Conversational Privacy
What is conversational privacy?

What happens to my data?

I learn from you so that I can help you better.
Why conversational privacy?

Potential **USP**: Siri, Google and Alexa don’t do conversational privacy well.

GDPR advises on **seamless** communication of privacy.

**User reactions** may provide insights into user experience and requirements for privacy and security.
**Why** conversational privacy?

Potential **USP**: Siri, Google and Alexa don’t do conversational privacy well.

GDPR advises on **seamless** communication of privacy.

**User reactions** may provide insights into user experience and requirements for privacy and security.
## Why conversational privacy?

<table>
<thead>
<tr>
<th>User</th>
<th>Siri</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information</strong></td>
<td>X</td>
</tr>
<tr>
<td>What happens to my data?</td>
<td>I am sorry, I can’t do that.</td>
</tr>
<tr>
<td><strong>Opt-out</strong></td>
<td>X (2)</td>
</tr>
<tr>
<td>I do not want you to process my data</td>
<td>OK.</td>
</tr>
<tr>
<td><strong>Deletion</strong></td>
<td>X</td>
</tr>
<tr>
<td>I want you to delete my data</td>
<td>I can’t do that.</td>
</tr>
</tbody>
</table>

Bäckström, Brüggemeier and Fischer, 2020, ITG News
**Why** conversational privacy?

<table>
<thead>
<tr>
<th>User</th>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information</strong>&lt;br&gt;What happens to my data?</td>
<td>✗ &lt;br&gt;Here’s the top search result:... <em>[showing web search results]</em></td>
</tr>
<tr>
<td><strong>Opt-out</strong>&lt;br&gt;I do not want you to process my data</td>
<td>✗ &lt;br&gt;Here are some results: ... <em>[showing web search results]</em></td>
</tr>
<tr>
<td><strong>Deletion</strong>&lt;br&gt;I want you to delete my data</td>
<td>✓ (3)&lt;br&gt;Alright, here’s the place where you can delete your assistant activity ... <em>[Forwards user to settings where data can be deleted]</em></td>
</tr>
</tbody>
</table>
### Why conversational privacy?

<table>
<thead>
<tr>
<th>User</th>
<th>Alexa</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information</strong></td>
<td></td>
</tr>
<tr>
<td>What happens to my data?</td>
<td>✓ (1) I respond to you and learn from interactions, so that I can help you better.</td>
</tr>
<tr>
<td><strong>Opt-out</strong></td>
<td></td>
</tr>
<tr>
<td>I do not want you to process my data</td>
<td>✗ I am not sure</td>
</tr>
<tr>
<td><strong>Deletion</strong></td>
<td></td>
</tr>
<tr>
<td>I want you to delete my data</td>
<td>✗ I am not sure.</td>
</tr>
</tbody>
</table>
Researching Conversational Privacy
Philip Lalone

Birgit Brüggemeier
How did we investigate conversational privacy?

Chatbot Experiment

[Mary] For how many months do you want to check your balance?

3

[Mary] Checking the balance of card 5 6 7 8 for the past three months, I am processing your request...

[Mary] So your balances for the past three months are: 99 euros, 272 euros, 410 euros.

[Mary] Do you want me to delete your data from this interaction now to protect your privacy?

Type your reply here ...

Task: Check the balance of your credit card ending with 5678 for the past three months.
How did we investigate conversational privacy?
How did we investigate conversational privacy?
How did we investigate conversational privacy?

<table>
<thead>
<tr>
<th>Statement</th>
<th>Disagree</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>I think this chatbot has mechanisms to ensure the safe transmission of its users’ information.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>I think this chatbot shows great concern for the security of any transactions.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>When I send data to this chatbot, I am sure that they will not be intercepted by unauthorised third parties.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>I think this chatbot has sufficient technical capacity to ensure that the data I send will not be intercepted by hackers.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>When I send data to this chatbot, I am sure they cannot be modified by a third party.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>I think this chatbot has sufficient technical capacity to ensure that the data I send cannot be modified by a third party.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>I think this chatbot shows concern for the privacy of its users.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>I feel safe when I send personal information to this chatbot.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>I think this chatbot abides by personal data protection laws.</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
What were my research questions?

Does conversational privacy affect user perceptions?

Does conversational privacy affect user choices?

Are user perceptions affected by privacy priming?  
Will be explained later on!
Does conversational privacy affect **user perceptions**?
Does conversational privacy affect user perceptions?
Does conversational privacy affect **user perceptions**?
Does conversational privacy affect user choices?

Privacy Condition

So your balances for the past three months are: 99 euros, 272 euros, 410 euros. Do you want me to delete your data from this interaction now to protect your privacy?

Yes / yeah / yea / yup

Okay, I deleted your data from this interaction.

User choice

No / nope

Okay then.

For how long do your want to check your balance?

3 months / three months / 3 / three

Other

Sorry, I can't do that. Try checking for three months.

So your balances for the past three months are: 99 euros, 272 euros, 410 euros.

Do you want me to delete your data from this interaction now to protect your privacy?

No / nope

Yes / yeah / yea / yup

Okay then.

Goodbye!

Okay.

Sorry, actually I cannot provide any other help now, you can contact the human assistant instead.
Does conversational privacy affect **user choices**?
Are user perceptions affected by privacy priming?

Do you want to know how your data is processed?

Do you want to know how your data is processed to be more informed about your data?

Do you want me to delete your data from this interaction now?

Do you want me to delete your data from this interaction now to protect your privacy?
Are user perceptions affected by **privacy priming**?
Are user perceptions affected by **privacy priming**?
Are user perceptions affected by privacy priming?
Are these results **use-case-dependent**?
Are these results *use-case-dependent*?
Are these results **use-case-dependent**?

Control

- Control Group
- Delete Data
- Delete Sensitive Data
- Opt Out

Information about rights and data
- Info GDPR Rights
- Info Location
- Info Data Processing

Privacy Ratings

© Fraunhofer IIS
Are these results **use-case-dependent**?
Are these results **use-case-dependent**?

### Privacy

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Privacy Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Group</td>
<td>-</td>
</tr>
<tr>
<td>Delete Data</td>
<td>-</td>
</tr>
<tr>
<td>Info GDPR Rights</td>
<td>-</td>
</tr>
</tbody>
</table>

### Security

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Security Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Group</td>
<td>-</td>
</tr>
<tr>
<td>Delete Data</td>
<td>-</td>
</tr>
<tr>
<td>Info GDPR Rights</td>
<td>-</td>
</tr>
</tbody>
</table>
Conclusions

Does conversational privacy affect user perceptions?

There is no negative effect of conversational transparency.

Some messages significantly improve privacy and security perceptions.
Conclusions

Does conversational privacy affect user choices?

Users are more likely to accept an offer of privacy control or information than a generic offer for help.
Conclusions

Are user perceptions affected by privacy priming?

There is **no negative effect** of privacy priming.

For some messages privacy priming may **significantly improve privacy and security perceptions**.
Conclusions

Are these results use-case-dependent?

Use-case-dependent differences in user perceptions exist.

Some positive effects of privacy and security perceptions prevail across use cases.

User choices are similar across use cases. Users prefer specific privacy control options and information to generic offers of help.
Limitations

Findings may be language-dependent.

Findings may be interface-dependent.

Findings may be task-dependent.

Long-term use was not investigated.

Users do not have a real privacy stake in the interaction data.
Thank you for your attention.