Are They Always Listening? How Secure Is My Smart Speaker?

June 2, 2021

Webinar from Pennsylvania Assistive Technology Foundation's
Smart Homes Made Simple Project

Susan Tachau: I think we'll go ahead and start. We can have the next slide. Thank you very much. Hello, everyone, and thank you for joining us today. My name is Susan Tachau and I am with Pennsylvania Assistive Technology Foundation. Welcome to today's webinar, *Are They Always Listening and How Secure is My Smart Speaker?* Our presenter today is Kirby Smith, we're pleased to have him. Kirby is a consultant with our project but also, he's the president of SunKirb Ideas. He will introduce himself in just a minute.

This webinar is part of our project that we have *Smart Homes Made Simple*, a project that's funded by the Pennsylvania Developmental Disabilities Council. If you go back a slide Susie, real quickly, you'll see that we have a website, smarthomesmadesimple.org if you would like to learn more about the work that we do, and read some blog articles, some of which are written by Kirby, so you'll probably be eager to hear more from him after today's webinar. Now we can go to the next slide.

Before we start our webinar, we want to have our first of two poll questions so that Kirby will be able to start us at the very beginning. The poll question is, do you think your smart speaker, for example, an Amazon Alexa, or a Google Nest is always listening to you? Yes or no? If you fill those in, Susie, you can let us know when all of the responses are in there.

Susie Daily: Yes, people are still working on it. I apologize it looks like it cut off the last word of our question. All right, I'm going to end the poll and show the results.

Susan: Aha. Do you think your smart speaker, for example, your Amazon Alexa, or your Google Nest is always listening to you? 73% or 11 of you said yes and only 27% or four of you say no. All right, so Kirby, you've got your work cut out for you?

Kirby Smith: [laughs] Well, good afternoon, everyone. As was stated, my name is Kirby Smith and I own and operate a business that designs and sets up smart homes with a focus on people who are either aging or with disabilities. My primary type of device that I like to use if the recipient is able to use it is a smart speaker, especially smart speakers with screens. Of course, over the years, I've been asked many times, aren't these things always listening? Are they safe? We were thinking of putting one in my kid's bedroom, will it be listening to their conversations? Will my banking information or other information be overheard and spread or stolen by someone?

What I'm going to do is talk to you about basically how they work, and also open it up to a larger scope in that there are many devices we use that we take for granted and we aren't asking that same question. I'm going to focus on that and then come back to whether or not they're actually secure. If we can go to the next slide. Let's start with, what are the concerns? Your watch, your cell phone, your computers, some people's refrigerators, there are so many devices right now that are listening, not whether they're recording, whether

they understand whether it's going anywhere is something different, but almost everything around us is listening.

Why is it that smart speakers tend to be the focus of so many people's fears while they carry their phones freely around with them? Well, the reason why is because they advertise that they're listening. In other words, buy the Google smart speaker because that way if you come in and you need something you just call it and it's going to answer or for Alexa, the idea that this device is going to turn on your lights when you need. To a degree, yes, they're always listening. Now, are they processing or doing anything with it? That's the part that's different. To understand that, let's talk about exactly how do they work.

First off, they're nothing but very sophisticated Bluetooth speakers. They're built for music and sound primarily. If you say take something like an Echo Show, you have a screen on, that screen gives you feedback information. It has a camera, it can also do things with the camera. For example, in the newest model of the Echo Show, you can take Zoom calls on it, so it is transmitting and sending information backwards and forwards. However, it has limitations. These smart speakers are not full-on computers. What makes the big difference? One, it doesn't have a real processing chip.

In other words, the chip that's designed to do multiple things like the chip in your cell phone, or the chip in your computer. The primary computer, and if you want to call it that is really only doing a couple of things and the primary function it has is to figure out when are you talking to it. It hears everything, but it's not necessarily doing anything with it. It's just taking something, processing it slightly, and sending it off. What is it processing? Well, they would be pretty useless if they were always listening. I've had times that I've said the word Alexa or hey Google tube boots, too many times in a row.

