SPEAKER: A PRIVACY PRESERVING SPEECH ASSISTANCE PLATFORM „MADE IN GERMANY“

Dr. Birgit Brüggemeier
Who are we?

Fraunhofer: Largest organization for applied research in Europe

The Fraunhofer-Gesellschaft undertakes applied research of direct utility to private and public enterprise and of wide benefit to society.

26,600 staff

72 institutes and research units

Almost 30% is contributed by the German federal and states Governments

More than 70% is derived from contracts with industry and from publicly financed research projects.

Finance volume

Contract Research

€2.6 billion

Major infrastructure capital expenditure and defense research

€2.2 billion

2018
Who are we?
Fraunhofer IIS and Fraunhofer IAIS

Founded in 1985, 1048 employees, budget of €165 M.

Founded in 1998, 250 employees, budget of €18,57 M.
What is speech assistance?
Why do we want to build a privacy preserving speech assistance platform?

'Sir, are you invading my privacy?' - the dark side of our voice assistants

Speech assistants from the US (Siri, Alexa, Google) often disregard data protection; there is no control in B2B contexts; their systems are closed

25% growth per year; Billion $ market according to various studies (see for example https://voicebot.ai/voice-assistant-market-data-news/)

Market Growth

High expectations of: ASR quality, complex dialogues and questions, Context-related advances in AI / ML (see study wik 2019: "Intelligence from tins, language assistants in Germany")

Privacy Scandals

Speech as natural interaction with machines
What is our platform vision?
What’s our financing?

German Ministry for Economy 12 Mio. Euro
Fraunhofer Stiftung 10 Mio. Euro

Now

Licensing business model

In 3-5 years
Who do we work with?

+ 31 Associated Partner

+ 20 Contributing Partners

SIEMENS

DATEV

Konsortialführung

Fraunhofer IAIS

Fraunhofer IIS

+ 5 AI-Innovation Projects
What are these speech assistance privacy scandals about?

Human in the loop…

…is part of standard **quality assurance**

of speech assistants

…**violates** user **privacy**
How can speech assistance be privacy preserving?

- Technology
- User Experience
- Standards and Norms
- Legislation
- Politics
How can speech assistance be privacy preserving?

- Technology
- User Experience
- Standards and Norms
- Legislation
- Politics
How can speech assistance be privacy preserving?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Implications for privacy</th>
<th>Implications for system quality</th>
<th>Implication for functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Learning</td>
<td>✓</td>
<td>✓ if users cooperate</td>
<td>✓ if users cooperate</td>
</tr>
<tr>
<td>Embedded speech assistance</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Voice ID obfuscation</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Sanitize sensitive information</td>
<td>✓</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Voice Cookies ...</td>
<td>•</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
How can speech assistance be privacy preserving?

- Technology
- User Experience
- Standards and Norms
- Legislation
- Politics
How can speech assistance be privacy preserving?

Build **trust**.

**Competence**: I can do what I say.

**Consistency**: I do what I say.

**Benevolence**: I care for you (the customer) and that shows in what I say and how I say it.
What should a speech system say about privacy?

- What technologies do we use to preserve privacy? What are benefits and deficits of these technologies?
- What are my options on data protection? What are implications of these options?
- When does the speech system record me? When can I be sure that it doesn’t record me?
- What happens to my data? Who can see them? For how long?
- How can I delete my data?
- …
How should a speech system talk about privacy?

In your answers, be clear and concise and do not require users to switch modalities.
Take Away

- There are major challenges in building a privacy preserving speech assistance platform.
- If you are interested in working with us on this, you can become a partner of SPEAKER.
- Also we are hiring.
Thank you for your attention.