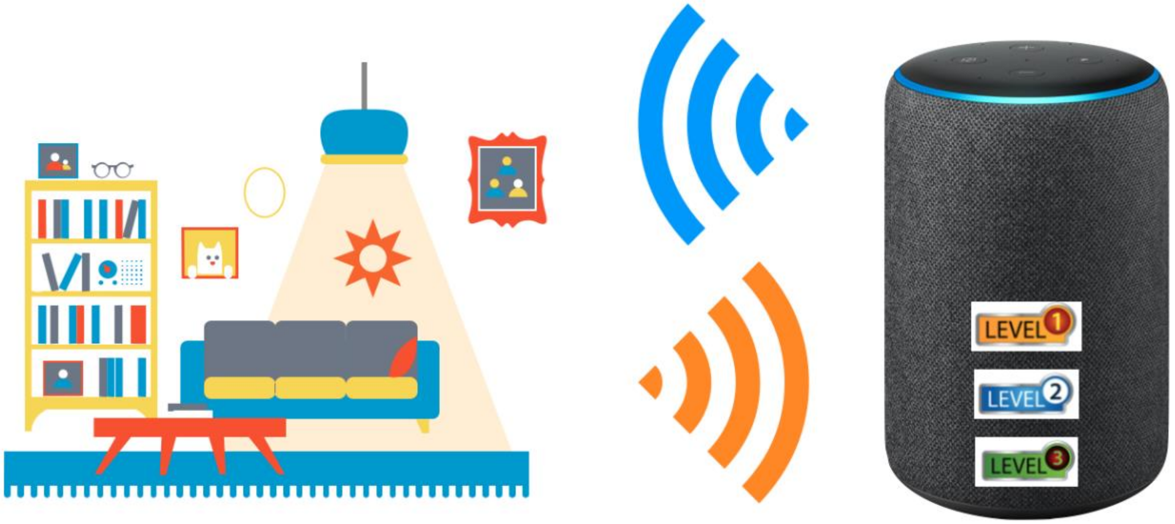
Key value tension: customer privacy v.s. Amazon data collection

Since Echo devices are supposed to respond timely, their microphones are active all the time and their processors are analyzing what the microphones receive. That alone is a little uncomfortable when people are having private conversations. That process of "identifying the trigger word" is mostly done locally so it is less a problem to most of the people. However, Echo devices can be mistriggered and sometimes even if users intentionally trigger the devices, unwanted voices might accidentally appear. In those cases, the recorded voices will be uploaded to Amazon's cloud servers, which could lead to a bigger privacy issue because recorded voices are all exposed to Amazon. Although these privacy data may help Amazon improve their services such as customized advertisements, customers' privacy also would be in the risk of being exposed because the data in Amazon Clouds may leak or hackers steal these data illegally. Customers' privacy is important because if customers' privacy is exposed to the public, their fame, mental health, and profit may be damaged.

Each and every person has to have privacy when it comes to their homes. For example, their basic personal information, their health condition, their attitudes towards different social issues, and so forth. If their privacy is exposed to the public, their personal benefits may suffer. Assuming no modifications to the current way of how Alexa operates, private conversations are prone to be recorded without explicit user permission and stored on the cloud without being completely anonymized, as each conversation could be traced back to the persons involved in.

Amazon needs more customer speech data to do further natural language processing in order to improve the user experience, quality and stability of Alexa’s responses. Sometimes, customers' speech include some personal information which can be used to identify a certain person, customer privacy may be violated without anonymity processing. Also, knowing that Amazon Echo could listen without being invoked and without notifying its user, and the people would worry more about their private conversations being exposed to Amazon.

Prototype 1: Redesigning the Echo product



The new version of Amazon Echo

Description: We plan to redesign Alexa with privacy level choices, users can set the privacy level (like range from 1 to 3, 3 means the highest privacy option) by clicking corresponding buttons manually, or using voice commands. The customer can tell Alexa which kind of room it is placed in and let Alexa determine the privacy level automatically, or just set the privacy level directly.

