Are Alexa and Her Friends Safe to Use in Your Law Office? The Pros and Cons of Personal Assistants

by Sharon D. Nelson and John W. Simek

Many commentators have predicted that 2017 will be the year of Amazon's Alexa. Alexa is one of several virtual voice assistants that are working their way into our everyday lives. The Amazon Echo and the smaller Echo Dot had a great sales year in 2016 and finished off the holiday season as the best-selling items on Amazon. Estimates by Forrester indicate that 6 million Amazon Echo devices were sold by the end of 2016. That's a lot of hardware.

Alexa is just one of the virtual assistants available for lawyers today. There's also Google Home/Google Assistant, Siri, Cortana and Samsung's Bixby on the Galaxy S8 and S8+. Siri was the first on the market but has rapidly lost ground to Alexa and Google Assistant, the two big players in the virtual assistant offerings. Google has the advantage for research since it has access to the power of Google search. Alexa is a better integration device, especially with the addition of "skills" that allow it to connect to other services and apps. Bixby is the newest player in the virtual assistant space and promises to have some unique features that don't exist in the others. One such feature is the ability to take a picture of something in a foreign language (e.g. road sign, business advertisement, etc.) and Bixby will translate it for you.

There have been many articles about how a lawyer would use a virtual assistant. Some of those uses could include accomplishing simple tasks such as adding entries to calendars, setting reminders, calling people in your contacts, getting directions, obtaining weather conditions, obtaining answers to questions, making purchases, controlling items (e.g. turn on/off lights), reading news items, playing music and the list goes on and on.

Cybersecurity and Personal Assistants

The obvious question revolves around the security of these types of devices. Is Alexa safe to use in a law office? That's a question we get quite often these days. The short answer is yes if you take certain precautions and understand the pros and cons of the technology. Let's start with how Alexa works. Alexa is tied to your Amazon account. That means it is already associated with you and is not anonymous. Alexa is constantly in listening mode, waiting for the wake word to be spoken. You configure Alexa to respond to one of the four (Alexa, Amazon, Echo, Computer) wake words. Amazon has announced that they are working on allowing users to define custom wake words, but no delivery date is currently available.

Once Alexa "hears" the wake word, it starts recording just a few seconds before the wake word and sends the data to the cloud. Amazon performs a speech to text conversion and tries to properly respond to the command or question. Amazon stores the actual recorded session so that you can play it back from your account. That means Amazon also has a recording of any ambient noise that may have been picked up as well.

It is unclear how long Amazon may store the recorded sessions. You do have the ability to delete individual Alexa requests or delete them all. Think of it as clearing up your Internet history. Unfortunately, Amazon uses all of the history to make Alexa "smarter" by learning what you ask for and how you ask it. If you delete all the voice history, Alexa will effectively revert back to a new factory setting. That's the tradeoff between privacy and usability. Maintaining your privacy means less usability.

Alexa can't differentiate between voices either. Some people think that's an advantage since all of your family members or law firm personnel can talk to Alexa using a single account. We believe not differentiating voices is a disadvantage and a big security hole. Anybody within hearing distance of Alexa can ask for information that may be related to your account. As an example, a nosy relative could ask what is on your to-do list, read your mail, send a text message or access any other information that is linked to your account. Amazon has announced that it is working on differentiating voices, but no timetable has been given for delivery of the enhancement.

Samsung has taken a different approach to always-listening devices like Alexa. By default, Bixby won't listen until you press a button. This means the user is in control of the data. With always-listening devices, you really don't know what is being stored by the vendor.

Tips for Keeping Your Data Secure

Because Alexa cannot distinguish voices and it is always on, a best practice would be to physically secure Alexa in your law office. That means it should be in a room away from typical conversations and probably even behind a locked door. Physically securing Alexa gives you much greater control over access, especially since you can command Alexa without giving it a user ID or password. It's another trade-off between security and convenience. If you had to give Alexa your login ID and password every time you asked a question, you would probably ask for your money back within 24 hours.

Another security configuration is controlling purchasing through the Alexa app. By default, Alexa will allow purchases using your Amazon Prime account, where you have already registered a credit card. It's probably not a good idea to leave this at the default setting. Anybody within earshot can make a purchase using your account. You may have heard the San Diego news story about a girl in Texas that ordered a doll house and four pounds of cookies using Alexa. The problem was that a bunch of Alexa devices in the San Diego area "woke up" when they heard the wake word and tried to order doll houses. Humorous, but you see the danger. You can configure Alexa to require a 4-digit PIN confirmation code to complete a purchase or turn off voice purchasing all together.

