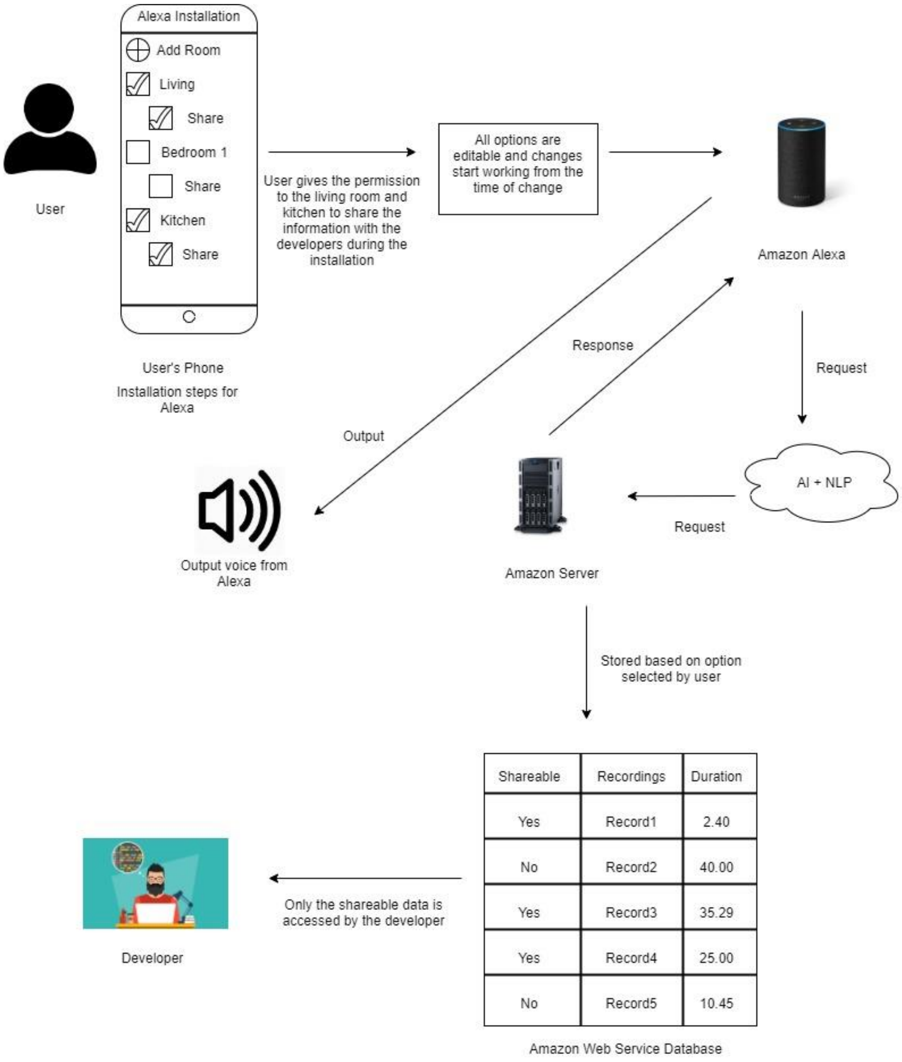
Durga Prasad Rangavajjala – 300123236
Yamuna Satheesh Kumar – 300115516
Vidhi Mistry – 300101658

Ethics in AI : Design Assignment 3

Design Topic : Amazon developers listening to audio recordings of users
Key Value Tension : User's Privacy vs Amazon's Accessibility to Data

In the ethical analysis, three design solutions to the abovementioned design problem were suggested, out of which two design solutions were explored further and prototypes in the form of system diagrams were developed for them. The two design solutions and their concerning prototypes are :
1. Privacy levels based on room : Prototype 1
2. Amazon Alexa responding to two wake words: Prototype 2
Echo Smart speakers have Alexa technology at core, and hence the words Echo smart speaker and Alexa are used interchangeably in this report.

Prototype 1 : Privacy levels based on room


Alexa Installation
⊕ Add Room
☑ Living
☑ Share
□ Bedroom 1
□ Share
☑ Kitchen
☑ Share
User
User's Phone
Installation steps for Alexa
User gives the permission to the living room and kitchen to share the information with the developers during the installation
All options are editable and changes start working from the time of change
Amazon Alexa
Response
Request
Output
AI + NLP
Request
Output voice from Alexa
Amazon Server
Stored based on option selected by user
Only the shareable data is accessed by the developer
Developer
Amazon Web Service Database

Shareable	Recordings	Duration
Yes	Record1	2.40
No	Record2	40.00
Yes	Record3	35.29
Yes	Record4	25.00
No	Record5	10.45

Durga Prasad Rangavajjala – 300123236
Yamuna Satheesh Kumar – 300115516
Vidhi Mistry – 300101658

Description:
The prototype suggestion is in the form of a high-level system diagram for the Amazon Echo. It's a visual representation of the suggested system design for the Amazon Echo, that depicts the key system components and interactions between them.

