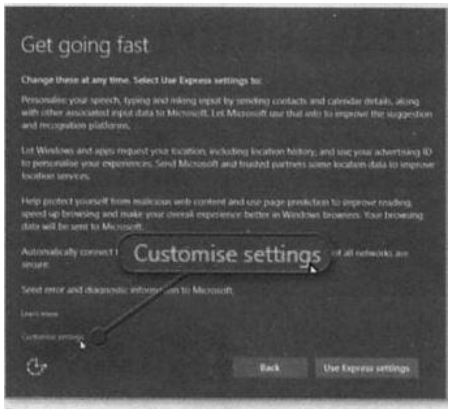
Stop Microsoft spying on you
Copied from Computer Active magazine

PROTECT YOUR PRIVACY IN WINDOWS 10

Here's how to disable all of the snooping features Microsoft has built into its latest 0perating system.

1. Don’t use Express settings
Urgency level: Very high

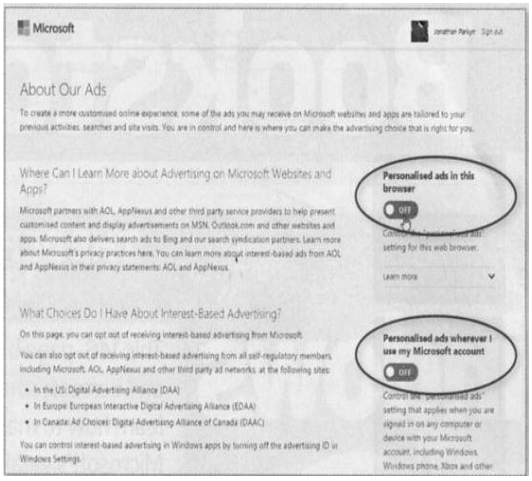


Protect your privacy by clicking the tiny ‘Customise settings’ link when upgrading to Windows 10

During the Windows 10 upgrade Microsoft sneakily glosses over a very important part in the procedure. It uses misleading wording to trick you into agreeing to a load of default settings many of which potentially compromise your privacy. By choosing this 'Use Express setup' option when prompted you'll shave a few minutes off your setup time. But you'll also be allowing Microsoft to collect personal data from your contacts and calendar.
If already upgraded to Windows 10, it's too late to change this. Instead you'll need to switch off each tracking individually - follow our tips below.
But if you've not upgraded, when do so just click the tiny ‘Customise settings’ link on the ‘Get going fast' screen to disable most of Windows 10's snooping features (see screenshot).

2 Disable targeted advertising
Urgency level: High

You can't turn off advertising completely, but can stop advertisers from using information about you to target you with personalised ads. To do so, click Settings, then Privacy. Click General on the left, then switch off "Let apps use my advertising ID for experiences across apps'. While you’re there, also switch off ‘Let websites provide locally relevant content by accessing my language list’



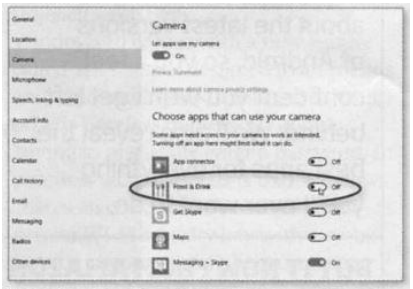
You'll need to change settings elsewhere too. Click ‘Manage my Microsoft advertising and other personalisation info' to be taken to Microsoft's About Our Ads web page (www.snipca.com/19455). Sign in with your Microsoft account. then switch both 'Personalised ads in this browser' and ‘Personalised ads whenever I use my Microsoft account' Off - (see screenshot).
To block Start menu adverts, click Start, Settings, Personalisation, then Start and switch off 'Occasionally show suggestions in Start. Finally, open the Windows Store app, click on your account and choose Settings. Here, switch off ‘Show products on tile' if you'd rather not see adverts in the Stores Start menu Live tile.

3 Block location tracking
Urgency level: Medium

If you don't like the idea of people knowing where you are and where you've been, click Start, Settings, Privacy, then Location. The settings you need to change here depend on what type of device you're using and the services you want to use. If you're using a standard desktop PC, for instance, there’s no real benefit to

having location switched on at all, as the PC is fixed in one place. To plan journeys in the Maps app. you can always just use your postcode instead.
To disable Location altogether for anyone who uses the PC, click Change, then turn it off. To turn it off for individual user accounts click the switch under Location to Off. To erase location data, click Clear under ‘Clear history on this device’.
If you're using a laptop - or a Windows phone or tablet - location can be pretty useful for navigating, so you may wish to leave it on. But if you do, scroll down on the Location settings page and disable any apps you don't want tracking you under ‘Choose apps that can use your location'. Almost all can be safely switched o ff.

4 Stop apps watching and listening
Urgency level: High



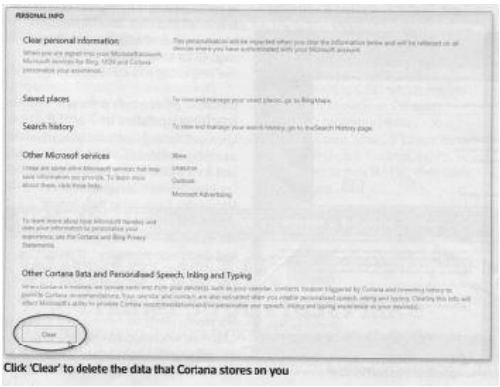
Why does the ‘Food & Drink’ app need access to your camera? Simply turn it off

Giving apps permission to use your device's camera or microphone means that they could spy on you. They could even record your voice and take video footage of you. By default, Windows 10 lets apps use your camera and microphone, so to change this, click Start, Settings, Privacy, then either Camera or Microphone. The setting at the top of both pages turns off the camera and microphone for all apps. but you may not wish to do this – Skype, for example, won't work if it can't access the microphone or camera. Instead, turn off individual apps listed under Choose apps that can use your camera/microphone'.