What happens is it pretty much goes dead for the next couple of minutes because it gets in a loop. What it's trying to deal with it is the wake-up word. If we can jump back to me for a second. This is an example that's an older model but I don't know if you can see it clearly. I think you can. You'll see little indentations, tiny holes that are going around the device. For this one with the Google speakers and others, they tend to have multiple microphones going around them to allow them to separate the different sounds out. Why is that?

Well, if you're in your room, your voice and other sounds are bouncing around.

For example, in my background, I've got an air purifier because I have the door open is running on high, if birds are tweeting on the outside, you may occasionally hear a conversation from downstairs. What it's doing with all these microphones is it allows it to compute and figure out where is the sound coming from. For starters, it's hearing everything across those microphones not really doing anything with it until you have a wake-up word. If we're talking about Echoes, and we tend to call them Alexas, it's waiting to hear either the word Alexa, Echo, Amazon, or computer, and that's based on your settings when you set it up. The default wake-up word is going to be Alexa.

Once it picks that up, the other thing that happens and so you have multiple ones, so let's say I've got my fire cube sitting in one area, this one sitting but they're close in the same room is by using these microphones, it can figure out which unit is sitting closest to you.

Then the assumption is okay, that's the one that's going to take the command. Once it receives the wake-up word, it does have enough memory to record a long sentence, but in terms of conversations or whatever, that's not going to happen. It just simply can't hold it that long.

It hears the wake-up word, it figures out. It did actually hear the wake-up word address to it and then it begins to record that sentence that it hears. It then fires that off over the Internet to cloud servers. If we're talking about Amazon, that's the AWS, as it's called Amazon Web Services, if it's Google, they have the Google Web Services. What that is, it's just a bunch of very powerful servers that able to process information very fast, and then act on it. Going back to what happens when you use the wake-up word Alexa on this, it here's the wake-up word, records that little bit of the sentence following it, and then it shoots that out to the servers, the servers process it.

What they're doing is not truly natural language processing. Google is a little better but neither one is really near where it truly is understanding you. What it's doing is just picking out keywords. If I were to say, "Alexa, turn on the bedroom lights." It might even pick up someone's voice but what it's going to see is Alexa to wake it up, turn on which you can also say switch on. You can also say-- what other things people say? Tune up lights and then it'll be the name of the light. It's going to put that into a table, those keywords, process those keywords, and then make a decision on that. It will then go out.

If you do happen to have a device that has the proper name, that it has the ability to turn on and off, it will go ahead and execute the command. The execution of that command gets sent back to the Alexa services and then your speaker will say to you, "Okay, [chuckles] to let you know that the command was carried out. What you got once again if we go back to the concerns people have is a device that's built to listen to you. But in terms of really listening to you, really doing anything with it, it's not going to do anything until that wake-up word is executed.

Whether it is a unit based on Apple HomeKit and you say something like Siri or Google or Alexa, they're not truly listening. The other reason they're not truly listening to everything you say, bandwidth. They really just can't process it that much. If I go and I look at my logs on my router to see which devices are using the most, my Alexa units are at the bottom of the barrel. They're hardly even making the list. The reason why is that they're only shooting that information out when you do the wake-up word. That information is pretty much going to be things like turn on the lights, turn off the lights, what's the news, what's the weather, how's the traffic, things like that.

You're not getting any real hardcore information that's shooting across the system. How do they compare to other systems? Well, it is very easy for me to go into my Alexa app and see or hear everything it has heard, see every command that was given, and see every device that was affected by it. It's not buried under any things. It's right there on the main menu under history and activity and I can go in and see it. Later on, I'm going to show you an example of that. It's as boring as it can get. In the several years that I've been looking over these listening to the logs, I had never once heard something that concerned me such as a banking number or a big secret.

