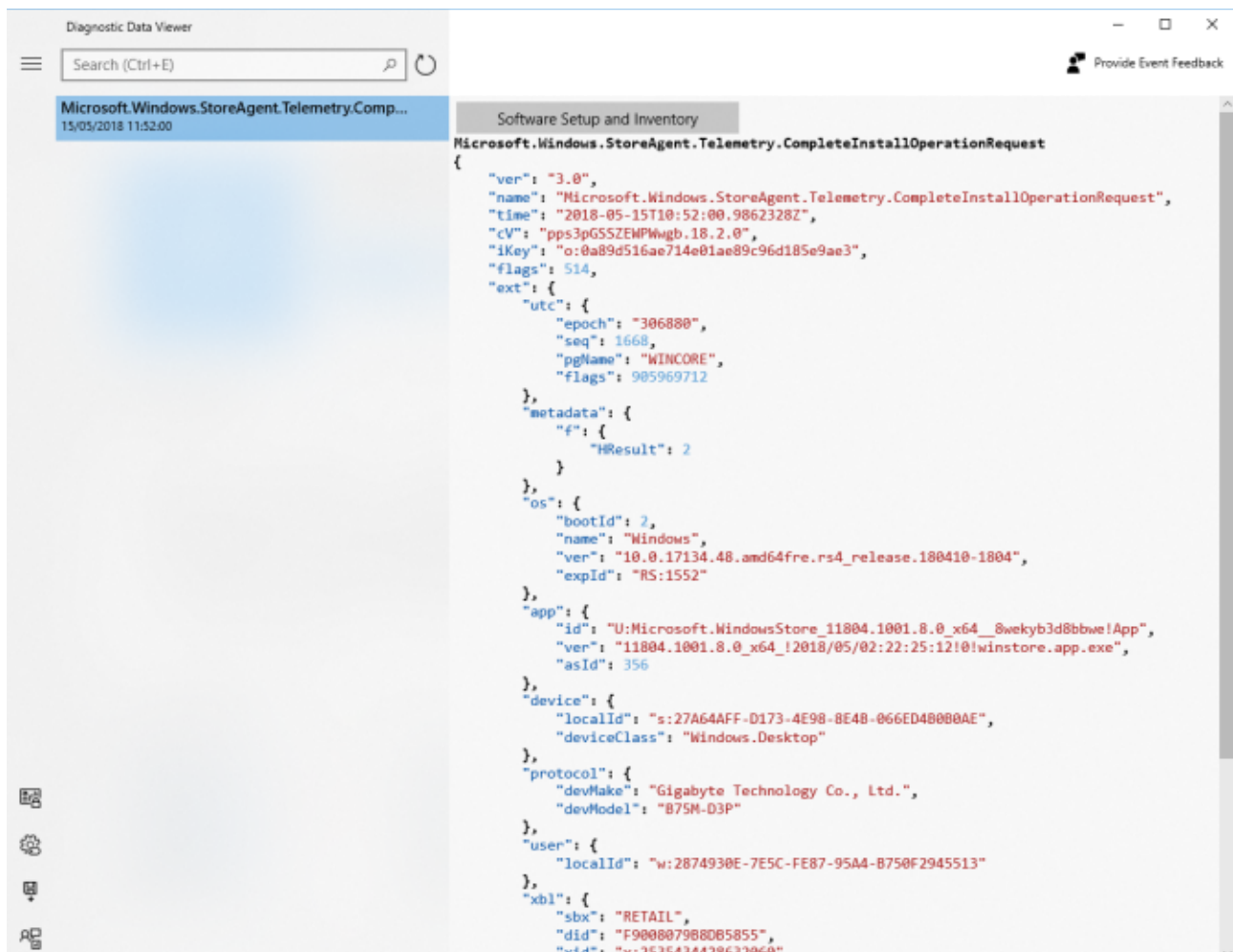
Tailored Experiences

Microsoft's Tailored Experiences uses the diagnostic data level you choose to provide a range of personalized tips, app suggestions, and more. These also feed into product suggestions and other similar services.

