LTT LAW TECHNOLOGY TODAY

ALEXA, HOW DO I PROTECT MY ORGANIZATION'S DATA FROM YOU?

Brian Schrader | January 15, 2020

Has Alexa infiltrated your company yet? There are 3.25 billion users of digital voice assistants in the world. It stands to reason that if you haven't seen one of these devices on employees' desks yet, you soon will. The industry is expected to grow to eight billion users by 2023.

The prevalence of smart speakers

From the multitude of Alexa devices to Google Home to Apple HomePod to other smart home devices, there are ears everywhere. The devices are trained to listen to what you say and respond as you need them to. In fact, they are listening even before you say "Alexa" or "Hey Siri" because they need to know when you are addressing them.

Amazon, Google, and Apple have been in the news lately because their smart speakers may have been violating users' privacy. The companies had human reviewers listen to data

continued next page

collected by the devices—unbeknownst to the users. While that practice is changing, there is still the possible dilemma of a device recording you, even when you don't want it to.

That is something to think about as digital assistants, like Microsoft's Cortana and Alexa for Business, make their way into the workplace. Smart speakers initially handle simple tasks, making it easy for a user to check the calendar and add meetings, create and track to-do lists, read and send emails and instant messages, and ask general-knowledge questions. Eventually, those devices will also become the go-to for accessing business applications, financial reporting, system monitoring, customer support and information from other custom integrations.

More than 18,000 companies already use Alexa in some capacity, and the total jumps higher if you include devices from Apple, Google, and other manufacturers. For example, McDonald's uses voice-activated devices to accept job applications. Companies and law firms also use them in a variety of ways, placing them in individual offices and common areas, like break rooms and conference rooms.

With wider use comes increased security concerns.

Business confidentiality, phishing, and hacking concerns

If these devices are not set up and monitored properly, they could pose serious problems to organizations. For example, last year, a family in Oregon found out that their smart home device not only recorded a private conversation without their consent or awareness, but it also randomly sent the recording to someone in their contacts list.

It is very easy to accidentally trigger an unintentional recording. That means the device may listen to background comments and sensitive business conversations. Additionally, as the smart speaker gains access to a business's platforms with the idea of increasing production and efficiency, a bad actor could put those pathways to nefarious use.

Recently, researchers used Alexa's "skills" and Google's "actions" to conduct malicious test tasks. Unfortunately, it was surprisingly easy to pull off. When a user would ask for something seemingly simple and innocuous, like a horoscope reading, the device would respond as anticipated while also conducting additional tasks in the background, such as eavesdropping or phishing. The researcher-developed apps could trick the user into thinking the device wasn't recording or, even worse, providing a password to access confidential files.

continued next page

The devices could also be used to monitor employees, tracking characteristics like tone and sentiment using AI. They could even access employees' health statistics. Digital voice assistants could use data already collected to forecast a person's future actions and then see if their predictions are correct.

Data protection and legal issues

As GDPR considerations make their way into the U.S. legal system, and as states take the lead on privacy laws—like California's recent Consumer Privacy Act—there are increased calls for transparency and disclosure. That means rules will require the user to understand and agree with what the device is doing before private data gets collected. That is also why Alexa, Google and other apps allow you to log in and see data files and transcripts.

Legal disclosure obligations also may be triggered by these devices. Regardless of when or how a digital voice assistant gets data, that data may need to be collected, analyzed and produced for a legal or investigative matter. That means the devices may cause more hassle and cost than estimated. When it comes to the courts, it doesn't matter where the data resides; if it's potentially relevant, it needs to be gathered for review and analysis.

Data from these kinds of speakers are already being used in criminal cases. For example, Amazon Alexa data and recordings were used in murder cases in Arkansas and New Hampshire. Other digital devices, including Fitbits and pacemakers, have been used in additional cases.

When it comes to corporate data, smart speakers could reveal information that wouldn't come from emails or other documents, such as a private conversation in the break room or complaints in an office. That data could be discoverable in a document request, whether or not the recording was intentional.

Creating an implementation plan

Right now, the use of smart speakers is similar to when smartphones first came into use. As they did then, companies typically respond one of three ways:

1. Ignore it and wait for it to be a problem (or hope it goes away).
2. Forbid smart speakers entirely, which can be difficult to enforce.
3. Create formal policies that outline acceptable and non-acceptable usage.

continued next page

The third option makes the most sense, and it will have to be done eventually anyway, so it's best to start now. That will help you create a path to smart adoption.

Your policy should:

- Include a formal corporate statement regarding which, if any, smart speakers are acceptable to use.
- Provide use cases, especially within the context of the normal and routine operations of your business, that give clear examples to employees of both acceptable and non-acceptable usages.
- Detail areas where the smart speakers can and cannot be used, such as areas where especially sensitive information may be routinely discussed.
- Encourage the use of privacy options like a microphone mute and camera blocks that are built into or available as add-ons to most smart speakers.
- Create a formal training program to ensure that all employees are informed of the new smart speaker usage policies and follow up with routine refreshers.
- Routinely track and survey employees regarding their use of smart speakers, including asking for examples of how they use them, which can help further develop corporate policies.
- Keep abreast of compliance solutions, which will inevitably come into place with widespread corporate usage.

Smart speakers have the potential to help corporations and law firms get more work done — and to complete it in an easier, more effective way. But the truly "smart" part of the speaker still comes from humans. Make sure you take advantage of their capabilities in an intelligent, well-planned way.

ABOUT BRIAN SCHRADER

Brian Schrader, Esq., is President of BIA (www.biaprotect.com), a leader in reliable, innovative and cost-effective eDiscovery services. With early career experience in information management, computer technology and the law, Brian co-founded BIA in 2002 and has since developed the firm's reputation as an industry pioneer and a trusted partner for corporations and law firms around the world. He can be reached at bschrader@biaprotect.com.