SECURETHOUGHTS
INTERNET SECURITY FOR EVERYDAY PEOPLE

Digital Personal Assistants and The Risks of Device Eavesdropping

0

Kevin Wells • October 5, 2016 • Feature Articles

0

Digital virtual assistants certainly make searching for information easy, and they're becoming increasingly common. You can use the device or app hands-free, and it's much easier and more natural than having to click or type queries into a search engine.

Voice activated devices are fun as well as easy to use, but that leads us to wonder about the security and privacy issues involved with this form of technology.

Digital Virtual Assistants Are Growing Fast in Popularity

Digital virtual assistants come in many forms, both as software and as dedicated hardware devices. Some are apps you can install and activate on your devices. Well-known examples are Apple's Siri, Microsoft Cortana, or Google Now (used on Android devices). Another new development is the creation of standalone voice-activated assistants, such as the cylinder-shaped Amazon Echo, which is a device whose sole function is to listen for questions and respond with the requested information.

Echo can provide you with news, weather data, music and all sorts of other information. You'll also be able to use it to control and manage Internet of Things (IoT) devices in your home. All you have to do is state your question out loud and the assistant replies with the answer. What could be easier?

As Microsoft corporate vice president Derrick Connell says, "natural language is really the main UI (user interface)."

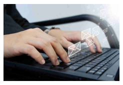
And he's right. Although we also use the written word, it's primarily through that we communicate with each other most effectively.

Latest articles

Digital Personal Assistants and The Risks of Device Eavesdropping
Feature Articles • no comments

3 Best VPN's For Apple Mac Computers
Reviews • 2 comments

Mobile Banking Malware Gets Real
Feature Articles • no comments


How To Keep Your Email Secure From Hackers
Feature Articles • no comments

Best VPNs for College
Reviews • no comments

Recommended topics

- Internet Security
- Protect Your Information
- Phone and Tablet Security
- Protecting Your Children

We just need to remember that these new intelligent apps and devices also come with a risk.

What Are the Risks with Digital Virtual Assistants?

Is your virtual assistant always standing by, ready to listen?

Last year's Samsung smart TV incident was a wake-up call about the dangers of internet-connected devices and the ease in which they can be used for eavesdropping.

Samsung were forced to admit they were logging user activity and voice commands and then sending this data to their central server for evaluation. This functionality was enabled by default in Samsung's smart TVs.

This is a common feature of voice recognition apps and devices. Simple commands are processed immediately by the device. More complex or so far unrecognized requests are sent to the provider's server for analysis, so the device can then understand and remember them for the future.

Samsung was merely engaging in what many companies do, namely using data analysis to improve the reliability of their voice recognition software.

Yet what happens to that data?

The obvious answer is that data mined from voice recognition apps and devices can be used for marketing purposes. As an example, your smart TV could suddenly start showing commercials that reflect your queries. It could even recommend programs that you might want to watch.

And what about the rights of third parties who are present in the range of the device? What about those who haven't given their consent to be listened to, recorded or have video and audio recordings of them analyzed?

I have developed mixed feelings about these new listening apps and devices.

We've become used to the idea that search engines analyze our searches. Data tracking already occurs when you work online. Search for something in Google or Amazon and chances are your browser will start displaying ads about what you were looking for.

Intelligent voice recognition takes this to a whole new level.

As a tech guy who's enthusiastic about the benefits new digital technology can bring us, I think there's great potential for new digital applications and devices to improve our lives, save us time and money, and help us more effectively access the information we need.

As a libertarian who believes in the importance of protecting our freedom, I also have doubts and concerns about the way this new technology might operate in practice.

While I'm a tech enthusiast, I don't fancy the idea of having one of these virtual assistant gadgets on my desk or in my living room. There are too many open-ended questions that need resolving before I go and buy an Amazon Echo or a Samsung Otto.

These devices also want to provide you with the information you need without too much prompting. The idea is for the device to become intelligent and actively anticipate what you want.

I'm not sure I want some smart gadget sitting on my desk or in my living room there listening. I'm happy with my devices being on tap – not on top.

