

Industry Watch: *The pros and cons of listening devices*

ROBERT DALE

Language Technology Group
e-mail: rdale@language-technology.com

(Received 30 August 2017; first published online 25 September 2017)

Abstract

Vastly improved speech recognition, backed by a more slowly improving ability to make sense of the recognized speech, has brought state-of-the-art NLP into our homes in the form of smart speakers and other devices that listen. There's no doubt these devices can be incredibly useful, but they also may also support incursions into our privacy. We look at where we are today, consider what might be coming, and express just a tad of caution.

Say hello to a new housemate

You will have noticed that the battle for the living room is well under way. It's looking to be the big money fight of the decade. In one corner, we have the Amazon Echo, slightly reminiscent of the black monolith from Kubrick's 2001, or perhaps looking more like a deluxe Pringles can. In the opposite corner, we have Google Home, whose similarity to an air freshener has been noted by many. Each wants to be the favoured house guest, and there's a lot at stake.

In my house, opposite corners of the lounge room are indeed where we've chosen to locate our two fledgling AI cohabitants—being suckers for gadgets, we're amongst the 8 per cent of smart speaker owners who have hedged their bets by accommodating an instance of each.¹ I'm not quite sure why we've physically separated them in this way, allocating them separate territories as if they were two cats forced to tolerate living together. A suspicion they might get into an argument if they were too closely co-located, perhaps? Or an anthropomorphic sentiment that they each deserve their own space? Or maybe just that they don't look that good sitting next to each other.

Of course there are other embodied intelligent assistants knocking at the door. Harman Kardon's Cortana-powered Invoke is due in the United States in the fall, and may be available by the time you read this.² Apple's HomePod is due at the end

¹ <https://www.voicebot.ai/2017/06/23/amazon-alexa-82-percent-smart-speaker-market-share/>

² <http://www.harmankardon.com/invoke.html>

of the year.³ Samsung is said to be working on a smart speaker driven by Bixby, a virtual assistant whose first appearance on smart phones received a fair bit of criticism.⁴ There will be others. But right now, the focus of attention is on Google versus Amazon.

Each of the contenders for being your resident AI has a different ecosystem that it fits into. If you make use of any of Google's services, Google knows a great deal about you—it's worth periodically checking out myactivity.google.com or www.google.com/maps/timeline to remind yourself—and is well placed to leverage the knowledge implicit in that data. The Echo knows your Amazon purchase history, and not surprisingly a key part of the game plan there is to make it incredibly easy to go voice shopping for more stuff at The Store That Has Everything (one-grunt ordering?). Traditionally Google has made money from you via targeted advertising, but in a sign that it too wants a cut of your shopping dollars, the company has just announced a partnership with Walmart, positioning itself for head-on competition with Amazon.⁵

Mom, there's a salesperson in the kitchen

I doubt that many people select which smart speaker to buy based on appearance alone. You could choose based on capabilities, and right now the Echo seems to be the clear winner here, with 17,000 skills as compared to Google Home's 468 actions.⁶ But that difference is largely an artefact of Amazon's 16-month lead in entering the market, and is likely to be evened out over time, just as the Apple and Android app stores have grown to be roughly the same size.

Your choice of device is perhaps more likely to be influenced by which of the offerings is able to take advantage of what it knows about you to add value. There's a kind of self-perpetuating soft lock-in that we're already familiar with from alliances that tie together airline frequent flyer programs, gas station franchises and supermarket chains. Indeed, as the market here develops and matures, it's not entirely inconceivable that you might even choose your smart speaker based on your preferred grocery store.