The proposed system design here allows the Amazon Alexa technology to incorporate different shareability preferences based on the room.

Explanation:
While setting up Amazon Echo, the user is asked about the room where Amazon Echo is being set up. It also detects other Amazon Echo set up in the other rooms in the house and prompts the user about them and their sharing preferences. Based on the room, the user's has choice to allow/disallow sharing of his personal voice recordings. For example, as shown in the diagram, the person has chosen to share his recordings from the Echo placed in the living room and kitchen, whereas sharing disabled for private bedroom space. Also, by default, the sharing options would be disabled for private spaces like bedroom and bathroom. Moreover, these options are made available to the user at any time, not just installation, and could be changed by the user at any point of time, accessing the Amazon Echo settings from his account. Whenever an interaction is done with Alexa, the Alexa sends the data (voice recording) as a request to the speech recognition (AI and NLP) services and then request is processed and stored in the server. The server then responds back to the user's query to the Alexa and the output is spoken loud by the Alexa. Another key design idea here is to augment the data stored with a field 'Shareable'. The value of this field is determined based on the preference chosen by the user for concerning Echo and the room. If sharing was disallowed, this field would have value 'No' and if it was allowed, the value for this field would be 'Yes'. The developers now would only be given access to the data that has 'Shareable' field set to 'Yes'.

How it solves the value tension?
In this way, the users would be given more choice with how their data would be handled providing sharing options based on each room. Such settings are aimed to make user's more aware of the implications of using Amazon Alexa in each room. Moreover, with default settings set to not shareable for usual private spaces like bedroom would still adhere to privacy concerns of majority of people even if the user hurries up through key parts of installation. The developers on the other hand would still have access to limited pool of data containing recordings that were deemed as shareable by the user.

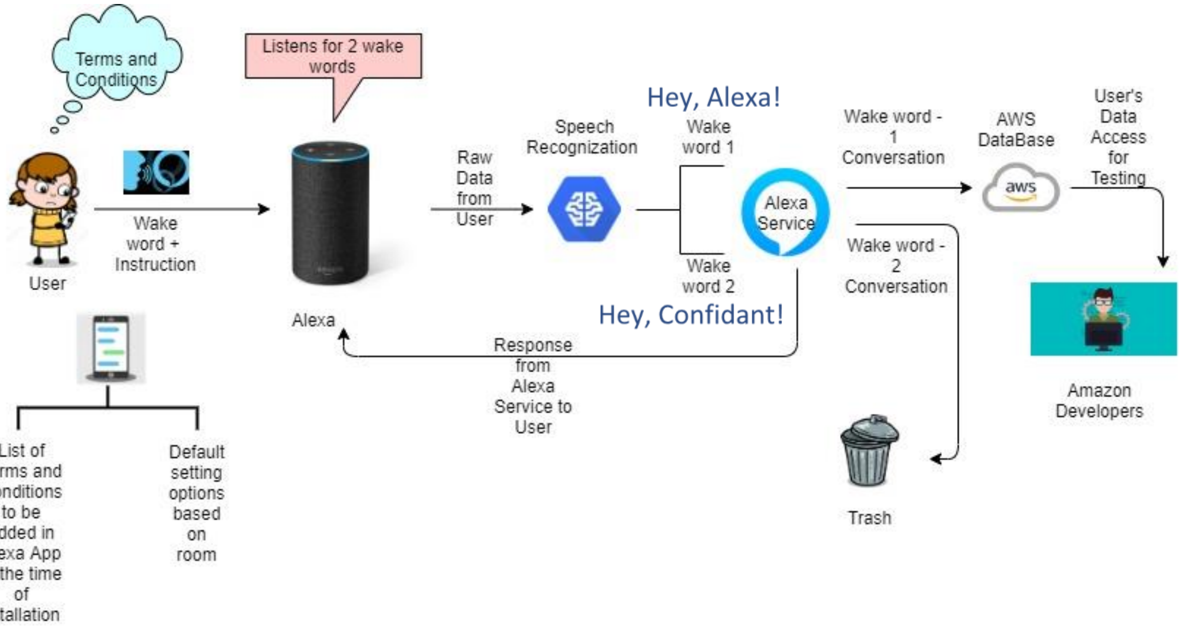
Pros:

