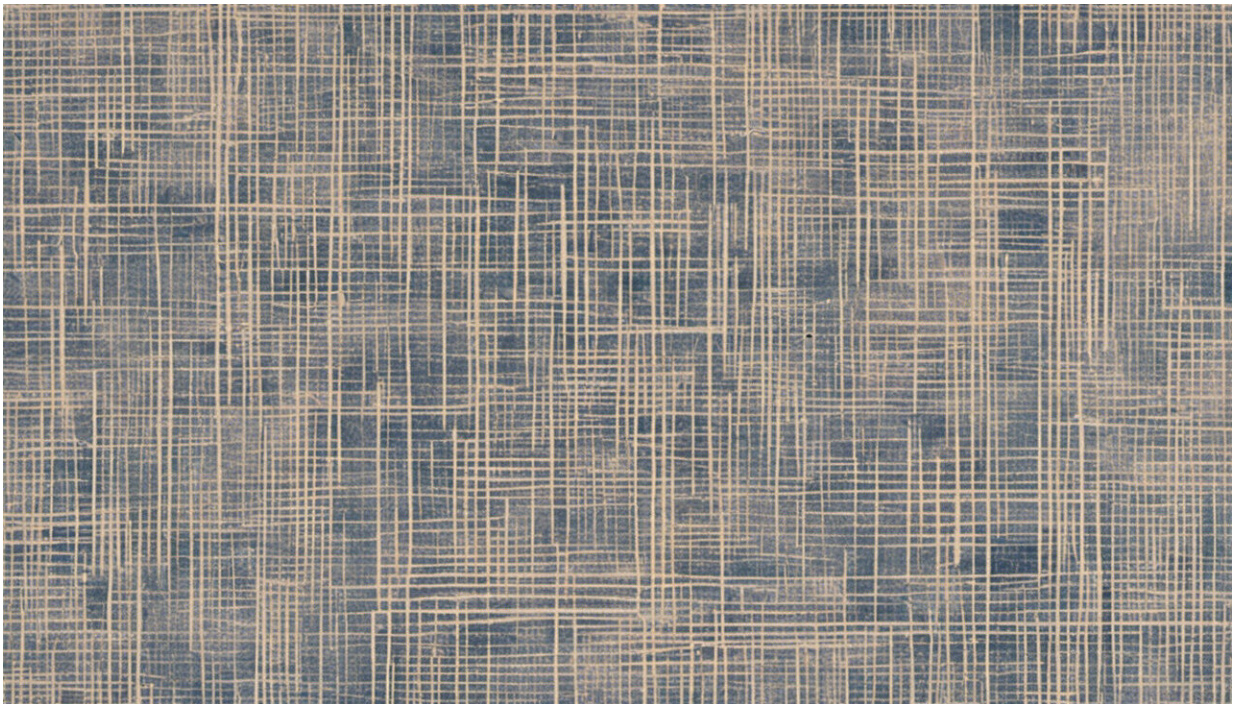


Do I want an always-on digital assistant listening in all the time?

July 16 2018, by Heather Woods



Credit: AI-generated image ([disclaimer](#))

The smart device market is [exploding](#). Smart home kits for retrofitting "non-smart" houses have [become cheaper](#). Earlier this year, Apple released the [HomePod speaker](#), the company's response to dominant smart devices [Google Home](#) and [Amazon Echo](#). Amazon, too, is expanding its lineup. Recently, it debuted the [Amazon Echo Look](#),

promising to make users more stylish.

All of these smart devices are equipped with an artificially intelligent virtual assistant, which allows users to interact with their devices hands-free. These devices, which vow to make your life easier, have another thing in common: They often have [microphones on all the time](#) to listen for your requests.

As a [scholar of rhetoric and technology](#), I study how [people](#) make sense of new technological innovations. [My research](#) outlines several reasons why people might find these smart devices equipped with an always-on microphone attractive as well as unsettling.

Convenience matters

First, smart devices offer exceptional convenience at an unprecedentedly low cost. Amazon, Apple, Microsoft and Google all pitch their products as ways to make users more efficient by outsourcing tasks. This isn't new. Wealthier people have long relied on the labor of others to manage their households and workspaces. Smart home technologies promise similar effects. They can automate chores, including [vacuuming](#), [grocery shopping](#) and [even cooking](#).

