Smart speakers are everywhere—and they're listening to more than you think

March 27 2019, by James Parker

Credit: Dani Hart from Pexels

Smart speakers equipped with digital voice assistants such as Siri and Alexa are now the fastest-growing consumer technology since the smartphone.

Nearly 100 million were [sold](#) in 2018 alone, a [threefold](#) increase on the year before. And nowhere is this growth faster than in Australia.

But we should be concerned about what these smart speakers are actually listening to. It's more than just our voice commands to play a piece or music or turn down the lights.

We need to think carefully about where this sort of technology is heading. Very soon it won't just be our smart speakers listening, but all manner of other devices too.

Security systems that listen for the sound of gunshots or broken glass, CCTV cameras outfitted with microphones, auditory surveillance at work, and a growing range of other devices are all cause for concern.

Rapid take up

By the end of 2018 the percentage of Australian adults with a smart speaker had risen from zero to 29% in only 18 months, according to the [Australia Smart Speaker Consumer Adoption Report](#) released this month. The report was joint work of tech news site and [Voicebot](#) and digital consultants [FIRST](#).

Based on a survey of 654 Australians, the report estimates that some 5.7 million Australians now own smart speakers out of a total adult population of around 19.3 million.

The Australian user base relative to population now exceeds that of the US (26%), despite the devices being available here for less than half the time.

If the upward trend continues – Deloitte [expects](#) the market to be worth at least US$7 billion in 2019, up 63% on 2018 – smart speakers will

soon be even more common.

They're already in our homes and [workplaces](#), [hotels](#), [hospitals](#) and [universities](#).

We are also getting increasingly comfortable talking to our technology, according to the consumer adoption report: "Over 43% of Australian smart speaker owners say that since acquiring the devices they are using voice assistants more frequently on smartphones."

We are no longer surprised to find we can talk to our phones, [cars](#), televisions, watches, even our [Barbie dolls](#), and expect a response.

What about privacy?

But the recent consumer report also says Australians worry about such speakers. Nearly two-thirds of people surveyed say they had some level of concern over the privacy risks posed by smart [speaker](#) technology – 17.7% said they were "very concerned".

The report doesn't specify what those concerns are. Perhaps we are concerned about recordings of our conversations being [emailed to colleagues](#) without our knowledge or consent, or admitted as [evidence](#) in court.

But I believe we are much less concerned than we should be about where this industry is headed next. Smart speakers aren't just listening to *what* we say. Increasingly, they are also listening to *how* and *where* we say it.

They're listening to our vocal biometrics, to how we stutter and pause, to our tone of voice, accent and mood, to our state of wellness, to the size and shape of the room we're sitting in, and to the ambient noises, music and TV shows on in the background. All for the purpose of extracting

more and more data about who we are and what kinds of things we do.

Who's listening?

Even more importantly, though, the rapid rise smart speakers heralds the coming era of machine listening, where we can expect all manner of networked devices to be listening to, processing and responding autonomously to our auditory environments: listening for both sound and speech, with and without our consent, virtually all the time.

[Audio Analytic](link), one of the more prominent companies in this area, states on its website: "We are on a mission to give all machines a sense of hearing […]"

This is much less far-fetched than it sounds. Audio Analytic's flagship software, [ai3TM](link), claims to be able to recognise "a large number of audio events and acoustic scenes", with a view to enabling devices to understand and respond to sonic environments in their own right.

Already, this [includes](link) headphones that know when someone is talking to you and can tweak the volume accordingly; cars that autonomously adjust to the sound of horns blaring; [security systems](link) able to identify the sound of arguments brewing, windows shattering, as well as other acoustic anomalies. Systems can then either respond autonomously or notify the relevant authorities.

Another company, [Shooter Detection Systems](link), sells technology for the autonomous detection of active shooter situations including gun shots. Its so-called Guardian System can quickly pinpoint the location of any gunshot and issue alerts.

In a similar but even more troubling vein, [AC Global Risk](link), [reportedly claims](link) to be able to determine potential risk level of someone with

greater than 97% accuracy simply by analysing the "characteristics" of few minutes of their speaking voice.

Walmart [recently patented](#) a new employee performance metric based on algorithmic analysis of audio data (employee speech patterns, the rustling of bags, sounds from carts, footsteps and so on) gathered from microphones installed at terminals and other locations throughout its stores.

In 2017, Moreton Bay regional council in Queensland introduced always-on listening devices to [330 CCTV cameras](#) throughout its council area, a move the [mayor said](#) was to help police fight crime. The council says it deactivated the listening devices later that year after concerns were raised.

Sound the warning

Each of these examples raises complex questions of ethics, law and policy.

The kinds of questions we have recently begun asking about all AI – about the possibilities of algorithmic overreach, bias, profiling, discrimination and surveillance – all need to be asked of smart speakers too.

But it is also important to understand the ways in which [smart speakers](#) are connected to a much broader field of machine listening and auditory surveillance that many are rightly worried about.

Machine listening isn't just coming, it's already here and it demands our attention.

This article is republished from [The Conversation](#) under a Creative

Commons license. Read the [original article](.).

Provided by The Conversation