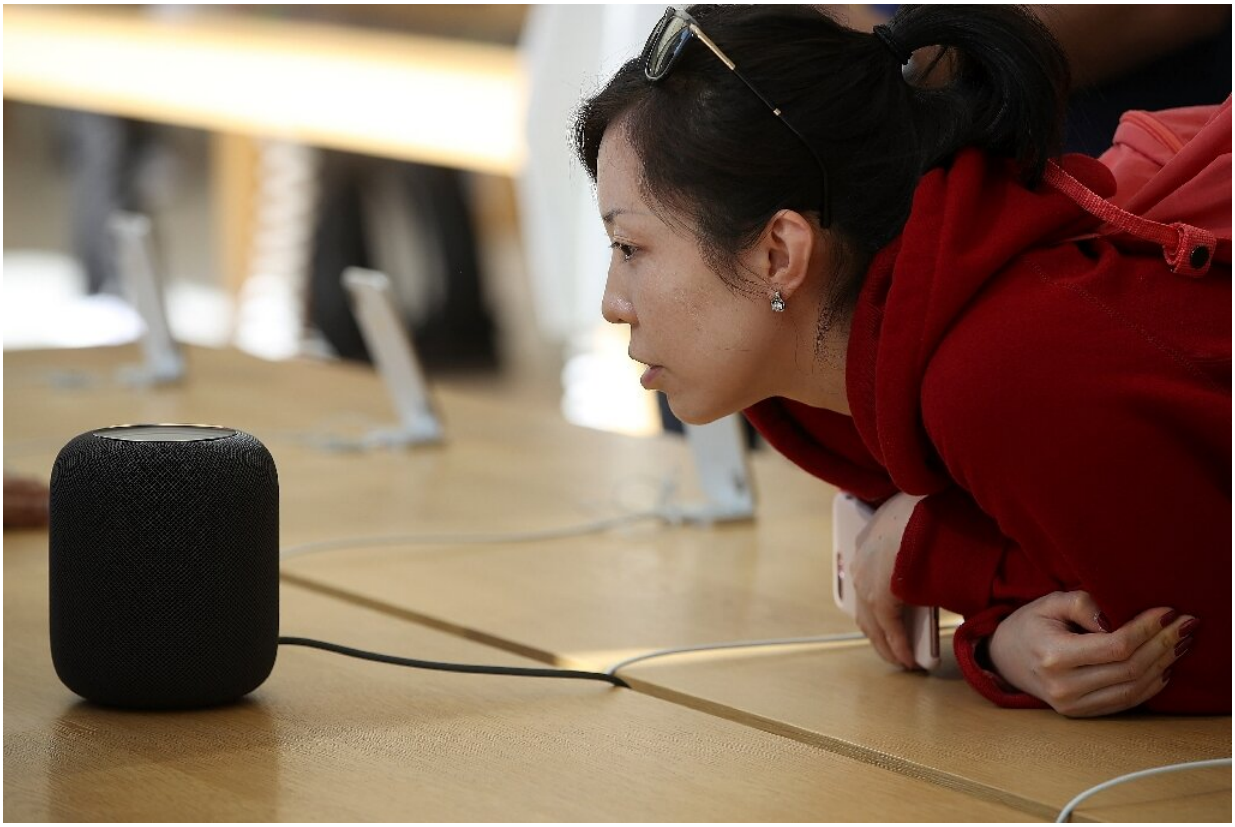
Privacy missteps cast cloud over digital assistants

August 3 2019, by Rob Lever



Concerns over privacy and data protection could cloud the outlook for digital assistants which are built into devices like the Apple HomePod

A series of privacy missteps in recent months has raised fresh concerns over the future of voice-controlled digital assistants, a growing market

seen by some as the next frontier in computing.

Recent incidents involving Google, Apple and Amazon devices underscore that despite strong growth in the market for smart speakers and devices, more work is needed to reassure consumers that their data is protected when they use the technology.

Apple this week said it was suspending its "Siri grading" program, in which people listen to snippets of conversations to improve the voice recognition technology, after the British-based Guardian newspaper reported that the contractors were hearing confidential medical information, criminal dealings and even sexual encounters.

"We are committed to delivering a great Siri experience while protecting user privacy," Apple said in a statement, adding that it would allow consumers to opt into this feature in a future software update.

Google meanwhile said it would pause listening to and transcribing conversations in the European Union from its Google Assistant in the wake of a privacy investigation in Germany.

