Is Windows 10 Spying on You?

by Sharon D. Nelson, Esq. and John W. Simek

It's hard to find statistics identifying how many people are currently running Windows 10. One thing we do know is that there were 14 million downloads within 24 hours of the release. Some estimates put the installed base at over 75 million devices. No matter what the right number is, it appears that Microsoft has added another hit operating system to its list. But is everything about Windows 10 a good thing? Not so fast. When Microsoft released Windows 10, it also updated its privacy policy. Should attorneys be concerned? The answer attorneys love to hate is…it depends. Perhaps if more people read the terms of service for software and services that they use, they would be a lot more informed as to the data vendors are collecting.

Microsoft is no exception. Suffice it to say, Windows 10 collects a lot of data and you agreed to it when you installed the operating system. According to the privacy policy, Microsoft collects information about your use of the software and services as well as about the devices and networks on which they operate. Some examples of the type of collected information include your name, e-mail address, preferences and interests; location, browsing, search and file history; phone call and SMS data; device configuration and sensor data; voice, text and writing input; and application usage. Many experts say that the data is anonymously sent to Microsoft and is primarily composed of telemetry data.

The one section of the privacy statement that attorneys should be aware of states:

"We may also access, disclose and preserve information about you when we have a good faith belief that doing so is necessary to:

1. comply with applicable law or respond to valid legal process from competent authorities, including from law enforcement or other government agencies;
2. protect our customers, for example to prevent spam or attempts to defraud Microsoft's customers, or to help prevent the loss of life or serious injury of anyone;

3. operate and maintain the security of our products and services, including to prevent or stop an attack on our computer systems or networks; or
4. protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our products or services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement."

This would suggest that the data really isn't anonymous and could be turned over to law enforcement or some other government entity. The good news is that you can actually opt out of all the features that might be considered invasions of privacy. Of course, most users will find that they are opted in by default.

It's a fairly simple matter to adjust the privacy settings in Windows 10. First, open **Settings** and then click on **Privacy**. From there just walk through all the options and turn off anything that you are not comfortable having Microsoft collect. We would certainly also suggest that users dump Cortana, Siri, Alexa and any other voice assisted service. After all, you really don't know what the vendor is doing with the data or how long they retain it.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com