European Data Protection Supervisor

TechDispatch

Smart speakers and Virtual Assistants

Issue 1 | July 2019

Ever since Alan Turing published his paper Computing Machinery and Intelligence in 1950, computer scientists have tried to get machines to mimic human behaviour and make them as *intelligent* or as *smart* as human beings, by having them play imitation games.

Turing raised the question: *Can machines think?* He suggested that something "resembling thinking" could be achieved if we provide *the machine with the best sense organs that money can buy, and then teach it to understand and speak English*. This is the main reason why we call modern machines with some imitation capacity smart devices.

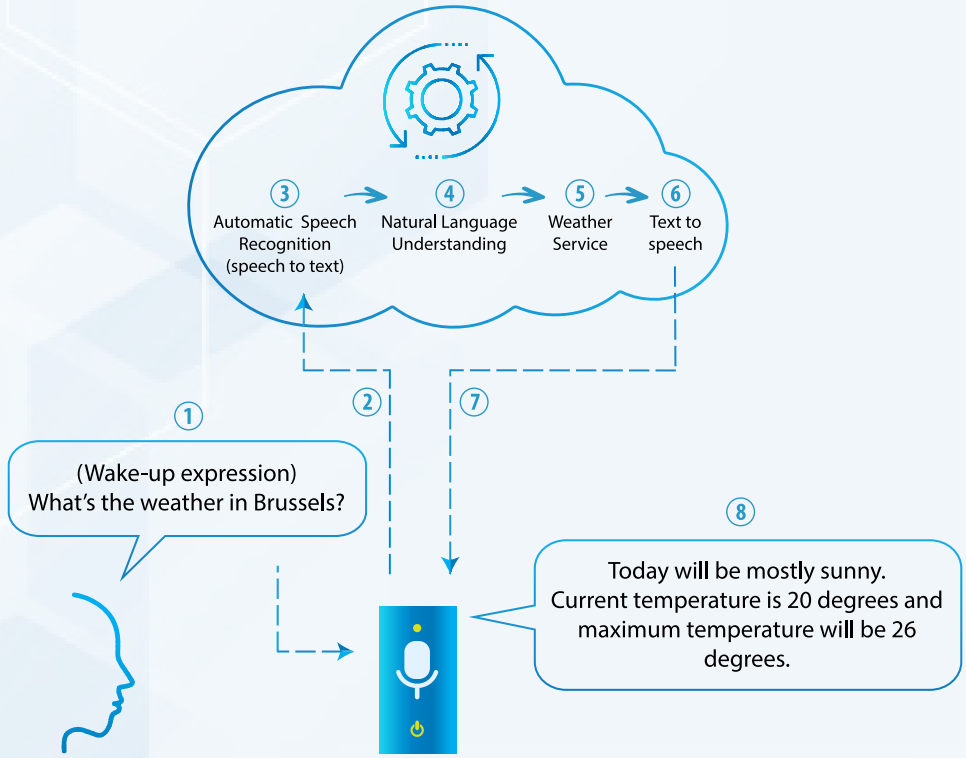
Today, a new generation of speaking devices interact with us in human-like ways to execute simple tasks and answer questions, and not only in English. How is this possible?

I. What is a Smart Speaker? What is a virtual assistant?

A smart speaker is a speaker with a built-in microphone that allows users to interact with other smart devices or internet services using their voice.

The *brain* that makes the *smart* speaker smart is the virtual assistant. A virtual assistant is a software service that takes the voice of the user as its input, identifies a command or question, interacts when necessary with other services and provides a spoken response.

Users say a wake-up expression to activate the virtual assistant, such as *Alexa*, or *OK Google*. Unless turned off by users, smart speaker microphones are switched on continuously in order to detect wake-up expressions. To indicate to users when the smart speaker is recording voice data, the device switches on a light.



The current generation of smart speakers typically have built-in functionalities to search for information on the internet, play music, make phone calls and manage lists. They may also allow for new functionalities and extensions, such as controlling a smart door lock, by installing third-party developed software, through Alexa's skills or Google Home's actions, for example.

Most popular smart speaker and virtual assistants

Vendor	Device	Virtual Assistant
Amazon	Amazon Echo, Echo plus and Dot	Alexa
Google	Google Home	Google Assistant
Alibaba	AliGenie XL	Genie AI
Baidu	Raven H and R, Xiaodu Zijia	DuerOS
Xiaomi	Mi AI speaker	Xiao AI
Apple	Homepod	Siri

There are other smart speaker vendors, but all their devices rely on the virtual assistants listed above, or on Microsoft's Cortana.

The number of smart speakers sold in the USA until January 2019 was 66.4 million. The smart speaker market is also growing in China, Europe and worldwide. Most smart speaker owners have more than one speaker and install them in different rooms in their home.

