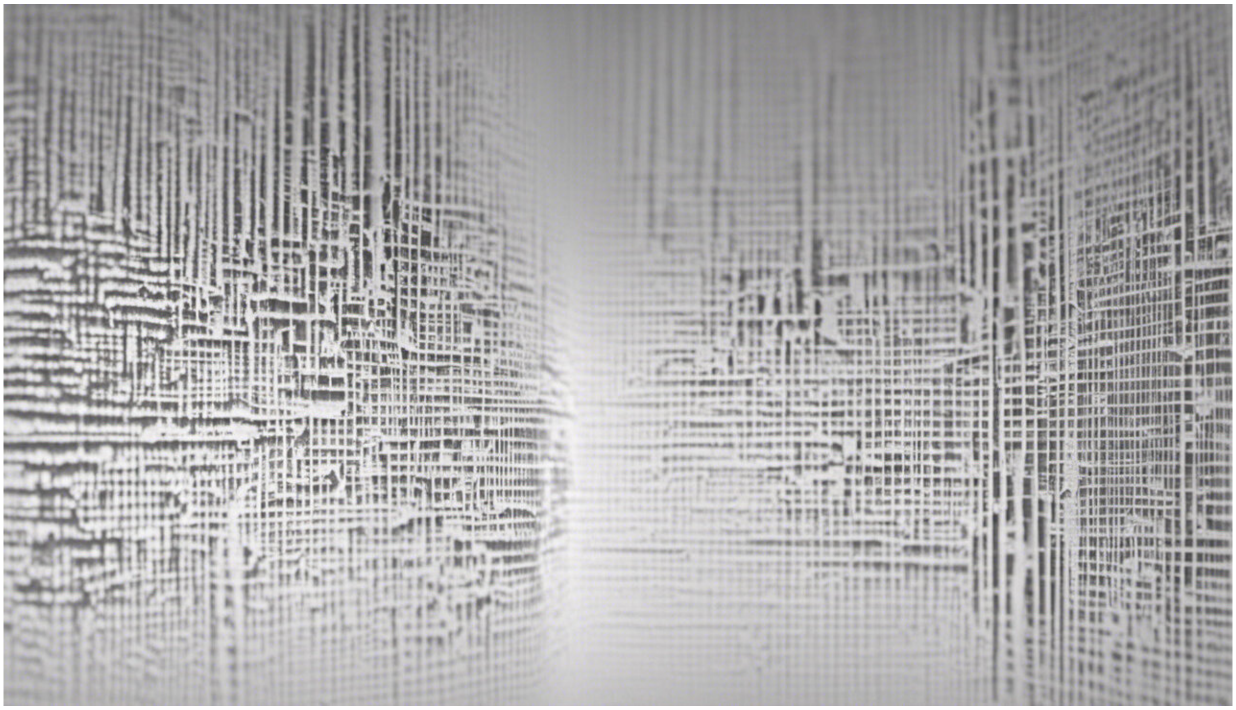
The dark side of Alexa, Siri and other personal digital assistants

December 16 2019, by Rozita Dara



Credit: AI-generated image (disclaimer)

A few short years ago, personal digital assistants like Amazon's Alexa, Apple's Siri and Google Assistant sounded futuristic. Now, the future is here and this future is embedded, augmented and ubiquitous.

Digital assistants can be found in your office, home, car, hotel, phone and many other places. They have recently undergone massive transformation and run on operating systems that are fueled by artificial intelligence (AI). They observe and collect data in real-time and have the capability to pull information from different sources such as smart devices and cloud services and put the information into context using AI to make sense of the situation. Although we have come a long way in the design and execution of these AI technologies, there is still more work to be done in this arena.

Much of the data that these digital assistants collect and use include personal, potentially identifiable and possibly sensitive information. Can Alexa or other personal digital assistants violate the privacy and security of our data? Possibly. There is a dark side to these virtual assistants.

My expertise is in data privacy, data governance and artificial intelligence. I was previously the Information and Privacy Officer with the Ontario Information and Privacy Commissioner's Office.

Welcoming service

Imagine the following situation.