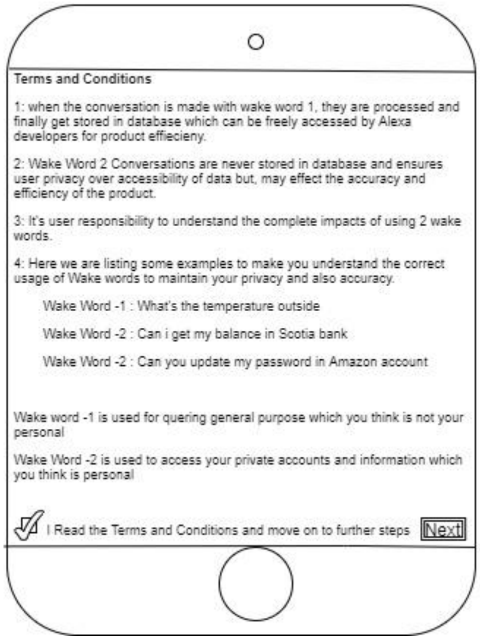
- User's would have more control over privacy settings with choices given for each room
- Granularity of the privacy level has increased, being assigned now per each room
- User's more aware about the data collection by Amazon and its implications based on room
- Allows Amazon to collect the data and share a pool of shareable data with developers

Cons:

- The data that was meant to be private (not shareable) is still stored in the Amazon database servers which poses risks of data leakage and hacking.
- Strictly restricts data sharing for a space, that is all the non-private conversations carried out in a space with sharing disallowed, would still be considered as private and wouldn't be accessible to the developers. This might limit the data accessible to the developers and hence impede improvements in Alexa services.

Prototype 2 : Amazon Alexa responding to two wake words


Terms and Conditions
Listens for 2 wake words
User
Wake word + Instruction
Alexa
Raw Data from User
Speech Recognization
Hey, Alexa!
Wake word 1
Alexa Service
Wake word 2
Hey, Confidant!
Wake word - 1 Conversation
AWS DataBase
aws
User's Data Access for Testing
Wake word - 2 Conversation
Amazon Developers
Response from Alexa Service to User
Trash
List of Terms and Conditions to be added in Alexa App at the time of installation
Default setting options based on room



Terms and Conditions

1: when the conversation is made with wake word 1, they are processed and finally get stored in database which can be freely accessed by Alexa developers for product effiecieny.

2: Wake Word 2 Conversations are never stored in database and ensures user privacy over accessibility of data but, may effect the accuracy and efficiency of the product.

3: It's user responsibility to understand the complete impacts of using 2 wake words.

4: Here we are listing some examples to make you understand the correct usage of Wake words to maintain your privacy and also accuracy.

Wake Word -1 : What's the temperature outside

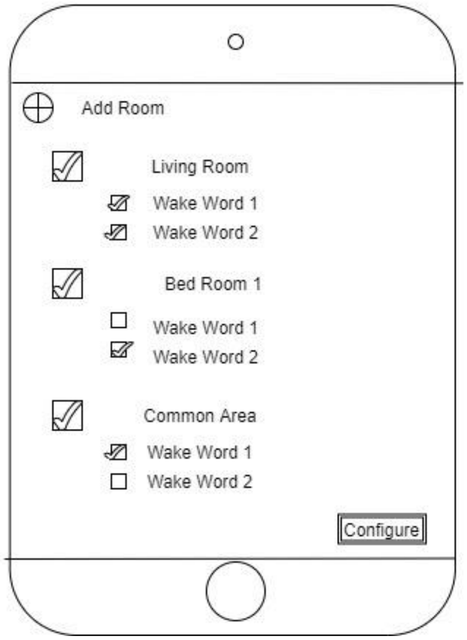
Wake Word -2 : Can i get my balance in Scotia bank

Wake Word -2 : Can you update my password in Amazon account

Wake word -1 is used for quering general purpose which you think is not your personal

Wake Word -2 is used to access your private accounts and information which you think is personal

☑ I Read the Terms and Conditions and move on to further steps [Next]



⊕ Add Room

☑ Living Room
☑ Wake Word 1
☑ Wake Word 2

☑ Bed Room 1
□ Wake Word 1
☑ Wake Word 2

☑ Common Area
☑ Wake Word 1
□ Wake Word 2

[Configure]

Durga Prasad Rangavajjala – 300123236
Yamuna Satheesh Kumar – 300115516
Vidhi Mistry – 300101658

Description:
The prototype suggestion is also in the form of a high-level system diagram for the Amazon Echo. It's a visual representation of another suggested system design for the Amazon Echo, that depicts the key system components and interactions between them.

