Windows 10 Privacy Concerns

Windows 10 has come under suspicion of covert privacy invasions since shortly before it was released in late July 2015. Most of that is overblown hype, so Microsoft is making an effort to clarify the muddy privacy waters. Here's what you need to know.

Microsoft has made two simple statements about Windows 10 privacy principles:

1. Windows 10 collects device information so the product will work better for you.
2. You are in control with the ability to determine what personal information is collected.

All information collected is encrypted before and during transmission to Microsoft, and is stored in encrypted secure servers. Microsoft stores three types of data collection and how they are handled.

Safety and Reliability Data, aka Device ID

“Safety and reliability data” is all about system or app crashes. This is nothing new; whenever any version of Windows has crashed, users have been asked if they want to send an “error report” to Microsoft. Internet Explorer and many other apps, including non-Microsoft apps, do the same.

What is new is that users no longer have any choice; Windows 10 will always send crash reports.

Each crash report is scrubbed of data such as names, user account IDs, IP addresses, email addresses, and other things that might personally identify a user. Crash reports also filter out filenames and file contents, delivering to Microsoft or app developers only data that will be useful in debugging what went wrong with Windows 10 or an app.

A crash report must include not only the “what” of an incident but also the “where.” Microsoft and app developers need to know whether 100 crash reports came from one hundred devices or one device. So Windows 10 generates a “device ID” unique to each device on which it is installed. But it bears no relationship to who owns or uses the device.

Advertising ID

The “Advertising ID” generated by Windows 10 is completely different from the device ID. It identifies a specific user account created on a Windows 10 device. A database of Advertising IDs is kept by Microsoft and shared with app developers. Developers may use your Advertising ID to customize the ads that their apps display to you on any device.

You can turn off the Advertising ID by clicking the Start button, then "Settings" and then "Privacy." On the "General" tab, the first item says "Let apps use my advertising ID for experiences across apps." Use the slider underneath to toggle it to the Off position if desired.

Personalization Data

“Personalization data” is collected so that the user’s experience on Windows 10 or an app can be customized to **“deliver a … personalized Windows experience.”** Such data may include the fact that you’re a fan of a particular sports team, or follow certain stocks, or use certain apps, or tend to frequently use certain words. Allowing collection of such personalization data can make your Windows experience more pleasant and productive (according to Microsoft).

But you can turn off collection of personalization data. Click Windows + I, then Privacy, then Account Info.

When you use Cortana, Microsoft collects and uses information including your device location information and location history, contacts (People), voice input, searching history, calendar details, content and communication history from messages and apps, and other information on your device. In Microsoft Edge, Cortana collects and uses your browsing history.

To turn Cortana off, go to **Cortana > Notebook > Settings**, and then turn the **Cortana** setting off. When you turn Cortana off on a device, she won’t give you suggestions, reminders, alerts, or ideas when you’re using that device.

Turning off Cortana clears the interests and information on your device, but won’t clear the information that’s saved on the Notebook or in the Bing.com dashboard.