Software Updates May Be Compromising Your IG

John Phillips, CRM, CDIA, FAI

Information governance (IG) cannot be thoroughly implemented in an organization that is operating uncontrolled technology systems and data repositories. Even when employees, contractors, and business partners work diligently toward consistent IG practices, external forces – namely, updates to cloud-based or resident software on laptops, cellphones, and other digital business devices – can modify internal IT operational activities in ways that violate compliance with IG expectations.

This happens, in part, because vendors encourage technology users to enable background, automated downloading of updates to software to ensure that virus protection, hardware drivers, and bug patches are implemented. Unfortunately, because software updates are so frequent and often seem minor, most non-technical users just trust that Microsoft, Apple, Google, and other vendors will not release anything that will negatively affect their systems.

Another issue is that even though downloading the latest innovations in software releases and updates typically requires users to click through a software license "acceptance," they are rarely read or understood.

Organizations that allow end users to download software and software updates in this manner may face grave consequences with respect to software operations, privacy, security, and compliance with IG mandates.

Using Windows 10 as an Example

A good example of the ubiquitous nature of software updates is Microsoft's Windows 10 operating system. Users of Windows 7 and 8 have been offered an opportunity (through July 29) to upgrade their current systems to Windows 10 for free. This update, though, comes with intrusive data-gathering demands, and it should generate concerns about reliability and compatibility with a user's current software configurations.

Spontaneous Downloading

An additional concern is that the Windows 10 operating system appears to already have been *downloaded to some computers spontaneously without users initiating a request for it*! As first announced on the *INQUIRER* website in September 2015, some computer users who enabled automatic downloads of Microsoft updates may have downloaded update KB3035583, which automatically adds to the computer a hidden directory with up to 6 GB

of files comprising the components necessary for Windows 10.

Allegedly done to speed up the eventual installation process, according to media reports, the premature downloads were exposed when it caused some users to momentarily exceed their data volume allocation with their communications networks. Although there is a way to delete these files, it is not for the technologically faint of heart.

Effects Not Transparent

Of more concern, Microsoft at the time provided little information on how Windows 10 affected privacy and security, simply stating, "This update includes improvements to enhance the functionality of Windows 10." A user's only reliable way to determine the effects of the updates was to match the update numbers with information on the Microsoft Knowledge Base.

Whereas in the past it was usually possible to discern how an update would alter functionality, it is now more difficult to know what to expect. It is even more concerning that updates are cumulative; every updated feature is expected to be updated again each time an update is issued. Not installing any particular update could make a computer unstable.

Windows 7, 8 Invasion

In fact, many of the functions that are new to Windows 10 are also being applied retroactively to any Windows 7 or 8 systems, which could impact IG compliance for systems running older software as well.

For instance, Windows 7 and 8 updates KB3075249 and KB3080149 operationally deliver data to Microsoft servers without any required user interaction. The first update adds features that enable remote monitoring of operating system activities, and the second update enables older versions of operating systems to receive updates that are intended for Windows 10 systems. Thus, users running Windows 7 or 8 may find themselves subject to many of the same intrusive functions associated with Windows 10, though they would prefer to avoid these functions.

By imposing updates on users without their knowledge or consent, Microsoft is damaging the trust that may exist between the company and its customers.

… users running Windows 7 or 8 may find themselves subject to many of the same intrusive functions associated with Windows 10, though they would prefer to avoid these functions.

Troubling Service Agreement

In light of the many organizations that have been unable to protect the data they collect, customers are increasingly concerned about how Microsoft, Google, and other major software vendors will respond to government requests for private information. Such concerns are perhaps justified by statements found in the new Microsoft Services Agreement.

This agreement, which can be read in full at *https://www.microsoft.com/en-gb/servicesagreement/default.aspx*, contains these troubling statements that could impact an organization's IG policy compliance expectations:

1. "By using the Services or agreeing to these Terms, you consent to Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statements.
2. "When you share Your Content with other people, you expressly agree that anyone you've shared Your Content with may for free and worldwide, use, save, record, reproduce, transmit, display, communicate (and on HealthVault delete) Your Content.
3. "To the extent necessary to provide the Services to you and others (which may include changing the size, shape or format of Your Content to better store or display it for you), to protect you and the Services and to improve Microsoft products and services, you grant Microsoft a worldwide and royalty free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, distribute via communication tools and display Your Content on the Services."

It's important to know that the content of the services agreement may be changed without notice. In addition, few people read these agreements because they are typically long and filled with "legalese" that would require consultation with professional legal counsel. If printed, this Microsoft agreement would be more than 100 pages long. Though most people don't understand what they are signing when they accept an agreement, such "agreements" are generally supported by the courts, which does not leave an organization using a Microsoft product much leeway in configuring a software system that avoids intrusive components.

