BlueOrange Alert:

Voice Control Devices and Remote Work

Is My Smart Assistant Spying on Me?

In response to minimizing the impact of COVID-19, organizations are adopting strategies to allow employees to telework remotely. With these processes and procedures come new security concerns. Keeping PHI and PII safe and secure are at the top of these concerns. Many remote workers are repurposing existing areas of their homes for their "office."

The Concern

Concerns have been raised regarding the class of devices known as Smart Assistants. These include Apple Siri, Google Assistant, Amazon Alexa, and the Facebook Portal, to name a few. These devices operate and respond when a 'wake word' is spoken in the presence of the device's microphone.

The primary concern with teleworkers on calls or video conferencing sessions discussing sensitive data is that the data is being captured and stored somewhere, putting it at risk of being exposed or breached.

What Can You Do?

Unplug or power down the device if you are concerned about data being captured.

Enable manual activation. Current generations of smart assistants support voice capture only after a button is pressed, thereby eliminating the threat of mis-hearing a wake word and capturing sensitive data.

Some smart assistants support setting up time frames to purge any captured data. Some, like Amazon Alexa, will let you
review the data that has been captured by your device.

How They Work

The devices themselves have a microphone or a series of microphones. The device is always listening for a word that is the wake word, the device starts sending information following the wake word to the host provider (Amazon, Apple, Google, Facebook, etc). The information is captured and if it corresponds with functions the device can perform, or related to services, those commands are executed. Once complete, the device stops capturing and sending the audio input and goes back to being a localized ‘always listening’ device.

The wake word is a predetermined word to let the device know that user input is following. The device only actively transmits what it hears after hearing the wake word for a specific length of time, anywhere from 4-25 seconds on average. Consider the following examples.

John has an Amazon Echo Dot in his home office. It's linked to his Spotify playlist, his calendar, and other productivity tools. His wake word for the Dot is the default "Alexa."

Published: March 25, 2020 © 2020 BlueOrange Compliance. All Rights

Scenario 1: John is working on a report and wants his "Get Stuff Done" playlist. He says, "Alexa, play my get stuff done playlist."

The Echo Dot goes through the following steps:

- The Dot hears the word "Alexa" and starts actively capturing audio, listening for a command it can respond to.
- It hears the command “Play” and a playlist.
- It starts playing the specified playlist.
- It actively sends audio for several seconds more in the event a follow-up command is issued.
- The device stops actively capturing* information and goes back to listening for the next time a wake word is issued.

Scenario 2: John is on a phone call talking with a client. On the call he says, "No, his credit score dropped because he took out a loan on a Lexus and it got repossessed."

The Echo Dot goes through the following steps:

- Voice-activated microphone hears "a lexus" and responds as though it was the wake work and starts actively capturing audio, listening for a command it can respond to.
- It hears no command it can respond to following the wake word.
- If the words following what it thought was the wake word are similar to commands it can perform, it may try to seek clarification.
- "Would you like information on Possession?"
- Or, it may actively capture information for several seconds more* in the event a follow-up command is issued.
- The device stops actively capturing* information and goes back to listening for the next time a wake word is issued.

Is Your Data Safe?

Major providers of smart assistants have given assurances that the data collected is randomized and is not stored in a way that would identify. They have also stated that any data that may be retained on their servers is done only in the interest of improving the response of the smart assistant and reducing the number of false positives from words that are similar to the wake words.

Amazon has developed ‘skills’ for its smart assistants that are some level of HIPAA compliant *in very specific instances.* This is not to imply that the device is HIPAA compliant in every use scenario. It is not.

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits. BlueOrange Compliance provides this alert for educational purposes only without warranty and specialized advice should be sought about your specific circumstances.

Published: March 25, 2020 © 2020 BlueOrange Compliance. All Rights