You are expecting some guests over. Your first guest arrives, and the outdoor security camera on your porch captures her walking up to your home. A polite voice welcomes her and unlocks the door. Once she is inside, your digital assistant explains to your guest that you are on your way and will be home soon. Through your home audio system, your digital assistant plays a selection of your guest's favorite songs (from your Spotify friends network). Your digital assistant asks your guest if pumpkin spice is still her preferred coffee flavor or if she prefers other ones: french vanilla or Colombian. Soon after, your guest picks the coffee up from the digital coffee machine. Welcoming duties now complete, your digital assistant goes silent, and while waiting for you, your guest makes a few phone calls.

It is fascinating how a digital assistant can accurately and autonomously validate the identity of your guest, select her favorite songs, remember her preferred coffee flavor and manage the smart appliances in your house.

Hosting assistants

But does your digital assistant's behavior concern you?

Digital assistants can record our conversations, images and many other pieces of sensitive personal information, including location via our smartphones. They use our data for machine learning to improve themselves over time. Their software is developed and maintained by companies that are constantly thinking of new ways to collect and use our data.

Similar to other computer programs, the fundamental issue with these digital assistants is that they are vulnerable to technical and process failures. Digital assistants can also be hacked remotely, resulting in breaches of users' privacy.

For example, an Oregon couple had to unplug their Alexa device, Amazon's virtual assistant, as their private conversation was recorded and sent to one of their friends on their contact list.

In another incident, a German man accidentally received access to 1,700 Alexa audio files belonging to a complete stranger. The files revealed the person's name, habits, jobs and other sensitive information.

Awareness privilege

Increasing popularity and availability of personal digital assistants has resulted in a widening of the so-called digital divide. The interesting paradox is that individuals who are aware of and sensitive to issues of privacy typically limit their usage of digital tools, while users who are less prone to protect their privacy extensively incorporate personal assistants into their digital lives.

Digital assistants either record data continuously or wait for a word to "wake up" or become activated. They do not limit data collection to the owners' or authorized users' information. Personal digital assistants may collect and process unapproved users' personal data, like their voices.

In the digitally divided society, someone who is privacy savvy would not invite such equipment into their lives, while others may accept or rationalize such behaviors.

Respecting others' privacy

In this age of ubiquitous devices and internet access, how should we deal with this paradox and respect each others' space and choices?

Let's revisit our imaginary personal digital assistant. It had to process different sources of information about the guest to operate as a smart host. Did the digital assistant use all that data to feed the algorithms or to invade the guest's privacy? Depending on who you ask, the answer will be different.

Our etiquette-conscious upbringing tells us that we have a social and ethical responsibility to respect each others' values when it comes to digital technologies. But the implications and growth of these technologies have been so significant and rapid that we have not yet been able to redefine our social norms and expectations.

For instance, as a host, do we have an ethical obligation towards our guests to inform them about our personal digital assistant? Is it polite for a home visitor to ask the host to turn their digital tools off? Should we inquire about the presence of smart tools and digital assistants before arriving at a friend's house, a hotel or an AirBnB?

The answer to these questions is yes, according to etiquette expert Daniel Post Senning. Senning explains that etiquette is most powerful when you use it as a tool for self-assessment. Would we like to be informed that we are being recorded in a business meeting or a private gathering? Or how do we prefer to be asked to turn digital tools off if we are hosting? The etiquette rules are universal: to be considerate, honest and kind.

Inform your colleagues and guests that your digital devices may record their voices, images or other information. Ask your host to turn off digital assistants if you are not comfortable having them around. But be considerate. You may not want to ask your host to turn off digital assistants in the presence of somebody who is elderly or has a disability and depends on those tools.

Maintaining our collective privacy

Privacy is a social norm that we have to work together to maintain. First of all, we need to educate ourselves on cybersafety and potential risks of digital technologies. We should also be proactive in keeping current with the latest news on technologies and take actions when required.

The government's role in this complex paradigm is critical. We need stronger privacy laws to address privacy issues associated with personal digital assistants. Right now, companies such as Amazon, Google and Apple are making the rules.

Other jurisdictions have developed and implemented regulations such as

Europe's General Data Protection Regulation (GDPR) which provides oversight on data collection for a wide variety of household devices. Canada should follow suit.

Provided by The Conversation

Citation: The dark side of Alexa, Siri and other personal digital assistants (2019, December 16) retrieved 8 March 2024 from https://techxplore.com/news/2019-12-dark-side-alexa-siri-personal.html