With this being totally different approach to solve the design problem, this system design also borrows some ideas like 'room wise privacy levels' from the previous design.

The system is designed to incorporate usage of two wake words for Alexa and to allow two different behaviors of Alexa as per the wake word used to summon the Alexa.
For example, two different wake words very well could be :
Wake Word 1 : "Hey, Alexa!" which summons Alexa with usual behavior.
Wake Word 2 : "Hey, Confidant" which summons Alexa in 'Incognito' mode. Like the 'Incognito' mode in Google that doesn't store the browsing history of the user for that window, the Echo here wouldn't store the conversation it had with user when it is summoned with this wake word.
Though by default, these two different wake words would be suggested to the user, but user can choose any wake words of his choice for both 'Wake Word 1' as well as 'Wake Word 2'

Explanation:
When the Amazon Echo is set up for the first time, the Amazon Echo prompts the user explaining the usage of the two wake word, when should they be used with few examples that make it clear to user the difference between them, and also the consequences of using each wake word. For, example, as mentioned in the Terms and Conditions, 'Wake Word 1' is to be used for conversations that user wouldn't mind to be shared with the developers, whereas 'Wake Word 2' is to be used when conversing privately with the Amazon Alexa. In the next step, the user's is asked about the preferences about the wake words based on each room. For example, as shown in the diagram, both the wake words are selected for living room, implying both wake words can be used for summoning the Alexa in the living room. Whereas for the private bedroom space, only 'Wake Word 2' is selected, implying that only 'Wake Word 2' could be used to interact with Alexa. Later, when user interacts with the Amazon Alexa, the recording is processed using the speech recognition service and the query is send to the Alexa service. The Alexa service then processes the query and sends back the answer to the Echo device, which is spoken out loud by the Alexa. Alexa service has a key role here, after processing the query of the user, the data recording is handled differently based on the wake word used. If 'Wake Word 1' was used, then the recording is stored in the AWS database, to which the developer's have access. Whereas, if 'Wake Word 2' was used by the user, the recorded conversation goes to trash and is lost forever.

How it solves the value tension?
In this manner, user can converse privately with Alexa without any concern of his recording being accessed by any other person. Settings like just using 'Wake Word 1' in some spaces would enforce restrictions on user's and would prevent them from exploiting this privacy settings by talking privately all the time and would allow Amazon to gather data for Amazon developers to improve existing Alexa services.

Pros:

- User’s would have even more control over privacy allowing usage of different wake words for each room
- Granularity of the privacy level has increased, being assigned per each recording, rather than a room
- With guidelines for usage of two wake words, and wake word usage per room would increase user’s awareness about the data collection by Amazon and its implications based on room
- Data leak flaw in first design is resolved with this new system design. The conversation that was meant to be private (‘Wake Word 2’) is never stored, ensuring complete privacy for private conversation and decreasing the chances of data leak
- Exploitation by user’s is addressed in this system. This system enforces restrictions on user from exploiting privacy settings for example carrying out private conversations in common spaces where Echo device is configured to listen to just ‘Wake Word 1’ and share the data with the Amazon developers.

Cons:

- User’s can still somehow manage to exploit privacy settings by allowing usage of both wake words in every room and carrying conversations with just the ‘Wake Word 2’. This again might limit the data accessible to the developers impeding improvements in Alexa services to some extent. However, the consequences of using the ‘Wake word 2’ is clearly mentioned in terms and condition in order to make user aware about consequences of such practices, as a workaround to this problem.
- User must be mindful about which wake word he is using

Conclusion

The second system can be also be viewed as an iteration of first system design. The second one includes the best parts of the first system design and tries to eliminate the flaws of the first one with introduction of new concept of using two wake-words. Both the flaws of first system design that are addressed in the second prototype. Moreover, the second proposed system doesn’t introduce any new alarming ethical issues concerning both the stakeholders except a small responsibility on user to be mindful about the wake words; it simply weakens the concerned key tension amongst them by introducing usage of two wake words based on privacy levels. Furthermore, two wake word system design grants more freedom to users compared to first one, allowing them to make conversations with different privacy levels in different rooms at any point of time. And, looking from the perspective of Amazon Developer’s, they would also benefit from the recording made by the user with ‘Wake word 1’ in private spaces and incur more recordings assisting them in carrying out and release improvements to Alexa services. All these abovementioned reasons make it easy to choose the two wake word system design (Prototype 2) over the other proposed system (Prototype 1).