Windows 10: An operating system that gathers data on everything you do

Mark Blackwood
10 August 2015

Microsoft launched the latest version of its Windows operating system (OS) on July 29, promoting the event as the largest software update ever. Unlike previous releases, the new version has been offered by Microsoft to all domestic users as a free upgrade. Over 14 million users are reported to have downloaded and installed it within the first 24 hours of its release.

One question that remains unanswered, however, is: out of the 14 million who upgraded in the first 24 hours, how many had the time to read and study the 45 page privacy policy and service agreement in the End User License Agreement (EULA) prior to installation?

Following the customary corporate fanfare that generally accompanies a Windows OS release, reports rapidly emerged about marked changes to the company's privacy policy and service agreement. The new agreement, by default, effectively gives permission for Microsoft to monitor users' activities via the use of keylogger type spyware.

Spyware is software that enables the information about a computer and the activities that take place on it to be transmitted covertly from their hard drive to another computer. A keylogger is a type of spyware or surveillance software created to log every keystroke made on the infected machine.

A keylogger like the one in Windows 10 can record instant messages, emails, search requests, credit card details, the contents of documents and spreadsheets, or anything else that is typed on a keyboard. The log file created by the keylogger can then be sent to the designated receiver, in this case Microsoft.

According to the *Guardian*, the default settings of Windows 10 also permit Microsoft to control a user's bandwidth in order to "upload data to other computers running the operating system, share Wi-Fi passwords with online friends and remove the ability to opt out of security updates."

The main reason Microsoft wants to monitor its users en masse is to monetize information about them and their habits. With 90 percent of the world's laptops and PCs running a Windows operating system, the company's monopoly position gives it a huge potential for harvesting data on its customers and emulate the likes of Google and Apple.

According to Heini Järvinen, Community and Communications Manager at European Digital Rights, "Microsoft basically grants itself very broad rights to collect everything you do, say and write with and on your devices in order to sell more targeted advertising or to sell your data to third parties. The company appears to be granting itself the right to share your data either with your consent 'or as necessary'."

Many users, when installing Windows 10, will not know how to configure it to prevent the automatic installation of the new default software. Moreover, the vast majority of PC and laptop users download and install software without fully reading the EULA.

Web developer Jonathan Porta described the tactics used by Microsoft during the installation process of its OS, "Everything about this screen is urging me to just accept the default configuration and get on with life. … With all of these settings on these two screens enabled I might as well relocate my computer to Microsoft headquarters and have the entire company look over my shoulder."

What makes Microsoft's new operating system all the more concerning is the corporation's close relationship with the National Security Agency (NSA) and FBI, which have been engaged in the systematic and illegal violation of the democratic rights of computer users for years.

In 2014, NSA whistle blower Edward Snowden

described the aim of his employer as wanting to "collect it all"—in other words, capture the entire content of the world's Internet activity in order to analyze and profile all potential opponents of the American government, above all, political opposition from the working class.

Snowden revealed the depth of collaboration between the NSA and Microsoft (and other IT corporations) as they sought to monitor and collect data on users of Microsoft products. Documents sent via Outlook.com, Skype and SkyDrive were monitored. Microsoft even worked with the NSA to create a backdoor to its own encryption software to ensure the agency's fullest possible access to user data.

Rather than be greeted with excitement for being a free operating system upgrade, the question that should be asked by everyone is why is a corporation like Microsoft, with such history, is so willing to give out this operating system for free.