5. Disable Windows 10 keylogger
Urgency level: Very high

We've been warning readers about the dangers of keyloggers - tools that record what you type on your keyboard - for years. So it's astonishing that Windows 10 should come with one built-in. Microsoft claims it’s there to help improve services and provide with a more personalised experience, but we think it's just plain creepy. First, click Start, Settings, Privacy. General, then switch Off 'Send Microsoft info about how I write to help us improve typing and writing in the future'.
Once you've done that, click ‘Speech, inking and typing' on the left, then click 'Stop getting to know me' on the right. This will Stop Windows (and Cortana) collecting data from spoken commands and handwriting (on devices that support this), as well as from what you type. It'll also disable Cortana, and Stop the voice – dictation tool from working.
Click ‘Turn off’ in the warning message if you’re happy with this.

6 Stop Cortana storing your data online
Urgency level: High



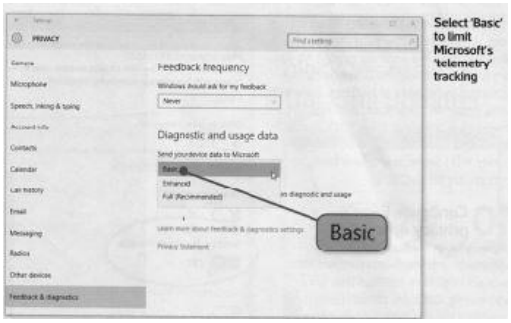
Click 'Clear' to delete the data that Cortana stores on you

For all of Microsoft's fanfare about Cortana, it's hard to ignore the fact that Windows 10's digital assistant is a privacy nightmare. Even if you disable it using the previous tip, Cortana will continue to store detailed personal information about you on Microsoft's servers unless you opt to delete it. To do so, click Start, Privacy, then click 'Speech, inking and typing'. Under 'Manage cloud info', click ‘Go to Bing and manage personal info for all your devices'. This will open a web page - sign in with your Microsoft account, then scroll down to Other Cortana Data and Personalised Speech, Inking and Typing' and click Clear (see screenshot).

7 Block apps from accessing your private info

Urgency level: Medium
Windows 10 allows apps to a wide variety of different personal data - from your calendar and contacts to emails and text messages. To stop this. click Start, Settings, Privacy, then click ‘Account info' , Contacts. Calendar, Call history’, Email and Messaging in turn. In each case (apart from Contacts) you'll see a main switch at the top of the page allowing you to turn off access completely.
However, as with Camera and Microphone, you may find that doing this prevents certain apps and tools from working properly. The Mail app, for example, needs to have access to your calendar, contacts and, of course, email. So, instead of disabling app access altogether, it's better to leave the top switch on in each case, then choose which apps to allow or disable from those listed below.

8 Limit Microsoft's telemetry tracking
Urgency level: Med



It's not possible to turn off all of Microsoft telemetry tracking in Windows 10, But you can customise it to limit the amount of data you share, and to Stop Windows nagging you for feedback. Click Start, Settings, Privacy, then click 'Feedback & diagnostics' on the left (you may need to scroll down if you can't see it). On the right, select Never from the 'Windows should ask for my feedback' dropdown menu, then select Basic from the dropdown menu under 'Send your device data to Microsoft' (see screenshot).

9 Stop Windows 10 sharing your Wi-Fi password
Urgency level: High

Windows 10 comes with a new feature called WiFi Sense, designed to let friends and colleagues quickly connect to each other's wireless networks without having to physically enter a password. In practice, what happens is that Windows shares an encrypted version of your private Wi-Fi security key with anyone in your contacts list. Others can't see your key, but the system does mean that contacts you don't really know or trust could end up with the ability to access your Wi-Fi when they're in the vicinity. Not only that, but your encrypted Wi-Fi key is stored on Microsoft's servers, leaving it vulnerable to hackers. To switch WiFi Sense off, click Start, Settings, 'Network & internet', then WiFi. Scroll down and click 'Manage WiFi settings'. Under WiFi Sense, make sure both options are set to Off.

10 Configure Edge's privacy options
Urgency Medium

Enable 'Send Do Not Track requests' to limit how much information Edge sends to Microsoft

Microsoft's new web browser has its own set of privacy settings that need addressing. Click the menu (three dots) button in the top right and choose Settings, then 'View advanced settings. Scroll to 'Privacy and services'. Leave 'Offer to save passwords' and 'Save form entries' enabled only if you are comfortable with the browser storing this information. We recommend enabling 'Send Do Not Track requests' to limit the amount your online activity is tracked (see screenshot) and disabling 'Get Cortana to assist me in Microsoft Edge' (though this may already be disabled if you've Cortana off). It’s convenient to leave enabled ‘Show search and site suggestions as I type’ and ‘ Use page prediction to speed up browsing’. But it will mean data about your searches and browsing being sent to Microsoft. Under the Cookies section, we’d suggest selecting ‘Block only third party cookies’, but bear in mind this will stop some sites working properly. *(Note – I would suggest that Password saving is switched off and a Password manager such as Lastpass is used instead.)*