Privacy-aware notification for voice assistants

Farida Yeasmin
sohanamou25@yahoo.com

Problem statement

- Voice user interface (VUI) enables a human to communicate with a computer. This became popular together with the popularity of voice assistant devices (VAD).

- A lack of understanding about user's privacy expectations from voice assistants and limitations of the voice interface creates several privacy concerns for many. For example, many considers voice fingerprinting and location tracking by voice assistants are serious breach of privacy and this creates a sense of distrust for voice assistants.

- This work explores user's emotional experiences for a privacy breach, their privacy expectations, and suggests/implements a privacy-aware notification mechanism based on user's privacy expectation. This presentation is based on a study, Details at https://fruct.org/publications/acm27/files/Yea.pdf

Scope & Methodology

Research Questions

- What are the emotional experiences and privacy expectations of the users, when communicating with VUI?
- How do the above experiences and preferences vary for changing contexts, e.g., in home or guest environment?
- What are the suitable notification modalities for VAD and do the modalities change with the change of context?

Geographic areas

- Espoo, Finland

Goal

The goal is to understand the emotional experiences and privacy expectation of voice user interface. We also want to identify preferred notification modalities in voice communication.

Methodology

Mind maps: We decided to perform two semi-structured interviews. The first interview targets the exploration phase, and the second one focuses on the evaluation of the implementation.

User interviews: We conduct the study, face-to-face in a lab setting, where we choose a moderate study process which guides participants through the study and helped them to understand the questions.

Data analysis: We use thematic analysis to analyze the qualitative data.We follow a cross-tabulation approach to analyze quantitative data.

Participant criteria

Recruitment

The participants are recruited through a social media group by advertising an interview description. They were selected in the first come first serve process. The interview took approximately 1 hour and 30 minutes to complete, and participants are rewarded with two movie tickets for participating in the interview.

We interviewed 8 people.

Criteria

We recruited participants using a random process from a known set of groups. Our participants have few specific requirements:

1	University student
2	From technical fields
3	Aged above twenty years
4	Fluent in English language

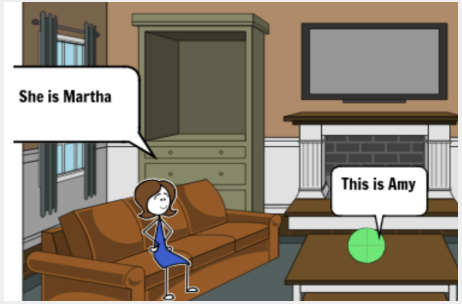
Participant tasks

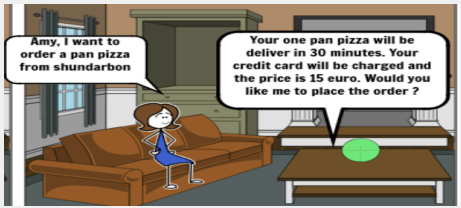
Task 1

Answer to several open-ended questionnaires to collect qualitative data

Task 2

Multiple-choice questions to collect quantitative data.





Storyboard

Task 1

During the study, first, we educate the users on VUI and VAD devices using a storyboard. Second, we describe scenarios, one by one, and ask open-ended questions regarding the user's emotional state for a set of privacy types, e.g., voice fingerprinting, habits, and location.

Example description

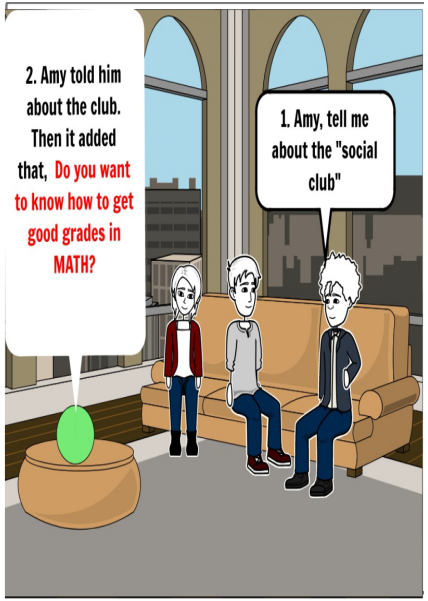
A storyboard for a home environment where there is a user called Martha and one voice assistant device Amy. Martha is ordering a pizza using the voice assistant device.

Amy provides several types of indicators while it processes an order so that the user can understand the actions of the device. For example, Amy makes an audio sound (beep) while it asks about the credit card, shows a visual color notification while it talks with Martha.