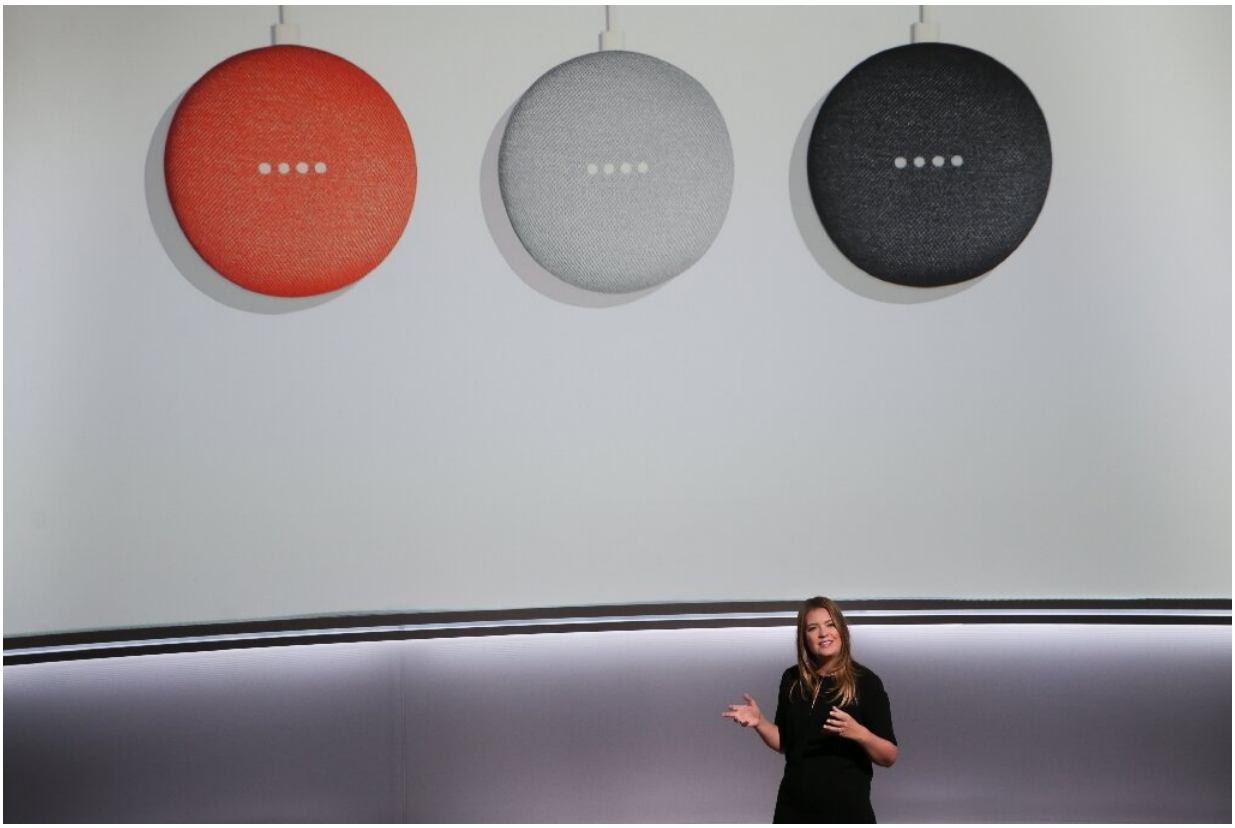
Amazon, which also has acknowledged it uses human assistants to improve the artificial intelligence of its Alexa-powered devices, recently announced a new feature making it easier to delete all recorded data.

The recent cases may give consumers the impression that someone is "listening" to their conversations even if it's rarely true.

"From a technology perspective it's not surprising that these companies use humans to annotate this data, because the machine is not good enough to understand everything," said Florian Schaub, a University of Michigan professor specializing in human-computer interaction who has done research on digital assistants.

"The problem is that people are not expecting it and it is not transparently communicated."

Carolina Milanesi, a technology analyst with Creative Strategies, agreed that humans are needed to improve the technology.



Many consumers express concerns about what happens to their data when they say "Hey Google"

"People have a somewhat unrealistic expectation that these assistants will by magic just get better eventually, that they can do machine learning and get better on their own, but right now we're still at the beginning of AI, and human intervention is still important," she said.

According to the research firm eMarketer, nearly 112 million people—one-third of the US population—will use a voice assistant at least monthly on any device, with many using AI-powered devices for searches, music and news or information.

A Microsoft survey this year of consumers in five countries found that 80 percent were satisfied with their experience with digital assistants. But 41 percent of those surveyed said they had concerns on privacy, trust and passive listening.

Unfounded fears?

Some of the privacy fears surrounding smart speakers are based on false assumptions, analysts note.