It has always pretty much been mundane things like, "Turn the temperature to 72," "What time is my next appointment?" Things like that, but never anything that really totally concerned me. The biggest concern we should have are our cellphones and our computers. I'm going to start with computers. Let's say you have a Mac and use Messages on your Mac. Messages, if you've never used a Mac is similar to the texting function that's on a cell phone, an Apple phone. The minute that system turns on, it switches on the camera. Whether or not you're aware of it, if you don't have the screen up, it's looking at you and it's listening to you to hear what you have to say.

On Windows 10, a lot of people aren't aware that it can be completely voice-controlled. If you give permission for that to turn on, that voice control ability kicks in which means it has to use the mic, it'll use the camera. So what's happening now is it's listening. How does that compare to smart speakers? Well, here's the issue. If I go in and I look at what has permission to use the-- I'm going to use the microphone here. Right now what I'm looking at is the list of apps that have permission to use my microphone. In many ways, there's no way around it because one, I voice-control a lot of things like my music and stuff. I use Facebook and I'll send messages through Facebook.

You have texting. There's games where it has to hear the answer to things. If we go through this list of things that are using my microphone, there's almost about 40 different apps. They have permission to grab use of my microphone. At the end of the day, what happens is you pretty much have to trust that when you end that app, you turn off that app and stop using it, they're going to stop listening or they're going to stop looking. Unfortunately, there have been some bad actors. Quite a few actually.

What will usually happen is that whether it's Apple or Microsoft or whatever, once they hear enough complaints, they may stop the app from functioning or make a pop-up that tells you that it's running in the background. But it is very difficult to manage what's listening. When I carry my phone with me on the bus, I'm driving, I carry it with me to the bathroom, it's listening and it can look potentially. Between the two, a smart speaker, a phone, or even my computer, I consider my computer and my phone the biggest threat. Especially the computer because it is more likely that you're going to be handling things like banking information, investments, your contact list to other people.

All of that information is sitting on your computer and once you've given permission to those apps that are running, whether it's on your phone or your computer, they can go in and use it if they decide to do so. Let's go to the next slide if we can. Once again, let's go back to why is it that smart speakers get so much worry from people. There. Why is this that it worries people? Well, the reason is that for a lot of people especially if you're not used to it, the idea that a device is listening and responding to you is creepy. It's scary. On the newer Echo Show, because it's designed for video calls, the screen actually follows you.

I installed it a couple of months ago into my mother's home for her to use because I call her a lot through video calling and the very first day she was like, "Oh, I don't like that. Turn it off. The idea that it's looking at me and actually turning its head," is what she said, "and following me, I don't like that at all." Two weeks later she says, "Oh, I love it because wherever I'm walking around the kitchen or whatever, if I'm using a recipe it's looking at me and it's giving me the information." I think the creepiness factor comes in because it's

literally responding to you real-time whereas your phone could be passively listening and you don't know.

You kind of know when these smart speakers are working. That's creepy on one hand. On the other hand, it's also good because I know immediately what's going on. There've been times I don't know maybe it was something on the television, something in the background, my Echo will flash meaning it's listening and that's another feedback thing. I see the little blue light on the bottom that lets me know it's listening. But the fact that I know it's listening helps. There's always been a mistake and if I go in and listen to the logs I'll hear what the sound was that was close to what it thought was the word, Alexa. If we look at Google, it's a whole other world.

If I have to point out two businesses that worry me way more would be Facebook and Google. On your phone, and I don't know why my light is on. Going back to your phone, when you turn on Facebook on your phone, it continues to listen, it continues to look. Now, not in an aggressive way like it's taking pictures of you or things like that. It could sometimes be using the camera just to know that you've picked it up, that you've moved it to a different environment. What's also scary is using GPS. If you were to go and look and you have to dig through Facebook and you have to dig through Google, if you go through the menus, you will see it knows pretty much who you talk to, it knows where you've been, where you traveled. It can tell you the number of times you leave your house in a day. They're collecting a tremendous amount of information.