The tailored experiences extend to suggesting a different app to use for video streaming, or for a different way to view images within Windows 10. However, it also makes suggestions to purchase additional OneDrive storage if your hard drive is filling up, advertising Windows products. Again, this option ties into Windows attempting to streamline and curate your user experience.

Turn this option off to stop these suggestions.

Diagnostic Data Viewer



The screenshot shows the Diagnostic Data Viewer application. On the left, there is a search bar with the text "Search (Ctrl+E)" and a refresh button. Below the search bar, a list of events is displayed, with the first event selected: "Microsoft.Windows.StoreAgent.Telemetry.Comp..." with a timestamp of "15/05/2018 11:52:00".

The main pane on the right displays the details of the selected event, titled "Software Setup and Inventory". The event name is "Microsoft.Windows.StoreAgent.Telemetry.CompleteInstallOperationRequest". The event data is shown in a JSON format:

```
{
  "ver": "3.0",
  "name": "Microsoft.Windows.StoreAgent.Telemetry.CompleteInstallOperationRequest",
  "time": "2018-05-15T10:52:00.9862328Z",
  "cV": "pps3pG5S5ZEMFWgb.18.2.0",
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "flags": 514,
  "ext": {
    "utc": {
      "epoch": "306880",
      "seq": 1668,
      "pgName": "WINCORE",
      "flags": 905969712
    },
    "metadata": {
      "f": {
        "HResult": 2
      }
    },
    "os": {
      "bootId": 2,
      "name": "Windows",
      "ver": "10.0.17134.48.amd64fre.rs4_release.180410-1804",
      "expId": "RS:1552"
    },
    "app": {
      "id": "U:Microsoft.WindowsStore_11804.1001.8.0_x64_8wekyb3d8bbwe!App",
      "ver": "11804.1001.8.0_x64_12018/05/02:22:25:12!0!winstore.app.exe",
      "asId": 356
    },
    "device": {
      "localId": "s:27A64AFF-D173-4E98-8E4B-066ED48080AE",
      "deviceClass": "Windows.Desktop"
    },
    "protocol": {
      "devMake": "Gigabyte Technology Co., Ltd.",
      "devModel": "B75M-D3P"
    },
    "user": {
      "localId": "w:2874930E-7E5C-FE87-95A4-B750F2945513"
    },
    "xbl": {
      "sbx": "RETAIL",
      "did": "F900807988085855",
      "xid": "x:2535434428632060"
    }
  }
}
```


The Diagnostic Data Viewer option gives you a chance to view the data Microsoft is collecting on your system. The Data Viewer itself is a **Microsoft Store download**. Once installed, you can browse diagnostic data as it enters the viewer.

Honestly, for most people (including myself), most of the data is raw, meaning it simply won't make much sense. You can, however, decrypt any encrypted data sent to Microsoft's servers, making it at least slightly more accessible for those who can analyze the information.

Delete Diagnostic Data

You can, however, delete your diagnostic data using this option. Hitting the **Delete** button erases any diagnostic data. It doesn't stop the future collection of diagnostic data. The delete button simply resets the counter, if you will.

Feedback Frequency

Your feedback frequency affects how often Windows 10 will ask for your opinion on changes to the operating system. If you are part of the Windows Insider Program, this option is set to Automatically (Recommended). If you are not, you can change this option to one of the alternatives.

Feedback frequency

Windows Insider Programme manages this option

Windows should ask for my feedback

Automatically (Recommended) 

Windows 10 1803 Feedback Frequency Setting Bug

There are numerous reports that the Feedback Frequency option has a bug locking it to automatic feedback, accompanied by the message "Windows Insider Program manages this option." Fortunately, fixing this bug doesn't take long:

1. Download this cumulative update from Microsoft.
2. Type cmd in the Start menu search bar, then right-click and select **Run as administrator**.
3. Now, type the following command:

```
dism /online /add-package /packagepath:[path to downloaded file]  
\\Windows10.0-KB4135051-  
x64_22fd6a942c7b686a5434bcc8dfc87f3379c99437.cab
```

4. Hit Enter, wait for the command to process, then restart your system.

Windows 10 Privacy Settings: Activity History

Activity history

Jump back into what you were doing with apps, docs or other activities, either on your PC or your phone.