There's a Trade-Off Between Convenience and Privacy

The bottom line is that there's a delicate trade-off between the convenience of intelligent devices and your digital privacy. That being said, this doesn't mean you should just accept infringements upon your privacy.

How much encroachment on your privacy are you prepared to accept in exchange for the convenience of using devices that are always attentive and online? This is something you need to ask yourself.

Can Governments Eavesdrop On Our Devices?

The short answer to this is yes. Just as governments tap telephones when they have what they consider a legitimate reason, it's also possible to tap into our connected devices.

It's already public knowledge that the National Security Agency NSA intercepts, evaluates, and stores vast amounts of data tapped every day from the internet.

Edward Snowden revealed that the NSA uses backdoors provided by device and software manufacturers to eavesdrop on devices as well as view emails, documents and images to determine the locations of people.

How Can You Best Protect Yourself Against Device Eavesdropping?

It's not absolutely certain whether the on/off button on Amazon Echo and other devices actually does what it claims. It's been suggested that mobile phones and devices like Echo can still be listening even when they are switched off.

The only way you can be certain your devices are not eavesdropping on you is to disconnect them from the internet.

There are a number of other steps you can still take to protect your digital privacy:

- Only switch on devices such as Amazon Echo when you actually need to use it.
- Avoid using the "quick" or "easy" setup options when you activate a new device. Instead, select "custom settings" that give you the ability to set privacy features on a more detailed level.
- Keep your webcam covered when you're not using it. You might also want to cover the microphone slit on your device as well. FBI Director James Comey publicly admitted that he puts tape over his laptop webcam and advises other people to do the same.
- Be wary of terms of service changes proposed by providers and app developers. Sometimes these can involve subtle changes giving the provider the right to eavesdrop on your device and data. Check any proposed changes carefully.
- Keep informed on software updates and what they do in terms of changing functionality related to privacy.
- Take the time to learn how the privacy settings on your device operate and how to set them. Contact customer support if you need additional help with configuring them.
- Seek out alternative apps and if necessary devices if you're unhappy with the privacy policy of your present ones.

Conclusion

The range of smart voice recognition devices and apps available is still small, but we're on the brink of seeing an enormous expansion in the volume and variety of devices that will employ voice recognition.

We can't stop voice recognition development – it's far too useful of a technology. Yet we do need to be careful that it does not get out of control and become too easily used against us.

We're going to be seeing a great deal more device eavesdropping issues in the future. We'll also see more hacking incidents as different types of household devices become connected to the Internet.

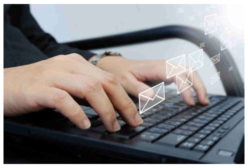
There are a whole range of matters of concern surrounding digital virtual devices which are going to have to be clarified. The future is going to be interesting.

Do you have any thoughts on device eavesdropping? Do you think that people will need to fight back for their right to privacy? Do you think that this issue is something we don't really need to worry about? Please let us know what you think by leaving a comment below.

0

RELATED ARTICLES

Mobile Banking Malware Gets



Real

How To Keep Your Email Secure From Hackers

How Encryption Can Help Protect Your Data from Theft and Interception

We will be happy to hear your thoughts

LEAVE A REPLY

Name

E-mail

Website

Post comment

□ Notify me of followup comments via e-mail. You can also subscribe without commenting.

‹

atest Articles

- Digital Personal Assistants and The Risks of Device Eavesdropping
- 3 Best VPN's For Apple Mac Computers
- Mobile Banking Malware Gets Real
- How To Keep Your Email Secure From Hackers
- Best VPNs for College

Feature Guides

How To Watch Netflix Outside the USA
Best VPN Service Review Guide
Reviews

SECURETHOUGHTS
INTERNET SECURITY FOR EVERYDAY PEOPLE

Secure Thoughts is the industry leader in helping everyday people make sure their information and loved ones are protected online.

Your future and the future of those you love is too important to gamble with.

When you need the right advice, trust Secure Thoughts.