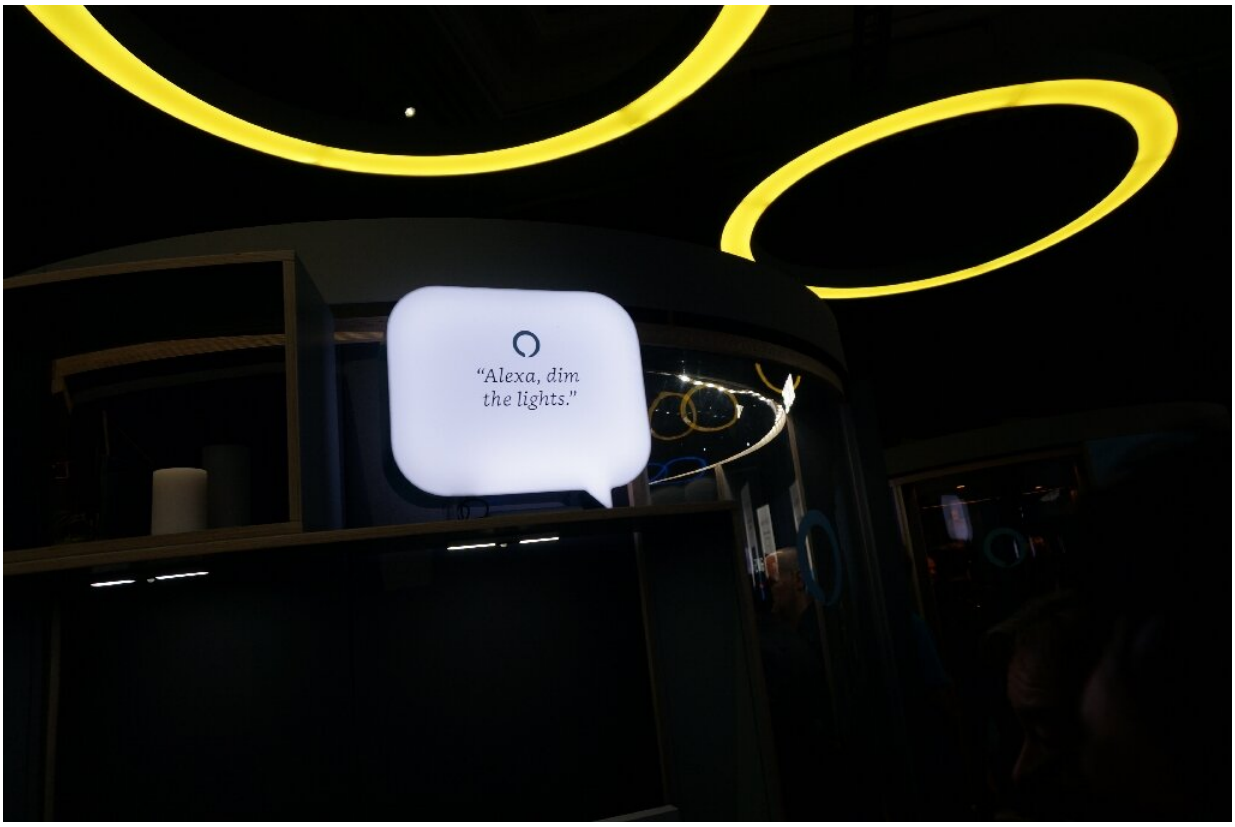
The devices don't record or transmit information until they are "activated" with a keyword or phrase such as "Hey, Siri" or "Alexa."

But "there is always a risk of false activation," Schaub noted.

"You have to trust the device and the company making the device that the microphone is only locally processing until the activation word is heard."

Ryan Calo, faculty co-director of the University of Washington Tech Policy Lab, said that while the devices are not listening, there remain concerns over access to conversations.

"If employees are hearing things they shouldn't have access to, that is really a red flag, it's a bad practice," Calo said.



Amazon showcased its Alexa digital assistant at the 2019 Consumer Electronics Show for smart speakers and other devices

Boiling the frog

Calo said the privacy concerns around digital assistants are likely to grow as the devices expand their capabilities.

"I worry about a trend where these systems begin to listen for more than just your affirmative command—it could listen for breaking glass or signs of distress, or a baby crying. All of a sudden the system is listening for all kinds of things and the frog gets boiled by incrementally heating the water," he said.

Calo also expressed concern that devices may be turned on remotely, a potential threat to civil liberties.

"If law enforcement gets a warrant, it could turn your Echo into a listening device," he said.

Schaub said consumers are also concerned that data from the devices may be used for ad targeting.

"People want these benefits but without allowing their data to be used against them," he said.

Still, the allure of digital assistants will mean the market is likely to keep growing.

Schaub said one way to reassure consumers would be to build privacy features directly into voice commands so users can understand how their data is used and make better choices.

"Companies should see this as an opportunity to engage with customers about how they are protecting them," he said.