II. What are the data protection issues?

Until now, user interaction with most technology was mainly visual and tactile. Smart speakers and virtual assistants use voice as the main means of interaction. In our preliminary understanding, this poses several data protection challenges to most of the existing smart speakers and virtual assistants.

Lack of transparency

Ensuring that all users are clearly informed about the data controllers and processors involved in the processing, the types of data processed – such as the user's voice, location and usage history - or the purposes of the processing, is very difficult. For example, once a smart speaker is up and running, it is unlikely that users other than the person who installed the device will have read the written notices that came with the device.

Without transparency, personal data collected by smart speakers could be misused for purposes that go far beyond user expectations. For example, newly patented technologies aim to infer health status and emotional states from a user's voice and adapt the services provided accordingly.

Excessive data retention

It is not easy for users of smart speakers to find out how long their data will be stored. Users are generally left with the task of deleting any data the virtual assistant has processed and kept. In some cases, it might not even be possible to delete all of the data stored. Depending on the virtual assistant, the deletion function might only partially delete the data, deleting only voice data, for example.

Lack of an appropriate consent management mechanism

Smart speakers process the data of voices recorded by their microphones, whether these voices are one of the intended users or not. There is no mechanism yet to prevent a smart speaker from processing the data of a specific individual.

When it comes to processing children's data, there seems to be no way of ensuring that the person with parental responsibility has provided their consent. Parental controls are available to a certain degree but in their current form they are not user friendly. More alarmingly, there are already reports that voice recordings of children are being used to create voiceprints that could be used to identify them when detected by other devices in other locations.

Processing without consent

Smart speakers can mistakenly detect a spoken expression as their wake-up expression and therefore process personal data without user consent.

The wake-up expression can be changed and an individual who is not aware of this change could accidentally switch on the smart speaker.

Repurposing of data

By analysing data collected via smart speakers, it is possible to know or infer user interests, schedules, driving routes or habits. All this data could be used, without people knowing, for profiling and to provide unsolicited personalised services, such as advertising or modified search results.

Security of personal data

Current smart speaker and virtual assistant designs do not offer yet proper access control to personal data. Authentication by voice recognition is optional and does not allow for control of access to personal data by all services. If it is not using voice recognition, access control relies on an optional PIN number that a user has to say.

It is possible to manipulate a smart speaker remotely via signal broadcasting and compromise the speaker via radio or TV. Most smart speakers blindly trust their local networks. Any compromised device in the same network could change the settings of the smart speaker or install malware on it without the user's knowledge or agreement.

Potential for mass surveillance

If working as currently designed, smart speakers locally record for a few seconds and do not send any information to the speech recognition cloud service until the wake-up expression is detected. However, smart speakers could be the target of attacks and access requests from law enforcement agencies. They could access local voice recordings before they are deleted, turning smart speakers into a massive surveillance system installed by the victims of this surveillance.

Data protection by design and by default

As is evident from the previous examples, the current design and behaviour of most smart speakers and virtual assistants does not fully comply with the principles of data protection by design and data protection by default. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should take into account the right to data protection from the outset.

The design of a smart speaker should address data protection issues, in particular to make sure users are informed about the processing of their personal data, to enable them to manage their consent and to demonstrate accountability so that users are fully aware of what happens to their personal data.

III. References and related reading

Adam Wright, 'Worldwide Smart Home Device Forecast Update, 2018–2022: CY 4Q18' [2018]

Amazon Web Services Inc. 'Alexa Privacy and Data Handling Overview' [2018]

Hyunji Chung, Michaela Iorga, Jeffrey Voas and Sangjin Lee, 'Alexa, Can I Trust You?' [2017]

Candid Wueest (Symantec) 'A guide to the security of voice-activated smart speakers' [2017]

Veton Këpuska and Gamal Bohouta, 'Next-generation of virtual personal assistants' [2018]

Hyunji Chung and Sangjin Lee, 'Intelligent Virtual Assistant knows your life' [2018]

Whitney L. Hosey, 'Alexa, transmit client data to amazon: ethical considerations for attorneys looking forward to virtual assistants' [2018]

Eoghan Furey and Juanita Blue, 'She Knows Too Much – Voice Command Devices and Privacy' [2018]

Xuejing Yuan et al, 'All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo' [2018]

Martin Courtney, 'Careless talk costs privacy' [2017]

This publication is a brief report produced by the Information Technology Policy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Author of this issue: Xabier Lareo
Editor: Thomas Zerdick
Contact: techdispatch@edps.europa.eu

HTML ISBN 978-92-9242-423-7 ISSN 2599-932X https://data.europa.eu/doi/10.2804/004275 QT-AD-19-001-EN-Q
PDF ISBN 978-92-9242-424-4 ISSN 2599-932X https://data.europa.eu/doi/10.2804/755512 QT-AD-19-001-EN-N