Now, let's go back to when I was talking about memory capacity on smart speakers. Once again, if I go in and look at my Wi-Fi for what's been used in terms of bandwidth, it's very very low on my smart speakers. If it does jump a little bit, it's because a lot of times I watch a movie or something on my Echo Shows. However, if you go and you look on your phone for bandwidth and this is whether we're talking about Android or iPhones, the number one app that will use bandwidth is always going to be at the top of the list unless you look at a lot of movies throughout the day, is going to be Facebook.

The reason why is it's running in the background, collecting information, and shooting it back to the cloud server so it is always working. A recommendation that privacy is a big issue for you, when you're done with your Facebook app on your computer or your phone completely shut it down, don't leave it running in the background, and do not give it permission to operate in the background on its own. If we then take the comparison to a smart speaker, and a phone or a computer, the smart speaker's going to rank down here in terms of what's being collected on you.

The others are just through the roof. It's amazing. Even if you look at your battery consumption, what's using your battery, you're going to find almost always Facebook is going to be at the top of that list. Let's go to the-- Then another reason that these things can be a little scary is the artificial intelligence behind them now. Like I explained, it doesn't truly understand the words you're saying. Once again, it just seems strange that it can come across as so smart. When we're using these because there's no response because we don't see that they listen to us or whatever.

Because we're not seeing GPS being used, even though it is running in the background reporting back to Google and Facebook, it's a much more sophisticated AI running on this than it is on a smart speaker. Smart speaker's AI is almost all wrapped up and trying to carry out a command. That said, the information that Amazon is collecting on you is more around sales. They may look at how many times you turn a light on, but that'll tell them okay, we might want to sell more lights. For the most part, Amazon wants you to buy products from them by using these speakers because you can order items through them. They also get a sense of some of the products you use a lot by looking at lights that are turned on and off.

Pretty much everything I do on here is getting recorded and sent to Facebook and Google. Me personally, I am bothered by the amounts of what I consider to be spying on me from Facebook and Google because of the fact that I can't go and easily see what they've collected. For example, GPS is stored in a different area, recordings and things is heard, is stored in an area. But then the list gets crazy because the contact list that it's collected of who I've talked to. I have a friend, he doesn't use Facebook at all, but I had to show him that if I googled his name in Philadelphia, his face comes up because other people have taken his picture.

People went in on Facebook and identified him by his name. Facebook, even though he's not a Facebook user knows who he is, knows where he goes, knows the type of people he associates with. Once again, I'm more worried about Facebook. Next slide. At the end of the day, your phone and your computers are much, much more. Right now we're Zoom calling using a computer. Right now, our computers are acting as a video call system similar to a telephone with a screen, but still, everything in the background on that computer is still running.

Inside of your browser, there are what's called extensions. Those extensions are reporting where you're located. Every time you go to a site, it can even be a newspaper site and you pull up an article, that newspaper site gets back information on who you are, the article you pulled up, where are you located, and if you did a search where you're going, and possibly the time you're going. Smart speakers pretty much have a much more limited function. Phones, computers, universal functions. Next slide, please.

Susan: Kirby.

Kirby: Sure.

Susan: Before you move on we have a question. One that I might ask myself. Can you please explain again where exactly you can check on your phone to see if the phone is listening?

Kirby: Okay, that's the tricky part. [laughs] Once again, it's any one of those is fairly easy. The problem is it's all spread out. Let's go to the next slide if we can. Here I'm going to start with describing it on, for example, Alexa, and then I'm going to try and discuss it dealing with phones because unfortunately, it won't be as easy and answer. What you're looking at on the screen right now is the main menu if you're going to the Alexa app. If you go down second from the last at the bottom, you see activity with the clock. It's very noticeable. I've never had trouble conveying this to someone, I'll say go to the main menu, look for activity. If you click on the activity, and if we could go to the next slide.