☐ Let Windows collect my activities from this PC

☐ Let Windows synchronise my activities from this PC to the cloud

Review the [Learn more](#) and [Privacy statement](#) for info about activity history, what happens when you send your activity history to Microsoft and how we respect your privacy.

Your Activity History details the things you do on your PC. The activity history keeps track of the files you open, services you use, websites you browse, and more. Activity history stores the information locally, but if you are signed in to your Microsoft account and have given permission, that information is shared across Microsoft's services.

Your activity history can allow you to pick up work from another computer. For instance, if you were working on a Microsoft Word document on another PC, but had to leave the computer, the activity would appear in your history for a few days afterward. If the activity appears on the list, you can select and continue it.

The activity history feed is aggregated with data from other users and is used to improve Microsoft products and services.

Windows 10 Privacy Settings: Location

This page contains your location-based privacy settings.

Location

If location is on, each person using this device can choose their own location settings.

Location for this device is off

[Change](#)

If the location service is on, Windows, apps and services can use your location, but you can still turn off location for specific apps.

Location service

☐ Off

If an app is using your location, you'll see this icon: 

Default location

Windows, apps and services can use this when we can't detect a more exact location on this PC.

[Set default](#)

Location history

If location is on, your location history is stored for a limited time on the device, and can be used by apps that use your location.

Clear history on this device

[Clear](#)

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, the 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 countless other apps and websites are doing this otherwise, so it is up to you.

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 the broadcast of only one set of data.

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 labeled **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 Privacy Options Roundup

Microsoft has sneakily hidden another important location-related privacy menu: Cortana location services. Microsoft has streamlined Cortana settings into its own settings menu, but this is separate from the privacy options listed here.

Cortana “works best when she has access to your device location and location history,” although you can now safely turn those location settings off and the Windows 10 assistant remains functional. However, you won’t receive location-based contextual information.

To manage Cortana, head to Settings > Cortana > Permissions & History, then select Manage the information Cortana can access from this device.

Windows 10 Privacy Settings: Camera

Camera

Allow access to the camera on this device

If you allow access, people using this device will be able to choose if their apps have camera access by using the settings on this page. Denying access blocks Windows and apps from accessing the camera.

Camera access for this device is on

Change

Allow apps to access your camera

If you allow access, you can choose which apps can access your camera by using the settings on this page. Denying access only blocks apps from accessing your camera. It does not block Windows.

☐ Off

This page contains privacy settings for your camera.

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

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.

Windows 10 Privacy Settings: Microphone

Microphone

Allow access to the microphone on this device

If you allow access, people using this device will be able to choose if their apps have microphone access by using the settings on this page. Denying access blocks apps from accessing the microphone.

Microphone access for this device is on

Change

Allow apps to access your microphone

If you allow access, you can choose which apps can access your microphone by using the settings on this page. Denying access only blocks apps from accessing your microphone. It does not block Windows.

☒ On

This page contains privacy settings for your microphone. You will note the similarity between the camera and microphone options, along with other privacy settings to come.

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, users have raised concerns that Windows 10 will record their speech 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.

Windows 10 Privacy Settings: Notifications

Notifications

Let apps access my notifications



Choose apps that can access your notifications

Some apps need access to your notifications to work as intended. Turning off an app here might limit what it can do.

Apps that need your permission to access your notifications will appear here. Go to the Store to get apps.

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 wary of Windows Lock Screen notifications. These may display unwanted information in a public place without you realizing. However, you will find lock screen notifications (and quick actions) in **Settings > System > Notifications & Actions**, rather than the Notifications privacy settings page.

Windows 10 Privacy Settings: Account Info

Account info

Allow access to account info on this device

If you allow access, people using this device will be able to choose if their apps can access their account info by using the settings on this page. Denying access blocks apps from accessing anyone's account info.