Three privacy levels:

- **Level 1.**
  - Low privacy: Amazon can collect the data as usual, like the old version Alexa does
  - Potential places: living room, kitchen, backyard
- **Level 2.**
  - Medium privacy: Amazon can collect dialogs the Alexa can response.
  - The procedure is that customers may occasionally wake up the Alexa, and Alexa captures dialogs of customers. However, Alexa cannot respond to these dialogs because they are not talking with Alexa. **These data will not be stored in Amazon clouds because these dialogs are more likely customers' privacy**.
  - For example, if customers make some comments about Amazon and it is possible to wake up Alexa accidently because they are likely to say some wake words in their dialogs, like Alexa, Amazon, Amazon Echo, etc.
  - In another way, if Alexa can respond to customers' words, like booking a restaurant for me, opening the light, etc. These information are less likely to be related to privacy. **These dialogs can be collected by Amazon to be analyzed and improve the customers' satisfaction and product services**.
- **Level 3.**
  - High privacy: Amazon cannot collect any data
  - Potential places: bedroom, washroom

If there are no benefits for customers when they set low level security, all customers will set high level security in any rooms. As a result, Amazon cannot collect the data for their usage.

To deal with this issue, Amazon can provide customized services according to the data collected from customers, like personal advertisements, etc. if customers set a relatively low privacy level.

Also after the customer chooses which privacy level he would like for Echo to operate on, Echo does inform the customer briefly of how data will be collected while activating this specific privacy level, and what to expect from Echo during that period, and Echo will need the customer to give it consent to begin activating this privacy level, either using a physical button or by a voice command.

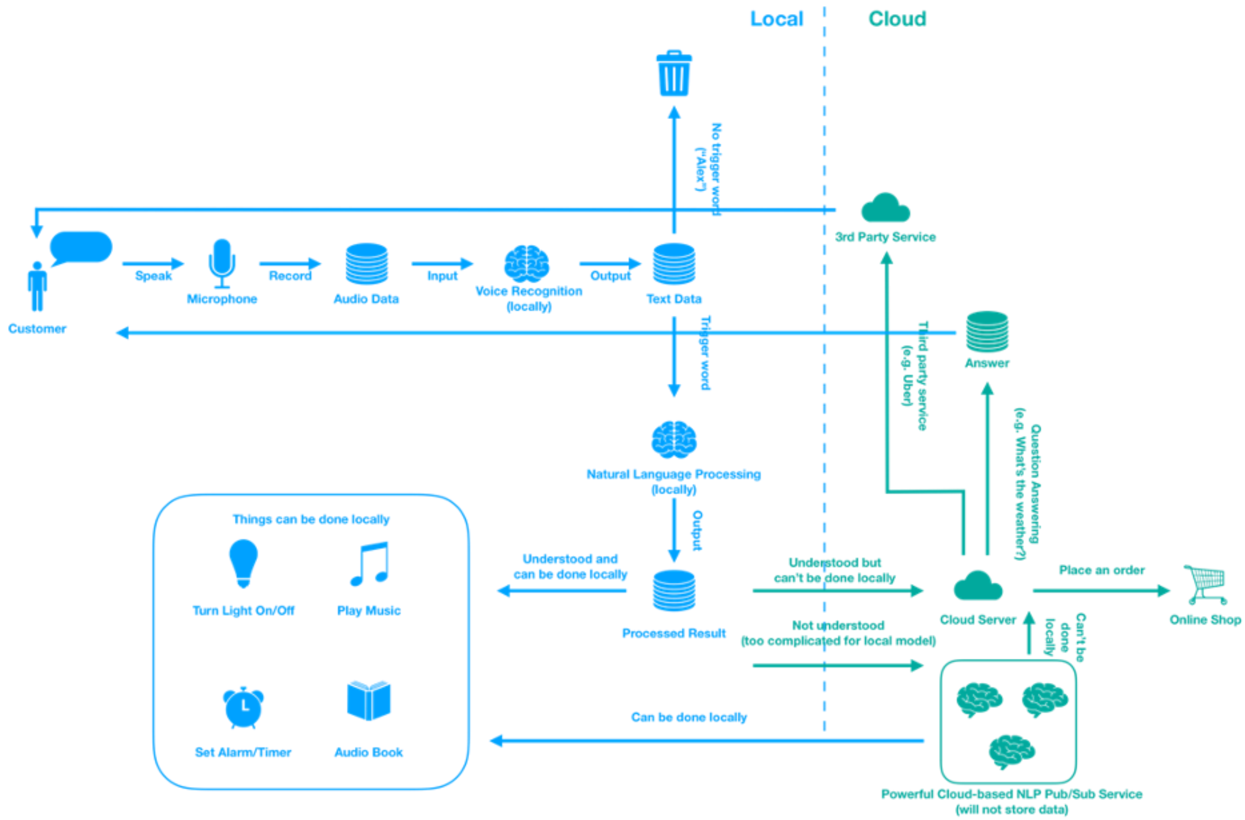
Advantages:

