ChatBot Questions Doc

Please enter your questions below for the ChatBot project. You can see the full design doc here. Enter your name with your question.

Ops

(Person1) If our service goes down, is there a way to set a default response from the bot?

- Built this in a way where we don't want this to be the case
- We will hold the incoming messages for response later
- Should think about if there's longer downtime having something
- If gateway goes down, FB will buffer for us

(Person2) Curious why you chose SQS queues. I haven't used them but I was talking with someone last week about different background options and he said that sometimes SQS can send multiple messages multiple times. Is that something we've thought about and if that happens what are options for handling that? Are there other contender options?

- When FB hits our webhook there is a unique ID so we can make sure not to handle messages more than once
- Should add FB Msg ID to the message model
- For sending? There is a small chance that we double send because of this

(Person4) Why did you choose RDS for managing conversation state? It seems like this could be very susceptible to load problems given the amount of state that is present in the DB.

- Interfaces well with Django
- Not that worried about load, only issues would be spikey traffic
- If we do consistently have high load, can shard
- We can also change number of workers servicing the SQS queue in order to throttle
- Are you using datadog to send metrics? Yes

User Conversations

(Person2) can you talk more about the thoughts around A/B testing of the conversations, specifically how that will work?

- Designing around the idea of having a state tree
- Every tree has a root
- Could have multiple roots and have different sets of people go through them
- Collect metrics, construct funnels and compare
- Each flow would be identifiable separately in data? Yes

(Person2) how does a conversation get initiated for the first time with a new constituent?

- Click on a link
- The bot wouldn't reach out to me? No, for FB need to opt in
- Opting in in facebook or somewhere else? Click on a link somewhere, takes you to FB
- Majority of people would come through ads on FB

(Person5) How do we plan on getting the relevant data from photos of drivers' licenses? Some automated OCR service or human agents?

- At first it'll be people
- Would like to use OCR
- Gerard and Bruno looked into this, talked to people who built an app that reads barcodes and decodes

(Person6) How do we handle free-form input from a constituent when the last message sent from the ChatBot had a menu? How does that affect the state machine?

- Parsing/regexes
- If we can't understand, we'll flag it as needing response from an agent
- Do they change state? No would stay in same place, agent would have an opportunity to respond

(Person6) How do we handle media other than written text? What if a constituent sends a sticker? Does the agent see a photo of the sticker? (It'd be awesome if agents / the bot could send stickers; makes it feel real and native.)

- Images and Video already works
- Don't know how stickers work yet
- Limited to type? On mobile yes, on desktop can send whatever
- Security: having agents looking at media
- Need to involve security in showing media
- Objectionable content: will probably receive this
- Should have ability to block people, and make this process quickly
- Should also have the ability to report things that the secret service etc

Agent access

- Need to figure this out
- Would restrict who can be an agent

(Person7) In the case where an automated reply is not available, is there any affordance for observing agents to prevent inaccurate or malicious information from being given to a user?

- Trusting agents
- Will also give guidance about what they can answer and/or preset answers

Machine learning

(Person7) Automating more responses could help with scaling. What is the mechanism by which we automate more conversations? Will there be a way to analyze past conversations in aggregate? (Also useful for measuring efficacy)

- Word counts for previous conversation histories
- All the conversations will be in RDS
- Should do this ahead of time
- Iteration: we'll get people in the team to test and figure

(Person8) Do we want to allow agents to classify user input we couldn't understand from the start in order to be able to make it easier to improve our regexes and possibly machine learn a model?

- Yes!
- Also everything is in RDS so we could pull it separately and provide a separate interface for classifying (interns!)

What about using out of the box things like Wit.AI?

- Person9 has looked at it and it wasn't that helpful for this usecase

Data Model

(Person4) What is your data model for conversations? I'm referring to the conversation itself, not the state/meta data.

- Have a conversation model around metadata that stores the sender id/userid
- Conversation owns the messages – in design doc
- Can we not use JSON fields and create columns instead? No, because the number of options we send is unbounded
- We're going to have to sync, this will be expensive to parse

(Person10) Why split first name and last name?

- That's what we get from Facebook
- We confirm your name in the conversation flow

Security

(Person11) Is the viable threat surface:

1. Facebook Auth
2. Potentially spamming all contacts
3. Slamming 3rd party APIs (also who's apis are you using? May i suggest VIP)

- How do we know FB is sending the message? FB sends an encrypted key
- If people hijacked this (got the API key, compromised the agent portal)? Could sent a message to everyone who's talked to us
- 3rd party APIs? DNC, Facebook, S3, Slack (incoming only)

(Person11) define "sanitization" of input. Are we just ascii'ing all the strings and dropping bad chars?

- Followup: We will run sanitization by Person11
- Need to support emojii
- Want to protect against