You have the option of restricting when Alexa listens by muting the seven microphone array. It is a manual process to press the mute button, which effectively disables Alexa. You know that Alexa is in a muted state by the red ring that glows around the edge. Pressing the mute button again puts Alexa back in listening mode and removes the red ring. It would be a best practice to mute Alexa if it is in a conference room where you are having a confidential conversation with your client to ensure that no part of the discussion is inadvertently recorded.

The Pros of Personal Assistants

One of the pros for using voice assisted technology is making tasks more efficient. Rather than opening a program on a computer and typing in data, you can just speak what you want to do and it happens. Control of devices is extremely easy using the technology. Google Home is the hardware that is "powered" by Google Assistant. It was originally designed to work with home smart devices such as thermostats, smart appliances, light controls, security systems, etc. Think of it as remote control on steroids. You can operate all sorts of smart devices just by using voice commands. Adjust the temperature in your office by saying "Set the thermostat to 72 degrees." When leaving the office for the day, you can command all the lights off with one statement like "Turn off all office lights." Even smart appliances can be controlled by voice. As you get ready to leave the house, just tell your voice assistant to turn on the office coffee maker. Fresh coffee will be ready when you arrive.

Another popular usage of personal assistants is access to a music library. Alexa can access music in your Prime library as well as Spotify, Pandora, iHeartRadio and TuneIn. Google Home can access audio tracks from YouTube Music, Spotify, Pandora, TuneIn and Google Play Music. You can play specific tracks, artists, genres, etc. Alexa can read books from Audible or your Kindle library. The Amazon Echo is a more expensive device ($179.99) that projects sound in 360 degrees using the included 2.5 inch woofer and 2.0 inch tweeter. The Echo Dot is a cheaper alternative ($49.99) and only includes a small built-in speaker. You can improve the sound quality by connecting external speakers using a 3.5 mm audio cable or over Bluetooth. In contrast, Google Home is $129.99 for the white version. You can add different color bases for an additional $10.

Siri and Cortana are more limited in what they can do for you. As an example, Siri only supports a handful of uses such as photo search, video and audio calling, payments, messaging and ride booking. Siri has begun to work with some third-party apps with the release of iOS 10, but usage is fairly limited. Apple is trying to get into the smart home control market with its HomeKit connected solution, which is still in its infancy.

Google Home has the edge for lawyers, especially when it comes to research. That's because Google Home has access to the vast database and power of Google search. Using Google Home is like using your voice to search Google instead of typing the search phrase in a Google search box. Alexa will respond with "Sorry, I couldn't find the answer to your question" for things that it doesn't know about. You do have the option of using Bing for searching if it can't find the answer to your question, but you have to use the Alexa app for that. The reality is that Alexa is pretty poor at searching. If you want to use your voice assistant as a legal research tool, you're better off with Google Home. Who knows? Perhaps some developer will release a "skill" for Alexa allowing the use of Google instead of Bing for searching.

What happens to your personal assistant data?

The big concern among lawyers is the potential evidence that a voice assistant may capture. We know that Amazon stores the requests to Alexa since you can see them in your Alexa app. As previously stated, you do have the option of deleting them. We already know that prosecutors in Arkansas have issued a search warrant for data from an Amazon Echo that was in the home of James Bates, who was accused of strangling and drowning a man in his home last year. Amazon has rejected the request as

being overly broad. We don't know if Amazon will be compelled to release the data, but the point is that Amazon does have data that can be used as evidence.

Apple reportedly stores your Siri data for two years. Supposedly, the data is anonymized to protect the users' identity, but do we really know for sure? Like Alexa, you can view your Google Home history and delete it if you want. Google does save your queries so the situation is very similar to Alexa. What if law enforcement wants access to your Google Home data? How long does Google keep the information and will they turn it over? Even though the vendors say they are concerned about users' privacy, the point is that technically your information can be stored for a long time and turned over to the government or law enforcement. The devices themselves (e.g. Echo, Google Home, etc.) don't store the user requests. The information is sent to the cloud. The situation is a little different if you are using a voice assistant on a mobile device. There is the possibility that some data resides on the mobile device as temporary storage in addition to being sent to the cloud.

Another best practice for lawyers is to periodically inspect the stored history. Deleting the history on an occasional basis is probably a good idea too, but that would impact the efficiency of using voice assisted technology.

What's a lawyer to do?

Lawyers have specific ethical duties, so they have to be more careful than the "who gives a darn about privacy?" masses. We have found that lawyers rarely think about keeping data confidential with respect to their personal assistants, which tend to be compellingly addictive. Just as it took a while to get used to the notion that we need to be serious about protecting confidential data on our computers and phones, it will likely take a while for the legal profession to wrap its head around the dangers of personal assistants – and the rich lode of potential evidence that may be found in the clouds that store questions or commands addressed to personal assistants.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com