Account info access for this device is off

Change

Allow apps to access your account info

If you allow access, you can choose which apps can access your name, picture and other account info by using the settings on this page. Denying access blocks apps from accessing your account info.

☐ Off

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

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

Windows 10 Privacy Settings: Contacts

Contacts

Allow access to contacts on this device

If you allow access, people using this device will be able to choose if their apps have access to their contacts by using the settings on this page. Denying access blocks apps from accessing any person contacts.

Contacts access for this device is off

Change

Allow apps to access your contacts

If you allow access, you can choose which apps can access your contacts by using the settings on this page. Denying access blocks apps from accessing your contacts.

☐ Off

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.

Windows 10 Privacy Settings: Calendar

Calendar

Allow access to calendars on this device

If you allow access, people using this device will be able to choose if their apps have access to their calendar by using the settings on this page. Denying access blocks apps from accessing any person calendar.

Calendar access for this device is off

Change

Allow apps to access your calendar

If you allow access, you can choose which apps can access your calendar by using the settings on this page. Denying access blocks apps from accessing your calendar.

☐ Off

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.

Windows 10 Privacy Settings: Call History

Call history

Allow access to call history on this device

If you allow access, people using this device will be able to choose if their apps have access to their call history by using the settings on this page. Denying access blocks apps from accessing any person call history.

Call history access for this device is off

Change

Allow apps to access your call history

If you allow access, you can choose which apps can access your call history by using the settings on this page. Denying access blocks apps from accessing your call history.

☐ Off

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 and tablet, 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.

Windows 10 Privacy Settings: Email

Email

Allow access to email on this device

If you allow access, people using this device will be able to choose if their apps have access to their email by using the settings on this page. Denying access blocks apps from accessing any person's email.

Email access for this device is off

Change

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

You can specify permissions on an app-by-app basis, but you should note that “Classic Windows applications” will not show up on this list. This means **Microsoft Outlook and other email apps** installed outside of the Windows Store will act according to their 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.

Windows 10 Privacy Settings: Tasks

Tasks

Allow access to tasks on this device

If you allow access, people using this device will be able to choose if their apps have access to their tasks by using the settings on this page. Denying access blocks apps from accessing any person tasks.

Tasks access for this device is off

Change

Allow apps to access your tasks

If you allow access, you can choose which apps can access your tasks by using the settings on this page. Denying access blocks apps from accessing your tasks.

☐ Off

This page defines which applications can access your tasks.

Turn this setting off if you do not want apps to access tasks set in other programs or anywhere else on your system.

Windows 10 Privacy Settings: Messaging

Messaging

Allow access to messaging on this device

If you allow access, people using this device will be able to choose if their apps have access to read or send messages via text or MMS by using the settings on this page. Denying access blocks apps from reading or sending messages (text or MMS).

Messaging access for this device is off

Change

Allow apps to read or send messages

If you allow access, you can choose which apps can read or send messages via text or MMS by using the settings on this page. Denying access blocks apps from reading or sending messages via text or MMS.

☐ Off

This page contains privacy settings for your SMS or MMS Messaging services (not to be confused with online messaging services, like Slack, and so on).

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.

Try turning off individual apps one by one and checking what is affected by the change.

Windows 10 Privacy Settings: Radios

Radios

Some apps use radios—such as Bluetooth—in your device to send and receive data. Sometimes, apps need to turn these radios on and off to work their magic.

Let apps control 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 smartwatches 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 Windows 10 Mobile users. You may find disabling the entire setting causes some apps to simply stop working as they do not have the correct permissions to work.

Windows 10 Privacy Settings: Other Devices

Other devices

Communicate with unpaired devices

Let your apps automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet or phone



Example: beacons

Choose apps that can communicate with devices

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

Communicate With Unpaired 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.”

Communicating with unpaired devices 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. Err, 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.”

Windows 10 Privacy Settings: Background Apps

Background apps

Background Apps

Let apps run in the background



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.