Private Data Exposed

Microsoft's perspective toward

Read More About It

Bott, Ed. "How to block Windows 10 upgrades." ZDnet, 28 April, 2016. Available at *www.zdnet.com/article/how-to-block-windows-10-upgrades-on-your-business-network-and-at-home-too/?ftag=TRE5369823.*

Meer, Alec. "Windows 10 Is Spying On You: Here's How to Stop It." Rock, Paper, Shotgun, 30 July, 2015. Available at w*ww.rockpapershotgun.com/2015/07/30/windows-10-privacy-settings.*

Merriman, Chris. "Windows 10 'updategate': Microsoft stays tightlipped as the world rages." The Inquirer, 15 September, 2015. Available at *www.theinquirer.net/inquirer/analysis/2425886/windows-10-updategate-microsoft-stays-tightlipped-as-the-world-rages.*

Microsoft End User Licensing Agreement. Available at *https://www.microsoft.com/en-gb/servicesagreement/default.aspx.*

Microsoft Privacy Policy. Available at *https://privacy.microsoft.com/en-us/privacystatement.*

Williams, Chris. "How to get a grip on your files, data that Windows 10 phones home to Microsoft." *The Register,* 24 February, 2016. Available at *www.theregister.co.uk/2016/02/24/windows_10_telemetry.*

its customers' privacy can be seen in its privacy policy at *https://privacy.microsoft.com/en-us/privacystatement*. It starts out by saying "Your privacy is important to us. This privacy statement explains what personal data we collect from you and how we use it." It then makes the following statements (see these and others at the "Learn More" link under the Microsoft privacy policy section "Personal Data We Collect"):

1. "We collect data about your interests and favorites, such as the team you follow in a sports app, the stocks you track in a finance app, or the favorite cities you add to a weather app.
2. "We collect data about your contacts and relationships if you use a Microsoft service to manage contacts, or to communicate or interact with other people or organizations.
3. "We will access, disclose and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary …."

Microsoft, like many corporations, mines user data by engaging in what some privacy experts call "spying." It does so without making it clear about what is taking place, relying heavily on abstractions like "…when we have a good faith belief that doing so is necessary." Consequently, the murky nature of concepts like data ownership and protection makes it more likely that an organization's IG policies are being compromised, especially if that mined data crosses international boundaries.

Escaping Windows 10 Surveillance

Opting out of many privacy-invading Windows 10 functions requires effort and dedication to self-protection. For example, users must slog through 13 screens to decline participation in many of Microsoft's ongoing attempts to gather data. By taking these steps, users can turn off anything that seems concerning, but they may want to be careful about accidentally turning off their access to data they access frequently, such as calendars, while doing so.

Among the other concerns is continued surveillance from the camera, microphone, speech, contacts, calendar, and messaging functions, including Cortana, Microsoft's speech-recognition function, which constantly "listens" for reasons to initiate Microsoft's Bing search engine to answer questions. Realistically, the act of opting out of any of these functions is best performed by well-trained IT staff.

Much of this intrusive data gathering is done so Microsoft can sell to advertisers the ability to use more individually targeted advertising. Some people like targeted advertising, but that does not mean the advertising a user sees is always appropriate for the moment when the ad pops up. For example, an employee might be looking at ads for vacations in Bermuda while at her desk during lunch. Later, the ads might pop up on her screen at inopportune moments, such as when her supervisor is in her office for a visit.

Reducing Impacts on IG Compliance

The fundamental problem with Windows 10 and any other commercially produced software is that users do not own the software and therefore must accept prescribed licensing agreements. To refuse the agreement could impair their business processes, as migrating data to other software environments is costly, time-consuming, and can bring other unforeseen risks. Sometimes data migration results in a loss of software support for critical business

components or an actual data loss.

The practice of slowly retiring older applications or operating systems is nearing an end. For instance, though there are still some users of the Windows XP operating system and older Office suite applications, Microsoft has ended support and maintenance for those versions. And, it may be impossible over time to continue using older systems if users are connected to the Internet and updates that interfere with the software operation are involuntarily downloaded. This means that ensuring compliance with IG guidelines is becoming even more challenging because IT staff will have to know all of the currently used technologies and how any updates will affect their operation.

Users of today's software systems can expect their communications content, travel agendas, business plans, and office location information to be increasingly subjected to data exchange during software updates in order for the vendor to ensure effective operation. For this reason, it is ideal to have IG-knowledgeable IT personnel monitor or manage all common software updates. It may be best to offer updates downloadable from a centrally coordinated IT server that monitors all devices to gauge how the updates affect the software configurations with respect to IG policy compliance.

The most globally effective IG/IT approach to new technology threats will be to enforce a policy that all software users must have permission from IT before installing any updates. To make this easier on users and to have the least impact on IT staff, organizations could post for download on an accessible website those upgrades known to pose no dangers to IG policy implementation. **END**

John T. Phillips, CRM, CDIA, FAI, can be contacted at john@infotechdecisions.com. *See his bio on page 47.*