Several Example Scenarios

Examples of some different scenarios for different types of privacy.

You are ordering a pizza



Your classmate does not know about your social club. So, he is asking about more information about the social club from Amy to be sure about the club.

you are at your home

You are having a conversation with Amy. The other characters in this pictures are your family members.

At your home

You are speaking with Amy with a heavy tone

Personas

Persona 1

P

Name: Afsar Ali
Age: 30
Education: Masters graduate
Hometown: Delhi, India
Family: Lives with partner
Occupation: PHD candidate

Bio

Afsar is a PHD candidate who lives with his wife. They use a voice assistant device at their home. As an introvert person, he does not want to share his personal lifestyle with other people, such as, he does not like the voice assistant device listen to his private conversation with his wife and share his conversation data with the other devices or give him any suggestions based on that conversation. He wants to live a life where other people or any kind of voice assistant devices won't steal his privacy.

Frustrations

- Not sure if the voice assistant device is collecting private conversation data or not. The notification is not clear.
- How dangerous it can be when the device shares the data with other devices.

Goals

- No type of personal data will be collected by listening private conversation through a voice assistant device located at home.
- Collected data by a voice assistant device can not be shared with other devices.
- If personal data is processed, it should notify with a visual or app message.

“

It is not acceptable at all if a voice assistant device collect my private data without my concerns and share it with other devices or give suggestions based on the collected data.

Taken from https://fruct.org/publications/acm27/files/Yea.pdf

Persona 2

Name: Olivia Samuelsson
Age: 24
Education: University student, final year
Hometown: Copenhegen, Denmark
Family: Lives alone
Occupation: Student

Bio

Olivia is a university student who lives alone in a student apartment . Every weekend she goes to her friends's house (who has a voice assistant device at her house) to group study. Sometimes they order food using her friend's voice assistant device (VAD). Whenever Olivia order food, the device gives her several food suggestions as the device recognises her voice from the previous food orders.

Frustrations

- Do not like that the device recognised her voice and remembered her.
- The voice assistant device offers different types of food suggestions while ordering food. Providing suggestions without asking for it is annoying.

Goals

- The device shouldn't recognise her voice while ordering food.
- Stop recognising options should be in the device.
- The notification for processing personal data should be clear even when not looking at the device, e.g., special audio notification.

“

I personally do not like that my friends VAD is recognising me even after a long time of using it. It should forget what I had ordered a long time ago. The device should have turn off this feature.

Taken from https://fruct.org/publications/acm27/files/Yea.pdf

Privacy expectations from VAD

- **Require consent to use private data**
- **Feature to forget the private data**
- **Feature to turn of processing of private data**
- **Data can only be used for positive purposes**

Key insights for privacy expectations

The privacy of the person (i.e. voice fingerprint)

Participants expect that a VAD should not identify voice if a user has not interacted with it before. This means they do not like sharing voice identification data from one VAD to another.

The privacy of behaviour and action (i.e. Habit)

Participants show curiosity about habit detection, i.e., how the device identifies habits. This means that participants want to know how the habit detection algorithm works and what data is stored for this process.

The concerns of privacy of data and image (i.e. Listening to a private conversation)

According to the participants, listening to private conversations and storing the data is not acceptable. Participants expect that the device should ask for consent from the user before listening on private conversations.

The privacy of thoughts and feelings (i.e. emotions)

Participants expect collected data should only be used for positive purposes. Participants also hope that collected data will not be shared with others.

The privacy of location and space (i.e. Location tracking)

Participants expectation for privacy is that location data collected by the VAD can be used only when appropriate consent is provided.

