Ethical Analysis

Design Problem: Alexa, stop eavesdropping!

Design Description

The system used here is the Amazon Echo which is a smart speaker developed by Amazon. The Echo device connects to the voice-controlled intelligent personal assistant service Alexa, which will respond when you say "Alexa". When the wake-word is said the device starts to record the conversation of the user and stores it which can be used by the developers to improve or update the system. These conversations can get recorded without the user's knowledge which can impact the privacy of the users. Alexa is incorporated in many devices; however, Echo Smart speakers have Alexa technology at core, and hence the words Echo smart speaker and Alexa are used interchangeably in this report.

Key Value Tension: User's Privacy vs Amazon's Accessibility to Data

A report in TechCrunch says nearly 70% of US smart speaker owners use Amazon Echo devices. Moreover, growth of 13.7% in smart speakers is predicted, reaching a total of around 83.1 million Amazon Echo users in US [1]. With these numbers just limited to US, number of worldwide Amazon Echo users could be anticipated to be even more. It's worthwhile to study the value – 'privacy' that is important to everyone in this horde, and the practices adopted by the Amazon with respect to Alexa voice services.

Description of Key Value Tension

With every utterance of wake word of 'Alexa', or any conversation with Alexa using Echo speaker, the user generates a voice recording. These voice recordings are of value to both the user as well as the Amazon. They are of value to the user because it is personal data. On the other end, Amazon needs this data to improve Amazon services including the speech recognition of Alexa. Complications arise as the user might not want to share the voice recordings or he might not be knowing about Amazon accessing the data for Amazon's own gain. This brews the tension between the User's privacy and the Amazon's data accessibility.

Ethical Issue: Privacy

Often overlooked is the aspect of human involvement in the machine learning especially behind technologies like Alexa. Not many know that every conversation with smart speakers is recorded, stored, and certainly not aware of the fact that Amazon's employees can listen to fragments of those recordings. In an investigation report by Bloomberg on April 10,2019, Amazon was accused of employing people around the world to listen to voice recordings from Echo users' homes [3]. The report made clear that some of the things user's say aren't just processed by computers but by real people. The report mentioned Amazon spokesman confirming hiring of contractors around the globe to transcribe and annotate the voice clips in order to improve the speech recognition systems. Charlie Osborne, a cybersecurity journalist shows her concerns in her article stating that idea of an unknown human listening in is enough to make her feel uneasy even though she has mundane interaction recordings with Alexa. [2]

In a response to this issue, the Amazon claims to use only a small percentage of the voice recording for parsing by humans and claiming the recordings being anonymized. However, it might still contain sensitive information like phone-numbers or addresses in the recording that make it easy to track down the people involved. Such privacy concerns are even higher when such Alexa Echo speaker is placed in a private space like bedrooms. Though not related to Alexa and Echo speakers but similar smart speaker technology by a competitor Google, a news service - VRT News

identified Google users by listening to 1,000 leaked recordings of user's Google Assistant queries [4]. The news firm said that they could easily hear sensitive information in those recordings which made the job of identifying the users easier.
To address the privacy concerns of users, the Amazon introduced new feature that lets the user disable the human review of their Alexa-recordings [5]. However, the feature is not known to all user's and by default it's set as to help improve Amazon services until toggled off. Also, Amazon gives users control to delete those recordings [6]. Christopher Coons, a senator (D-DE) questioned Amazon about how long the company holds on to voice recordings and transcripts. Coons shared the Amazon's response stating that there still exists a possibility that transcripts of user voice interactions with Alexa are not deleted from all of Amazon's servers, even after a user has deleted a recording of his or her voice [7]. Thus, there is need to analyze the ethical implications of privacy concerns related to Echo speakers and propose solutions addressing it.

Design Decisions
We will list some of the feasible design decisions for Amazon Alexa and their value outcomes.

1. *Amazon Alexa responding to two wake words*: As of now Alexa is responding to a single wake word and whenever the wake word followed by instruction is given, it is being processed and stored in cloud. This procedure is not prioritizing the difference between normal query and personal conversation with Alexa. So, our design decision is to have two wake words, where one wake word can be used for general purposes and data after processing will be stored in cloud and this data can be freely used by developers. Other wake word is for having personal conversation with Alexa, where the conversation is processed and stored locally in Alexa and deletes all the recordings once the conversation is completed. This wake word works like Incognito in browsers ensuring the user's privacy, data storing in cloud. However, it's important for the user to decide when to use these wake words because the personal conversation is not stored anywhere with second wake word may affect the Alexa's accuracy and performance. So, user's need to be made aware of the consequences of using both the wake words for effective utilization of wake words.

2. *Privacy levels based on room*: Rather than giving same data sharing and storing options in Amazon Alexa, we can also have a design decision to restrict some features based on the room where Echo smart speaker is set up. When it is installed for the first time in the house, user's is asked to configure the number of rooms, type of each room with some defaults whether to share the data with developers and for testing purposes. When the Amazon Alexa is set up in a room that has data sharing option set to private then conversations with Alexa in that room will never be shared with anyone. According to Andrew Burt, managing user consent is very difficult and they can change their preferences anytime [8]. So, design decision gives the editable preference setting option for the user to change the privacy option for room at any point of time ensuring user's privacy over the amazon accessibility to data. Thus, the consent management should be dynamic enough to accommodate these changes.

3. *Data sharing based on user's permission*: The Alexa starts recording each conversation of the user. These recordings get stored on the cloud without the user's knowledge. We

can have an alternate design decision to restrict the use of these recording by the developers. When the conversations are recorded and stored in the device a notification should be sent to the user regarding the storage of conversations. When the developers want to use these recordings to improvise the device, a message or notification should be sent to the user seeking the permission of the user. Then it is up to the user to give permission for the developers to use the recording or deny the request. Before the sharing the recording to the developers the user permission is needed. So, the design decision gives preference to user's permission on sharing those recorded conversations before it is used by the developers. However, this approach can significantly delay the developing and testing tasks as they wait for the user's permissions. Moreover, user would have to go through each recording before giving permissions and it might become tedious as number of recordings increase.

References

[1] S. Perez. (2020). Nearly 70% of US smart speaker owners use Amazon Echo devices. TechCrunch.com.
[2] C. Osborne. (2019). Amazon employees listen in to your conversations with Alexa. ZDNet.com
[3] Day, et al. (2019). Amazon Workers Are Listening to What You Tell Alexa. Bloomberg.com
[4] Hee, et al. (2019). Google employees are eavesdropping, even in your living room, VRT NWS has discovered. VRT.be
[5] B. Rubin. (2019). Amazon now lets you stop human review of your Alexa recordings. Cnet.com
[6] A Ng. (2019). Amazon Alexa keeps your data with no expiration date, and shares it too. Cnet.com
[7] C. Coons. (2019). Amazon responds to Sen. Coons' concerns about consumer privacy practices for Alexa devices. Coons.senate.gov
[8] A. Burt. (2020). How will the GDPR impact machine learning? O'Reilly.com