ISP 2023 Case Study 3*

Smart voice assistants

1 Description

The company DCI (Data Capture Industries) is a highly profitable company, part of the Chinese-based holding AliCent, that has produced a range of tech products like smart televisions, smart refrigerators, laptops, headphones, tablets and smartphones. Their products have been very successful in Western markets, especially in the EU. However recently, in the context of geo-political tensions, it has had some setbacks and came under scrutiny, especially due to some scandals of sizeable data breaches, unlawful access to sensitive data by the Chinese government and a biased voice-recognition that had difficulty of understanding minority languages. However, the company was very swift in addressing all these issues heads on through crucial technical and legal interventions, which have by now somewhat reassured Western policy makers and the public. In a recent renewal of their mission and vision, DCI now even proclaims to be one of the most privacy-friendly tech companies in the world promoting human dignity, among others by including privacy-enhancing features and by sponsoring numerous events, conferences, summer schools on privacy and data protection.

The company has just launched the third and improved version in its very popular smart speaker Ambi. A smart speaker is typically a wireless device activated through voice commands. This enables human-like conversations, personalizes responses based on user profiles, remembers preferences to offer solutions and recommendations, and can even predict user's future needs. These systems use artificial intelligence to continuously learn and improve themselves, for better adapting to their users. Smart speakers or 'communicative robots' have become widely popular since 2012. They are now routinely embedded in everyday life, whereby people are more and more dependent on them for executing simple tasks in the home. They are broadly for two types of activity: as information center (like playing music, checking weather forecasts, listening podcasts,...) and as control center (controlling home automation, setting timers, finding objects,...).

* Wed Jun 14 14:43:44 2023 +0200 / 93d317a / case-study-3.md

The new DCI voice-activated assistant comes to the market in two versions the ad-free Ambi+ ($ 249) and the ad-supported Ambi-pro ($ 39). The significantly reduced price-tag of the latter relates to the increased integration of advertising on input as well as on output side. On the input side the customer agrees that all voice signals can be used for improved personalized advertising, which besides the automated content analysis also includes emotion detection. Of course – DCI being a privacy-friendly company – all data input will be stored on a cloud in Europe and personal data will be processed in accordance with GDPR requirements. On the output side the smart speaker occasionally produces relevant personalized audio ads, which makes the Ambi-pro a servant as well as a salesperson. For these ads AI-generated voices of famous persons are used (like Beyoncé, Barack Obama, Lizzo, Steve Jobs,...), that give a special attractive cachet to the promotional messages.

In their efforts to be a privacy-focussed company they have commissioned an interdisciplinary research project to give independent data privacy advice on their new Ambi-pro. As member of the team of researchers you are asked to discuss ethical, legal, social and technological aspects of their new product, in order to better assess the risks and enhance the privacy of the system. A particular area of interest is privacy in speech and language technology, that would need to be tackled.

2 Tasks

- Analyse the case study from the legal and the societal perspective. Is personal data being processed, and if so, is this lawful? What extreme forms of personal data could be collected using the DCI voice assistant?
- What if visitors enter a house with a DCI voice assistant? What further ethical considerations you think are relevant?
- Analyse how much information about and control over the functioning the voice assistant their owners have.
- Could this be improved somehow? Give concrete suggestions.
- What other measures could DCI deploy to reduce the privacy risks associated with using their voice assistant?