On the left side, you see, I can look at my voice history. Everything, every single one of my units has heard. I can hear that, and I can see what it translated that to be. I can review the history of detected sounds. My system also acts as my security. I can say to it, for example, when I leave the home based on my phone's position, or when I leave the house, and I say I'm leaving, turn on the guard, and any strange sound record it. I can come here and see the sounds even that it has heard. I obviously have no interest if I'm in the house.

If I'm not in the house, and I want to see what it heard, I can go there and see it. I can review the Smart Home device history. Every device that Alexa has interacted with, I can go and see a list of the device, the date, the time, and what happened with that device. If I want to manage the skill permissions, so skills are similar to apps on Alexa. The thing is, they only run when you call them, and they tend to turn off when you stop using them automatically. An example of a skill is I play Jeopardy on my Alexa sometimes, the game I play with other people. It's using the mic, it's hearing what I'm saying constantly. It's not waiting for the wake-up word once it starts, but it's cueing me when it wants to hear things.

If I stop and go quiet for a short while, the app automatically shuts down and goes away. I can go in and see all the skills that have permissions and what kind of permission they have. Some skills have permission to use the camera. For example, if I'm running a security app, the app has permission to see through the camera, I can go and see that that app was using it. Once again, these are all laid out there. They're very simple. If we look to the right, this is the voice history of what it's heard. If I were to pull this up, it could be a year's worth of things like what you're looking at. Alexa go home, show the doorbell.

Can we go to the next slide, show the TV list. Alexa, delete number two. There's nothing on this list that concerns me. If it didn't actually respond or do something, those would be the ones that you'll notice it says audio was not intended for this device. They hear very well. I can be on a different floor, the one downstairs, here's what I said. Where you see that marking is saying the recording was actually answered on a different device, but it heard you. Not only am I seeing what the device heard that's responding to me, I'm seeing that the other devices heard it, and when they heard it, so it's very easy for me to say, "That's interesting.

My Alexa sitting by the television downstairs seems to pick up everything, but I can actually see it." I've scrolled through a year's worth of these, there's just never been a single line item on there that worries me in terms of security. If we come back to me. If we're talking about iPhones, it's going to be somewhat similar under on Android. What I do is I look for, where's it? The privacy setting. Settings, give me one second. Once again, as you can see, every time I do this, I have to search. There it is. Okay, so this small blue-- I keep hitting it with my hand. Sorry about that. This small blue line in the middle, you'll see privacy. If you click on that. Okay.

That is giving me the top-down report of my privacy, but it's for each app. As you can see, I've got quite a few apps that are running here. Even then that's only the apps that are reporting and working in compliance with Apple. Other apps don't necessarily report this information. If I go back. Does that show me everything? No. I literally have to go under the app itself to see that information. Let's go with the big guys, Facebook and Google. Two

problems there. If I bring up Facebook and I look at the opening screen, what is it doing? Okay, this is a new thing.

I might as well speak about it. What's happened is that Apple is trying to clamp down on all of these apps just grabbing things. What they're doing now is they're requiring apps to report when they're using your camera, when they're doing different things, and each time you go to do something, you have the option to give permission or not. Facebook has been fighting this, but I see now that they've said, "Oh, well, we're going to have to do this." Now it's actually saying what they do with the information. I'll read it to you. They try to go with the plus side, and they say, "You're going to get ads that are more personalized.

Help keep Facebook free of charge, meaning we don't want to have you actually pay for the service. We want to just sell your information and support businesses that rely on ads to reach their customers." In other words, businesses that want to know that I went to California last year and I shopped at a certain store, they want to sell them that information. It's interesting, this popped up just as I'm talking about this. What this does is it's going to force people to see how much of the information is out there. The minute I clicked on the continue button, the first question is allow Facebook to track your activity across other companies, apps, and websites.