Windows 10 Privacy Settings: App Diagnostics

App diagnostics

Let apps access diagnostic information



Choose apps that can access diagnostic information about other apps

Some apps use diagnostic information from other apps on your device to run as intended. Diagnostic information may include the names of running apps, the user account name that launched an app, app memory, CPU, disk and network usage. Preventing access to diagnostic information may limit what an app that uses that information can do.

Apps that need your permission to access diagnostic information from other apps are listed here. Go to the Store to get apps.

This page concerns Windows 10 app diagnostics and privacy settings.

‘Apps in Windows 10 are carefully isolated so that they don’t interfere with each other. However, there are scenarios where it’s useful for one app to see certain types of information about other running apps (for example, it’s useful for diagnostic tools to be able to get a list of running apps).’

Though the range of information that apps access is limited, some users have concerns that apps will overstep their boundaries. The information available is:

- The name of each running app.
- The package name of each running app.
- The username under whose account the app is running.
- Memory usage of the app, and other process-level information typically used during development.

You can choose which apps communicate individually, turning them off one-by-one.

Windows 10 Privacy Settings: Automatic File Downloads

Automatic file downloads

Windows can automatically download online-only files from your online storage provider (such as OneDrive) for apps that request them.

If you block any of those apps from requesting automatic file downloads, you can unblock them here.

Allow

This section concerns how Windows 10 handles automatic file downloads from online storage providers.

For instance, if you **use online-only files stored in your OneDrive account**, Windows 10 and some Windows apps might automatically download those files, so they are ready for use. You can block individual apps from downloading files or turn the entire feature off.

Windows 10 Privacy Settings: Documents, Pictures, Videos

Documents

Allow access to document libraries on this device

If you allow access, people using this device will be able to choose if their apps have access to their documents library by using the settings on this page. If you deny access, all apps that are available in the Microsoft Store on Windows 10 will be blocked from accessing any person's documents library.

Documents library access for this device is off

Change

Pictures

Allow access to picture libraries on this device

If you allow access, people using this device will be able to choose if their apps have access to their pictures library by using the settings on this page. If you deny access, all apps that are available in the Microsoft Store on Windows 10 will be blocked from accessing anyone's pictures library.

Pictures library access for this device is off

Change

Videos

Allow access to video libraries on this device

If you allow access, people using this device will be able to choose if their apps have access to their videos library by using the settings on this page. If you deny access, all apps that are available in the Microsoft Store on Windows 10 will be blocked from accessing any person's videos library.

Videos library access for this device is off

Change

These sections concern how apps access documents, pictures, and videos. They're combined into a single article header because, well, they're essentially the same setting under a different name.

When these settings are turned on, apps can access your document library or the pictures and videos on your device. When turned off, they cannot.

Windows 10 Privacy Settings: File System

File system

Allow access to the file system on this device

If you allow access, people using this device will be able to choose if their apps have access to all of their files – including their documents, pictures, videos and local OneDrive files – by using the setting on this page. Denying access blocks apps from accessing anyone's files.

File system access for this device is off

Change

This page concerns file system access for apps on your system.

Installed apps can access files on your system if given permission. This includes documents, photos, videos, audio files, local OneDrive files, and more. Some apps require access to these files as part of their core functionality. In this, double-check the installed apps list before turning file system access off.

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 about **Windows 10 security issues** when the latest version 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.

Microsoft did listen to the users—to an extent, at least. Adding additional control while simultaneously streamlining the number of privacy settings has helped users better understand Windows 10. And providing an overview of exactly what information Windows 10 is collecting, where it is going, and the data decryption tool further empowers users.

But by **gathering information on users by default**, 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 the broad spectrum of Windows 10 users while eroding customer trust.

However, will all that said, Windows 10 is still a very secure operating system, and that is what most users need; privacy demands of the individual fall by the wayside to protect the security of the many. It seems that in the age of data gathering and intelligence, Microsoft makes clear choices: **act first and never ask for forgiveness**.

Read more stories like this at

