I Know Everything About You! The Rise of the Intelligent Personal Assistant

August 12, 2015 | By Gavin Kenny

It seems to have sprung up from nowhere, but suddenly the intelligent personal assistant (IPA) is this year's must-have tool. From science fiction to today's reality, the ability to talk in natural language to a computer and have it answer questions or undertake actions at our request is commonplace.

On our mobile phones, Apple has Siri and Google runs Google Now. In our homes, Amazon has Alexa built into its Echo appliance, and now Microsoft is launching Cortana as part of Windows 10. These are all trying to help us be more productive, but can they be trusted with complete access to our data?

All these tools are designed to make our lives easier and more integrated, but in order to do so, they require access to our personal information, email, calendars, address books and more. That means IPAs need our passwords, which then opens the door to so much more. For users of cloud-based office applications such as Google Docs or Microsoft 365, those passwords provide access to not only personal messaging and diaries, but all intellectual property as well.

There is also the issue of how these systems work. The task of accurately decoding voice and understanding what is being said is 100 times more processing intensive than a simple Web search. To overcome this hurdle, IPAs send a recording of what you have said to a data center where the application actually resides. As a result, everything you ask of your intelligent personal assistant is stored and processed outside of your immediate control.

So these IPAs have complete access to your electronic life and an ability to undertake tasks autonomously, and these abilities are not within your immediate control. In fact, they could be monitored by unknown workers in data centers in countries that might have very different privacy laws from the country where you live. Should you be worried?

The crux of the matter is: In the white heat of cutting-edge research that has given birth to these amazing creations, how much time was given to security? How have these systems been built in order to keep personal information private? There are techniques that can be used to ensure that, while system administrators can look after the computer, they do not get easy, instant access to the data inside. But have these protective measures been used?

We can all make decisions as to how much we trust one company over another, especially when it comes to looking after our data and not abusing that position. If you don't trust Microsoft, for example, it is unlikely you will be a 365 customer, but even the most trusted companies could have program vulnerabilities exploited. What if an attacker could get inside the IPA and use its all-access pass into your life to siphon information?

A hypothetical scenario uses an IPA's mobile phone ability to screen your calls for you, instantly blocking callers who are deemed unknown or unimportant at the current time. They are making real-world decisions for you without your input.

Should attackers gain control of your IPA, they could use that information to gain access to your online banking system and set up direct debits or money transfers. When the bank's security system then calls your mobile to confirm the transaction, your intelligent personal assistant could silently intercept the call and confirm the transaction on your behalf.

The birth of the intelligent personal assistant will see us interacting with computer systems in a more natural manner, having them autonomously analyzing our interests and making suggestions on how to improve our lives. But we need to remember that IPAs are still only computers. We should not forget to ensure basic cybersecurity protection measures are in place and regularly checked — otherwise our electronic friend might also be the traitor in our midst.