Artificial intelligence, algorithms and automation now execute tasks for those who can afford smart devices. As a result, more and different people may take advantage of a digital assistant than would use, or could afford, a human assistant.

Increasing autonomy

For example, hands-free technologies may increase autonomy for the elderly and individuals with disabilities. Scholars are investigating how

smart devices can support "universal design," a way of making spaces and activities [accessible and convenient for people of all abilities](#). Smart home systems can assist people with physical or cognitive impairments by automating crucial activities and services, such as opening and closing doors, or contacting medical professionals.

Such systems may offer people increased autonomy in their homes. For instance, in Boulder, Colorado, [Imagine! Smart Homes](#) are equipped with [smart home systems](#) so that people with cognitive disabilities "may remain in more independent and natural settings." [Interviews with elderly users](#) suggest that technologies that monitor a person's health and movement around the home can help people "[aging-in-place](#)."

Ubiquitous surveillance and security concerns

While [smart home technologies](#) can offer feelings of comfort and security for some users, there may also be security risks associated with an always-on microphone.

Smart home systems are part of a larger suite of devices, apps, websites and spaces that collect, aggregate and analyze personal data about users. Scholars call this "ubiquitous surveillance," which means "it becomes [increasingly difficult to escape](#) ... data collection, storage, and sorting."

Smart devices require data – yours and others' – to serve you well. To get the full benefits of [smart home](#) systems, users must share their locations, routines, tastes in music, shopping history and so forth. On one hand, a well-connected device can manage your digital life quite well.

On the other hand, providing so much [personal information](#) benefits companies like Amazon. As they [gain access to users' personal information](#), they may monetize it in the form of targeted advertisements or collect and sell your personal characteristics, even if it's [separated](#)

from your [name or address](#). Perhaps that's why Wired magazine says, "[Amazon's Next Big Business Is Selling You](#)." Not all companies have the same privacy policies. Apple says it [won't sell its users'](#) personal information to others. Still, potential users should decide how much of their intimate lives they're willing to share.

Smart homes come with broader [security concerns](#). Unsecured devices connected to the "internet of things" can be targets for hackers. Access to smart devices might provide hackers a well-spring of useful data, including information about when users are home – or not. Additionally, smart objects can be deployed surreptitiously for nefarious purposes. In 2016, the [Mirai botnet](#) commandeered unsuspecting users' [IoT devices for use in a distributed denial-of-service attack](#).

There's another, perhaps less exciting, risk: Devices with always-on microphones can't always tell who is talking. Recently, Alexa users reported that their [children ordered unwanted items from Amazon](#). Others noted that background sounds, [like the TV](#), prompted unauthorized purchases. These vocal triggers – called "false positives" when they prompt devices to do something unexpected or unwanted – have led to users [unknowingly sharing private conversations](#) with others.

In early 2018, Amazon Echo users were forced to confront these security risks when Alexa began [laughing, apparently unprompted](#). Although [Amazon later said](#) that the laugh was an unfortunate false positive response to nearby conversations, the [laughter prompted some users to reconsider](#) letting Alexa into their most intimate spaces.

Objects like people

Potential surveillance and security concerns aside, users must consider the consequences of human-like virtual assistants in smart devices. It is not a coincidence that Siri, Alexa, Cortana and now [Erica, Bank of](#)

[America's digital assistant](#), are gendered feminine – and not just their voices. Historically, women were assigned to tasks related to their roles as mother or wife. As women joined the workforce, they continued to perform these roles in "[pink collar](#) jobs."

Siri and Alexa perform similar tasks, [taking care of users](#) while also offering [administrative support](#). Some even consider Alexa to [be a co-parent](#).

My [research shows](#) that gendering virtual assistants invites users to engage with [smart devices](#) because they're familiar and comfortable. Some users may be willing to share more intimate details about themselves despite security or surveillance risks. Ultimately, people may grow [to rely upon devices](#), which empowers those who own the data harvested from always-on devices in the home.

Smart device [users](#) must weigh the significant conveniences of a [device](#) with an always-on microphone against the substantial concerns. Some of these concerns – security and surveillance – are pragmatic. Others – about whether devices should have a gender – are decidedly more philosophical. The bottom line is this: When people ask devices to act for them, they must be willing to live with what – or who – is on the other side.

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation

Citation: Do I want an always-on digital assistant listening in all the time? (2018, July 16) retrieved 26 April 2024 from <https://phys.org/news/2018-07-always-on-digital.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.