When their makers deem that the time is right, you can be sure that these devices will start serving ads. Amazon has already dipped its toes in this water earlier in 2017, allowing six-to-ten second 'sponsored messages' to be played at start or end of an interaction with a skill.⁷ But shortly thereafter, they pulled back from this.⁸ I expect they will return before too long. At first these ads will be clearly marked

³ <http://www.techradar.com/news/homepod-release-date-news-and-features>

⁴ <https://www.cnbc.com/2017/08/23/samsung-working-on-smart-speaker-to-rival-amazon-echo-apple-homepod.html>

⁵ <https://www.nytimes.com/2017/08/23/technology/google-walmart-e-commerce-partnership.html>

⁶ <https://www.voicebot.ai/2017/08/02/google-assistant-apps-grow-24-percent-alexa-skills-pass-17-thousand-july>

⁷ <http://www.businessinsider.com/amazon-trials-voice-assistant-ads-2017-5>

⁸ <http://www.businessinsider.com/amazon-echo-shies-away-from-alexa-ads-2017-6>

as such, but, just as some newspapers carry advertorial content that can be hard to distinguish from independent news, the scope for ‘conversational advertising’ will inevitably blur the boundaries between our assistant just being its usual cheery and helpful self, and seeking out a commission via persuading us to buy a particular brand of pasta.

Amazon’s Echo Show adds a touch screen and camera to the basic smart speaker setup, resulting in a kind of iPad–Echo hybrid.⁹ Now that’s potentially really useful; a picture’s worth a thousand words, and I really want to see those socks before I buy them. And the same device that interactively steps you through a video of how to make a complicated dish can interrupt what it’s doing for some face-time with the kids. But it also enables a dynamic, personalised advertising billboard right there in your kitchen.

Hey Alexa, invite your friends over

Apart from weather updates and music streaming, a key potential of these devices that you hear a lot about is as controllers for the smart home: lock the door, dim the lights and turn the heating up with your voice.

Amazon and Google are falling over themselves to voice-enable all manner of devices. At the Consumer Electronics Show in January 2017, you could find Alexa integrations in Ford automobiles, robots, kitchen appliances and other brands of smart speakers.¹⁰ In July, Google had over 70 home automation partners and counting.¹¹

Samsung—which, as well as being first in worldwide smartphone market share, is also a massive white goods manufacturer—has indicated that, by 2020, all of its home appliance line-up will have smart features. The company is developing partners to expand voice to wearables, in-car systems and audio rigs.¹²

And of course Apple has HomeKit for Siri,¹³ although this seems a bit left out in the cold until the HomePod lands; it’s not so convenient to have to pull out my phone to switch on the heating.

The result of all this combination of voice interfaces and device integration: friction-free ubiquitous access to intelligent devices around the home. The gap between ‘future vision’ videos and what we have today has never been smaller.

But is this really such a good thing?

Take vacuum cleaners. Amongst the smart devices you can control with Google Assistant is LG’s new Hom-Bot Turbo+ robot vacuum cleaner.¹⁴ What’s interesting about the Hom-Bot is that it comes with six cameras, ‘to make navigating the home

⁹ <https://www.engadget.com/2017/06/26/amazon-echo-show-review/>

¹⁰ <https://www.theverge.com/ces/2017/1/4/14169550/amazon-alexa-so-many-things-at-ces-2017>

¹¹ <http://www.businessinsider.com/google-smart-home-ecosystem-partners-2017-7>

¹² <http://www.zdnet.com/article/samsung-to-apply-more-ai-voice-recognition-to-smart-home-line-up/>

¹³ <https://www.apple.com/ios/home/>

¹⁴ <https://www.psfk.com/2017/08/robot-vacuum-has-built-in-google-home-assistant.html>

easier and avoid getting stuck on objects or knocking them over'. But the cameras are also touted as having a security function: if the vacuum detects movement after the owner has left the house, it can record up to 100 minutes of video. Presumably it also has that capability when I'm still at home.

And newer Roombas are able to upload data about the layout of your home to the cloud.¹⁵ iRobot, the manufacturer, has indicated that it might sell that data to others, such as Amazon, Alphabet or Apple. Isn't it a bit of a worry that these things are wandering around your house looking in every nook and cranny?

Right now, we are assured that our data is safe and nothing will be done without our permission. But hang on, take a look at Google's terms and conditions; there's already a lot they can do with your data. And while these corporations might do no evil today, how can we be so sure that will be true into the future?