Product feedback

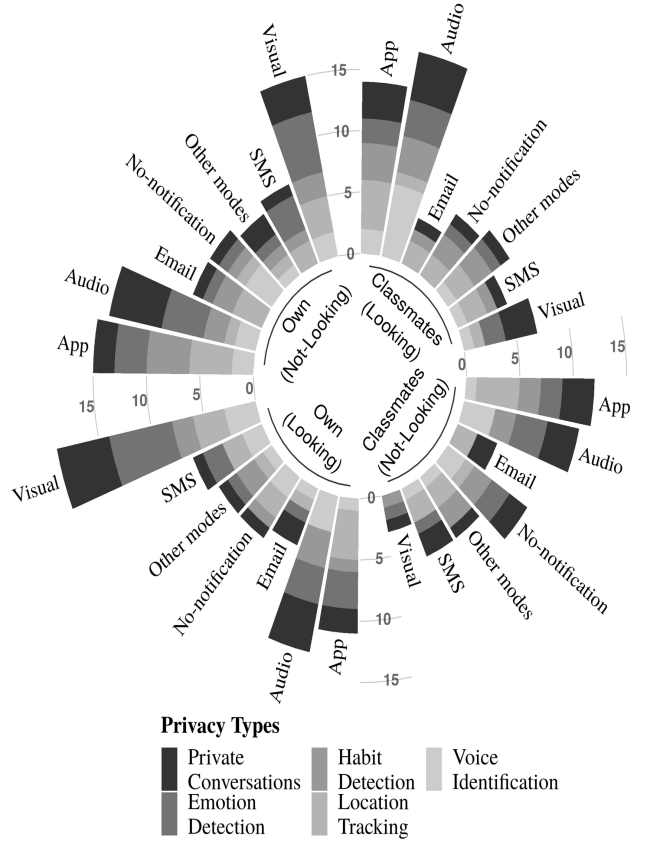


Image source: https://fruct.org/publications/acm27/files/Yea.pdf

Key actions to improve privacy notifications for VAD

- A privacy notification whenever a VAD device collects or processes personal data. The notification modalities differ with the context change
  - Own house, looking at voice assistant: Visual, app, audio
  - Own house, not-looking at voice assistant: App, visual, audio
  - Classmates house, looking at voice assistant: Audio, app
  - Classmates house, not-looking at voice assistant: App, audio
- A beeping audio should happen before asking to store private data. That way, the user would be more focused on what Alexa asks, knowing that the next thing that he or she speaks is important.
- Notifications to specify if the saved personal data is only used for the intended service or by other services as well.

Example privacy-aware notification application for VAD

Example Application User journey map

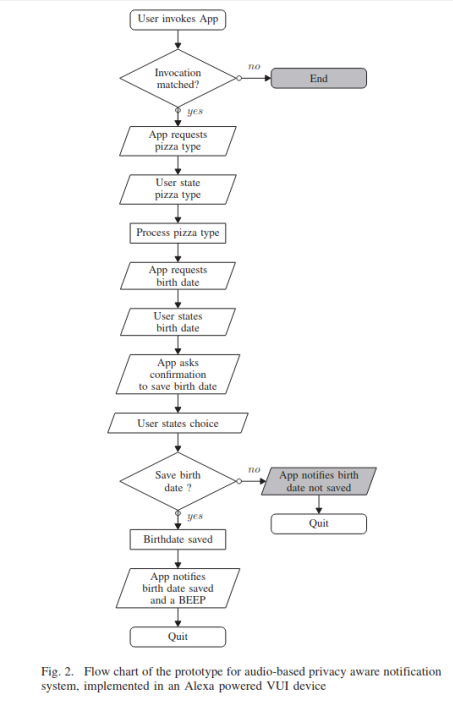


Fig. 2. Flow chart of the prototype for audio-based privacy aware notification system, implemented in an Alexa powered VUI device

Image source: https://fruct.org/publications/acm27/files/Yea.pd

Overview

We implemented an Amazon Alexa skill by incorporating the privacy expectations from our study. The skill uses audio modalities for privacy notifications. We implemented two types of audio notifications when storing private data, i.e., birthday. The first type is: (1) Audio-based explicit notification when a private data is stored and (2) Distinct audio sound to notify users that a privacy-sensitive operation has taken place.

In voice interaction, the user often does not think when providing confirmation. Due to this, our application also uses distinct audible two short **Beep** sound to guide users that sensitive data has been stored. For this, we use the Speech Synthesis Markup Language (SSML) feature of Alexa.

Un-answered Questions

We use the semi-structured interview in a lab environment to gather data for privacy experiences and expected notification modalities for VAD. Data collected using the semi-structured in lab settings may not reflect the actual pattern compared to realistic field studies with behavior tracking. In a lab setting, participants may not be express their genuine emotions for different privacy scenarios.

We only analyzed emotional experiences and expectations based on a defined five types of privacy in two primary contexts. Our defined five types of privacy, in some scenarios, may become coarse and fails to differentiate emotional experiences. For example, we analyzed the emotional reactions of participants when a VAD device tracks their habit. However, we did not further granularize different types of habits, e.g., purchasing habit and movie watch list habits.

We gathered and analyzed quantitative data about the user's expected notification modalities for five types of privacy. We did not present the notification in a real setting by a VAD during the user study (except during implementation evaluation). We assumed that participants of the user study could imagine the context and the presented notification modalities. Thus, it is likely that participants were unable to think which notification is suitable for each type of privacy.