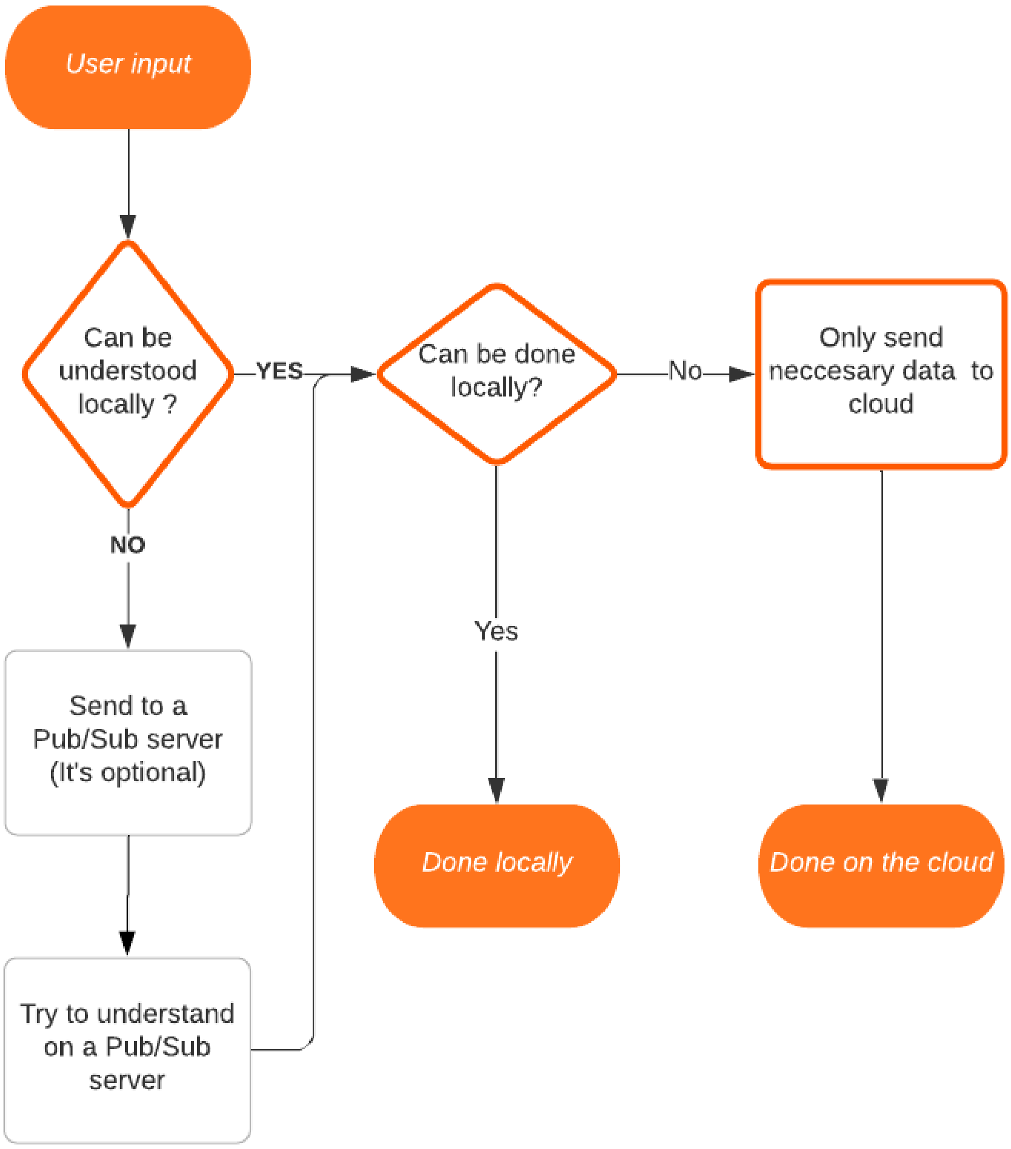
- New version Alexa has different security levels, so more privacy-sensitive in rooms, less data collection
- In a less-privacy-sensitive room, like the kitchen or living room, some data will be collected
- Amazon can use it for:
    - Fine-tuning AI algorithms
    - Enhancing user experience
    - Increase quality of service and stability of Alexa’s responses
    - Manual annotations for potential violent or offensive conversations