In 2015, it was revealed that Samsung smart TVs were sending unencrypted voice search data across the net.¹⁶ Earlier this year, Vizio, a TV manufacturer, was fined \$2.2M for tracking viewing habits and selling the data to advertisers.¹⁷ *Consumer Reports* was prompted to offer advice on how to stop your TV from snooping.¹⁸

Also in 2015, researchers found security flaws in Mattel's talking Hello Barbie doll that would allow a hacker to reuse its authorization credentials.¹⁹ And earlier this year, Germany's Federal Network Agency banned a doll called 'My Friend Cayla' on the grounds that it was an espionage device, transmitting everything it heard back to base.²⁰ In the wake of this, the FBI issued a privacy warning for Internet-connected toys.²¹ Long gone are the days when all a parent had to worry about was the ingestion of small pieces of plastic.

So what do you do? Some of the advice being offered is pretty extreme: Mark Pugh from iServPro suggests that 'When your device is on, it's your responsibility to remember not to say anything within earshot of it that you wouldn't say in public. Don't get too comfortable around it'.²²

Creeping creepiness

I remember the first time Google popped up a card on my phone to remind me, unsolicited, that my car was parked a certain distance away. I thought this was cute, but my partner found it creepy. As our smart devices work more and more together, I think we're going to have a lot of creepy moments. Do I really want my electric

¹⁵ <https://www.technologyreview.com/s/608344/your-roomba-is-also-gathering-data-about-the-layout-of-your-home/>

¹⁶ <https://www.theguardian.com/technology/2015/feb/19/samsung-smart-tvs-send-unencrypted-voice-recognition-data-across-internet>

¹⁷ <https://www.wired.com/2017/02/smart-tv-spying-vizio-settlement/>

¹⁸ <https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/>

¹⁹ <http://www.technewsworld.com/story/82842.html>

²⁰ http://www.huffingtonpost.com/entry/doll-records-children_us_5849c10ae4b0905b34427964

²¹ <https://www.ic3.gov/media/2017/170717.aspx>

²² <http://www.iservpro.com/2017/01/13/security-tips-now-amazon-echo-google-home/>

toothbrush to tell Alexa about my brushing habits so I can be better targeted for new dental care products?²³

It's not just that all these devices will be connected to each other. The fact that they are listening makes it infinitely harder for us to maintain an accurate mental model of what they know and what they don't know. Much is made of the fact that today's smart speakers only start recording when the wake words are heard. But this is a software-imposed limitation, and clearly the capabilities for always-on listening are there. We are simply trusting that the manufacturers will do the right thing. That might not be so comforting if you happen to live in an authoritarian state. And besides, there's always scope for hacking: *Wired* reported at the beginning of the year that a security researcher had succeeded in turning an Amazon Echo into an eavesdropping device.²⁴ Now, this particular hack required physical access; but should I believe that my internet-connected smart speaker is more secure than Iran's nuclear facilities?²⁵

I recall when CCTV cameras first started being installed in the United Kingdom in large numbers in the 1980s. Many people expressed concern about what was then seen as a gross invasion of privacy. Today, we are much more blasé about the divide between public and private; while there are still some who stick masking tape over their webcams just in case someone is snooping, there are many more who post pictures of the most intimate moments of their lives for all to see. As these smart devices become more and more integrated in all that we do at home, the boundaries become ever more fuzzy and hard to determine.

Like the frog that boils to death as the temperature of the water slowly increases, we have allowed our lives, and now our homes, to be step-by-step made accessible to third parties. It's easy to see why. Interacting with all these devices by voice is just massively convenient. But it comes with a price. From one angle, it looks like we are willingly installing and paying for the last mile of the infrastructure needed for the ultimate surveillance society. Just sayin'.

Let Cayla, the compromised doll we mentioned earlier, have the last words. In a YouTube video, Norway's Consumer Council's technical director Finn Myrstad asks Cayla, 'Can I trust you?'.²⁶ Cayla replies 'I don't know'.

²³ <http://connectedtoothbrush.com/>

²⁴ <https://www.wired.com/story/amazon-echo-wiretap-hack/>

²⁵ <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

²⁶ <https://www.youtube.com/watch?v=1A0j0H5c6Yc>