Unwrapping **Smart Speakers**

Payments Innovation Alliance®

December 2021

Best Practices: Consumer Education

When it comes to gift giving, smart speakers are one of the top sellers. Market research company Omdia estimates that 154 million smart speakers were sold in 2020, a 58% increase over 2019 sales – and 2021 promises to be another record year. It is estimated that there are more than 160 brands of smart speakers available on the global consumer electronics market.

Smart speakers provide the ability to allow voice interaction to access entertainment, shopping news, weather, financial services, and more. Smart speakers are incredibly convenient because they actively listen for their "wake word." However, smart speakers can create multiple points of vulnerability in your home, leaving you open to cyberthreats and unwanted data sharing.

Here are some simple steps you can take to protect your privacy and keep you safe.

Be aware of who is around you.

Anyone within earshot can hear what you and the smart speaker say. Don't speak any sensitive information such as credit card numbers, passwords, or any other personal data you would not share with other family members or strangers.

Mute your microphone when you don't want to be heard.

Some devices show an indicator light when recording. Be sure you know where it is and how to mute the microphone.

Activate and train your speaker for voice recognition.

Some smart speakers can record a "voice fingerprint" so only you can activate the device.

Consider using a different network for your devices.

By separating your smart speaker from your home internet connection, you can reduce the points of vulnerability in your residence.

Use secure passwords.

Set up a password that is at least 8-to-12 characters, uses symbols and numbers, and is generally difficult to guess.

Carefully review data the device uses.

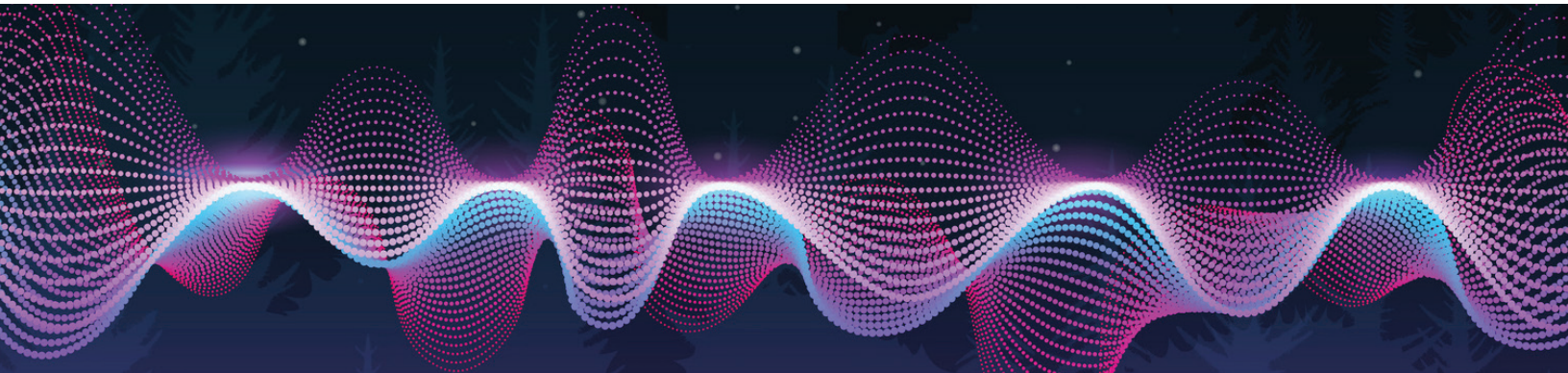
It may be convenient for your smart speaker to have access to your calendar, contacts and other data, however such access could create additional vulnerabilities unknowingly. Consider deactivating the settings that access your personal data and add only those that are appropriate.

Use two-factor authentication.

When someone uses your smart speaker, a code will be sent to you to authorize the use of your device.

Unplug your speaker when you are not home.

This is a simple way to make sure you stay secure when no one is around.



Changing the Default Settings on Your Smart Speaker

It is important to change the default settings on your smart speaker so you – and not the manufacturer – can control how to store and use your data. Here are some useful tips for being a smart user of products from Amazon and Google, which have the largest U.S. share of the smart speaker market.

Amazon Smart Speakers

By default, Amazon's Echo and other Alexa-enabled devices collect your personal information. You must change the settings for these devices and make an affirmative choice to opt out of surveillance. You must be logged into your Amazon account to make these changes.

To delete past Alexa recordings stored on the Amazon cloud

- Go to the Alexa privacy settings page.
- Select the "Privacy Settings" tab on the top center of the page.
- Under "View, hear, and delete your voice recordings," select "Review voice recordings."
- Where it says "Today," hit the drop-down menu and select "All History."
- Select "Delete all of my recordings."

For Amazon to stop saving the recordings of your voice interactions with Alexa

- Go to the Alexa privacy settings page.
- Select the "Privacy Settings" tab on the top center of the page.
- Under "Review and manage smart home devices history," select "Manage Your Alexa Data."
- Under "Choose how long to save recordings," select "Don't save recordings," then hit "Continue."

For Amazon to not to share your audio with humans

- Go to the Alexa privacy settings page.
- Select the "Privacy Settings" tab in the top center of the page.
- Select "Manage how you help improve Alexa."
- Under "Help improve Alexa," deselect "Use of voice recordings."

Google Smart Speakers

By default, Google Home does not store voice data on Google servers unless an account holder chooses to turn it on. To make these changes, access the history page or open the Google Home app and navigate to "My Activity."

To delete past Google Home voice recordings stored in the Google cloud

- Filter on Google Assistant/Voice and Audio Activity, if needed.
- Delete individual voice recordings by pressing on the three dots and clicking "Delete."
- To delete a specific range of activity, use the appropriate date and time filters.
- To automatically configure Google Home to auto-delete activity older than three, 18 or 36 months, select the "Auto-delete" option under the "Web & App Activity" banner.

For Google Home to stop saving the recordings of your voice interactions when the recording option may have been turned on previously

- Tap "Web & App Activity."
- Uncheck the "Include audio recordings" option.

This guidance was developed by the Conversational Payments Project Team of Nacha's Payments Innovation Alliance. To see more resources developed by the team, visit **www.nacha.org/alliance-download-conversational-payments-resources.**

About the Payments Innovation Alliance

The Payments Innovation Alliance is a 200-plus membership organization that brings together diverse, global stakeholders to support payments innovation. Through collaboration, discussion, debate, education, networking and special projects, the Alliance seeks to grow and advance payments and payments technology to better meet and serve the needs of the evolving industry.

For more information about the Alliance or the Conversational Payments Project Team, contact Jennifer West at **jwest@nacha.org**. If you are interested in Alliance membership, **click here**.