Let's think about what that is saying. As I use other apps, as I travel to different places, as I go on websites, on my phone, allow Facebook to track all of that. That's kind of scary. Now if I go in, and I try to find where the privacy settings are, I'm clicking, and I know you can't see it clearly but I'm clicking quite a bit and not finding it until I get to the bottom, Settings, and Privacy. I click that, and it's a list that's going to become a list that becomes a list. I really never ever get to what it has heard, what it has done. As you can see, the lists get more complicated. They get deeper and deeper.

I never actually see, and the reason why is because it's everything. I have to go into GPS or Maps to see that it's actually tracking everywhere I walk in my house, everywhere I walk outside. It's not easy. Sorry, Susan, I can't easily answer your question because they purposely make it hard for you to see and control that information. If we go back to the slides and go to the next one. To sum it up, smart speakers really don't have the memory to record all of your conversations. Times that it does record a conversation is because you literally told it to. For example, there is a skill I can use on a smart speaker called a 'send a message.'

For that to kick in, there are a lot of steps leading up to it. I have to say, "Send a message to a person that's in my contact list." It'll say, "Well, what's the message?" That is the moment when it starts recording. It's more than just a sentence. It's going to keep recording as much as it can, which might be pretty much a short paragraph, and then it will say, "Ready to send," and it goes away. At that point, it's not recording anymore. The reason it goes through those steps is it has to reserve the space, and then as I speak, it starts shooting the information immediately, instead of storing it locally. That's not easy for the speaker to do, and that's why it tries to grab what it can and it sends it out immediately.

Once again, going back to computers and phones, they have tons of memory. Depending on the app, they can start recording and working. I use sometimes a recording app to take

notes when I'm in meetings. One time, I forgot, I left it on, and when I realized that it, it had recorded everything I had done and said for two hours. Kind of scary in some ways that it didn't warn me and there wasn't anything blinking on the screen to let me know it was still running. We go to the next slide. I spoke about Facebook, and I spoke about Google, in general. At the end of the day, they don't have to use a smart speaker to spy on you.

No one has to spy on you because we freely give up the information. Imagine the uproar if one day Facebook said you have to pay $1 a day to use our service. A company that large making that much money has to get their money somewhere, and they get it by selling you. The government doesn't have to go through a lot of tricks to get your information. We just give it away freely on Facebook, everything, from what we ate in the morning, and even a picture of it, to where we've traveled. Google Maps knows everywhere you've gone. Instagram has people's entire life stories on there.

When you go into browsers, browsers are collecting information on you, and they're collecting information for the sites you go to, especially if you give them permission to do it.

If you use various banking services, or you link banking services, so let's say Amazon, and under Amazon, you link a credit card, the two companies begin to share information about your spending. If we go back to the concerns of it's spying on me, you don't have to spy if someone's going to open the keys, let you walk into their house, and go through every drawer in the house. That's pretty much what we do every day when we use Facebook and Google.

Every time we use Zoom, we trust when we stop the Zoom call that the camera is off. Now, some of us are paranoid. Some of us actually close it. I'm a paranoid type of person. Sometimes I'll check and see if it's still running in the background. For the most part, a lot of us would end the call and walk away from our computer and trust that Zoom isn't listening to us. We go to the next slide. All of this becomes about trust. We go through our day with probably a thousand different apps, where we're putting trust in people we don't know at all.

When we cross the street, we're trusting that the person is going to stop their car. When we do a bank transaction, we're trusting that this person, or a company, is holding our entire life savings, and when we ask for it, they're going to give it to us. Credit services, we trust that they are not going to turn around and charge us for something we didn’t buy, and the person that's having the credit card is trusting that this company is going to cover the costs until you pay them. When we have keys copied by our locksmith, we trust that that locksmith didn't make a copy of the keys so he could sneak into your home later and rob from you.

That's happened quite a bit. Going back even to the 1800s, there's a very famous politician who was a side locksmith, and that's how he got information. He copied the keys and went into people's homes and got information. We put little cable boxes inside of our homes all over the place, and now many of them have the capability to listen. Looking at everything and looking at the big picture, smart speakers generate more fear, is what I've seen, but everything in the world at this point, if you really start breaking it down, will generate much more fear.