Disadvantages:

- Still some data will be collected by Amazon and users might not expect it for some technical reasons

Prototype 2: On-device computation in Alexa (edge-computing)




User input
Can be understood locally ?
YES
NO
Send to a Pub/Sub server (It's optional)
Try to understand on a Pub/Sub server
Can be done locally?
No
Yes
Only send neccesary data to cloud
Done locally
Done on the cloud

This prototype focuses on how to do the majority of the computation on-device.

- The process of speech recognition is done locally, and the detection of wake words is also done locally. That means no voice data will be sent to the cloud in these basic procedures.
- After the speech recognition, Echo will try to "understand" the text on the device. If successfully identifying the command, and it can do without the help of cloud servers (such as turning on/off the light), meaning it will do it without calling any cloud APIs.

- If that command cannot be processed locally (e.g. booking an order or calling an uber), the command extracted from the text(transforming from voice messages) will be sent to the cloud for further processing.
- If the text is too complicated and the local natural language processing model cannot understand it, the text will be sent to a Pub/Sub cloud service in order to understand the meaning of that text (It’s optional, if the user really cares about their privacy, it can be turned off).
- The Pub/Sub style service is a service that processes data without storing them, just generating outputs according to inputs.

Advantages:

- All unnecessary data will not be uploaded to the cloud, user privacy is protected significantly
- Part of the functions can be done locally on the device, thus will not be influenced by poor connection

Disadvantages:

- The local natural language processing model may not be as accurate as the cloud one because of the size of deep learning architectures
- If the user turns off the Pub/Sub service, the chance that Echo will fail to give any useful responses to the user is higher
- Amazon barely can collect any data, which is negative if they want to use that data to improve their quality of services and user experience

The prototype we choose finally: Prototype 1: Redesigning the Echo product

We consider the Prototype 1: Echo product redesign is better than the second prototype mainly because the first prototype can balance the values of both customers and Amazon.

The ethical factor we mainly consider is that, while the protection of customers' privacy is of high priority, we should let Amazon collect users' data when personal privacy is not violated too much.

From a customer’s point of view, this prototype protects a customer’s privacy, and gives the customer full control over how he/she wants to use Echo, and how much information should be transmitted to Amazon clouds services.

From Amazon’s point of view, this prototype let’s Amazon collect data when the information collected is relevant to either fine-tuning AI models or enhancing the user experience, as any other private information collected from the user in places like washroom or bedroom wouldn't contribute much to making Echo better, considering Echo’s current functionalities and purposes of use defined by Amazon.

Although the second prototype can protect the customers' privacy a lot more, Amazon would almost completely lose the opportunity to collect data from customers.

This has a negative impact on the improvement of the product’s services and user experience over time, which should be an iterative process that happens frequently from time to time.