Finally, to answer the question, are they spying? They don't have to. They really don't have to. We're pretty much giving them everything. At that point, I will stop here and take questions.

Susan: Let us do one quick poll before you take questions. Susie, do you want to bring up that poll? If you're concerned that you might say the wake word when you don't want to, what can you do to make sure your smart speaker isn't listening and or watching you, turn on the mute button for the microphone, unplug the device, and or switch the toggle button to close the camera shutter? When everyone has finished doing that, we'll bring those up as a nice conclusion. Susie, pretty much the voting finished?

Susie: People are still clicking away.

Susan: What?

Susie: I'm going to give it just another minute. Looks like it's slowing down. Okay, going to end it.

Susan: All right. If you're concerned that you might save the wake word when you don't want to, what can you do to make sure your smart speaker isn't listening and or watching? 75% of you said, "Turn on the mute button for the microphone." 31% of you said, "Unplug the device." 13% of you said, "Switch the toggle button to close the camera shutter." I believe Kirby, all of those answers are true.

Kirby: Yes, that's correct.

Susan: You could click on all of those, and that's how, if you're concerned, like some of us are, that you might say, the wake word, you can do all three of those. Just before I turn this over to Kirby to answer questions, we have one more announcement to make, and that is, we definitely want to thank you for joining us in today's webinar. You will receive a survey from the Pennsylvania Developmental Disabilities Council at the end of this webinar, and we would really appreciate it if you answer that survey. It's a really quick survey that goes straight to the DD Council, it helps them know who attends these webinars, what your interest is, are you a person with a disability?

Are you supporting someone with a disability? Are you a family member? Thank you very much. I also really want to thank Kirby for your presentation. Let me turn it over to you, Kirby, and you can answer whatever questions. Tracy is also put in the chat room, the chat space, that the slides and the recording, and they're fully accessible, will be up next week on this website. For those of you who would like to have a copy, please visit in another week or you can also email us and we can send you the link, you can send all questions to Kirby. Kirby, take it away.

Kirby: Okay. Let's see, what are some of the questions we've gotten. I'll tell you what if you guys don't mind reading them or calling them out.

Susan: All right, so far, we answered the one question about the phone and I'm not seeing any other questions at the moment. What you have on your slide is if you'd like more information about smart home devices and how to install them, you can go to Kirby at

info@sunkirb.com or the next slide, you can go to PATF, and either email us at patf@patf.us or go to SmartHomesMadeSimple.org.

There you will find a lot of information about smart home technology. Look at our dictionary, read our blog, various blog articles in which Kirby has already written something about security. I guess if anyone has any other questions, please put them in the chat or the Q&A. Otherwise, we thank you very much for attending today's webinar, and thank you, Kirby, very much.

Kirby: Thank you. [chuckles]

Susan: All right. I don't see any, oh, here's one real quickly. Becky is thanking us. Becky's from Banking and Securities, and I am sure that they get questions all the time about security. Becky does a wonderful job of doing presentations around financial education and did a webinar for us, as Money Talks about scams and identity theft. All right. Well, everyone. Thank you so much for attending. Let's see, here's George, who's also saying thank you, Kirby, for expanding on the answer. The question I'd asked at the first smart homes meeting about security. Yes, George, that's the reason for this webinar, that you did ask that question about security and smart speakers, so thank you very much.

Everyone, I hope you have a great afternoon. We are going to have another webinar at the very end of June. We will send this information out. It's going to be Kirby and Jeremy Boothe who's going to talk about assessments and how do you think about putting together a smart home for yourself and what are some of the assessment tools. We will be sending out information about that, so stay tuned. We hope you will join us. Once again, thank you for joining us today. Bye-bye.

Kirby: Bye.

[00:45:13] [END OF AUDIO]