1. INTRODUCTION

Voice assistants are software programs that are designed to respond to voice commands and perform certain tasks. They are often used in smartphones and other devices to help users access information, control their device's settings, and perform various other tasks. These programs are designed to understand natural language and respond to spoken commands in order to perform tasks such as setting reminders, providing information, and controlling smart home devices.

These voice assistants can be useful in many different ways. They can help us to quickly and easily access information, control our devices, and perform various tasks without having to use our hands. For example, we can use voice assistants to look up information on the internet, set reminders and alarms, control our music and other media, and even control smart home devices such as lights, thermostats, and security cameras. In this way, voice assistants can make our lives easier and more convenient by allowing us to access information and control our devices more easily.

Although voice assistants can be very useful and convenient, there are also some potential dangers to consider. One potential danger is that a voice assistant can potentially be used to access sensitive information or to control devices without the user's knowledge or consent. For example, a malicious actor could potentially use a voice assistant to access a user's personal information or to control their smart home devices without their permission. Additionally, voice assistants can sometimes misunderstand commands or provide inaccurate information, which could lead to problems or dangerous situations.

The voice assistants can also be potentially used to profile users based on the information they collect. *User profiling* is the process of creating a profile of a user based on information that has been collected about them. This information can include a wide range of data, such as demographic information, behaviors and habits, interests, and personal preferences. User profiling is often used for various purposes, such as targeted advertising, personalization of services, and market research. It can be performed by companies, organizations, and even individuals, and can be based on data collected from various sources, including online activity, purchases, and interactions with digital platforms. For example, a voice assistant may collect information about the user's voice, the commands they give, and the information they access. This information can be used to create a profile of the user, which could potentially be used for advertising or other purposes. Additionally, voice assistants may collect information about the user's location, device usage, and other factors, which could also be used to create a profile of the user. It is important for users to be aware of this potential for profiling and to carefully consider the privacy implications of using voice assistants.

2. RESEARCH QUESTIONS

LINK TO WEEKLY UPDATES: HERE

2.1 PROJECT IDEOLOGY AND GOALS

In this project, our main aim is to investigate and answer the following questions::

- Do voice assistant interactions lead to user profiling?
- When and how do these profiling activities happen?
- Are the said activities been disclosed on the privacy policies of the devices?
- What are the risks associated with such profiling?

2.2 FOCUS TECHNOLOGIES

For this project, we were focusing on the leading voice assistant technologies namely *Apple Siri, Google Voice Assistant,* and *Amazon Alexa.*

Amazon Alexa is a virtual assistant developed by Amazon. It is a voice-controlled assistant that is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, and providing weather, traffic, and other real-time information. Alexa can also control a wide range of smart home devices, such as lights, thermostats, and security cameras. Alexa is available on a wide range of devices, including Amazon's Echo and Echo Dot speakers, as well as other devices such as smartphones and tablets. Users can interact with Alexa by using voice commands to ask questions, give commands, and access information.

Apple Siri is a virtual assistant developed by Apple Inc. It is a voice-controlled assistant that is capable of voice interaction, music playback, making to-do lists, setting alarms, and providing weather, traffic, and other real-time information. Siri is available on Apple devices such as the iPhone, iPad, and iPod Touch, as well as the Apple Watch and HomePod. Users can interact with Siri by using voice commands to ask questions, give commands, and access information. Siri is designed to understand natural language and respond to spoken commands, and it can also perform tasks such as sending messages, making phone calls and controlling other devices and services.

Google Voice Assistant is a virtual assistant developed by Google. It is a voice-controlled assistant that is capable of voice interaction, music playback, making to-do lists, setting alarms, and providing weather, traffic, and other real-time information. Google Voice Assistant is available on a wide range of devices, including smartphones, tablets, and smart speakers. It can also be used to control a variety of other devices and services, such as smart home appliances and media streaming devices. Users can interact with Google Voice Assistant by using voice commands to ask questions, give commands, and access information. It is designed to understand natural language and respond to spoken commands in order to perform tasks such as setting reminders, providing information, and controlling other devices and services.

3. RESEARCH METHODOLOGY

3.1 ANALYSING DISCLOSURE OF INFORMATION COLLECTED BY VOICE ASSISTANTS IN THE PRIVACY POLICIES

3.1.1 AMAZON ALEXA

- According to the privacy policy explanation, amazon uses this page to explain how they collect and use information: Click Here
- A detailed analysis of their privacy policy can be found HERE

1. ***Information user provides the platform***

2. ***Automatic Information:*** *"cookies" and other unique identifiers, and we obtain certain types of information when your web browser or device accesses Amazon Services and other content served by or on behalf of Amazon on other websites.*

3. ***Information from other sources:*** *such as updated delivery and address information from our carriers,*

- **Purpose -** Among other things, Amazon mentions they use info collected to comply with legal obligations.
    1) ***Comply with legal obligations.*** *In certain cases, we collect and use your personal information to comply with laws. For instance, we collect from sellers information regarding the place of establishment and bank account information for identity verification and other purposes.* (This information might be used to set pricing for a particular demographic area)

    2) ***Fraud Prevention and Credit Risks.*** *We use personal information to prevent and detect fraud and abuse in order to protect the security of our customers, Amazon, and others. We may also use scoring methods to assess and manage credit risks.*

3.1.2 GOOGLE VOICE ASSISTANT

Link to google's privacy policies

Google collects information about user activity in their services, which they use to do things like recommend a YouTube video that the user might like. The activity information that google collects may include:

- Terms that users search for and videos watched, Views and interactions with content and ads, Voice and audio information, Purchase activity, People with whom users communicate or share content, Activity on third-party sites and apps that use their services, Chrome browsing history that users have synced with your Google Account. If the user uses their services to make and receive calls or send and receive messages, they may collect call and message log information like phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information and types and volumes of calls and messages.
- Identifiers - name, number, address, and unique identifiers tied to browser/app/device.
- Demographic information - age, gender, and language.
- Commercial information - payment info, history of purchases made on Google services.
- Biometric information(like fingerprints)
- Internet, network, other activity information - Search terms, views/interactions with content & ads, chrome browsing history that is synced with google account, information about app/browser/device interactions (IP address, crash reports, system activity), activity on 3rd party sites & apps that use Google services.
- Geolocation data - GPS, IP address, and other data from sensors on/around the device, depending in part on your device and account settings
- Audio, electronic, visual, and similar information, such as voice and audio information.
- Professional, employment, and education status.

3.1.3 SUMMARY

Overall, as we can see from the documentation provided on these platforms, the privacy policies mentioned on these platforms are vague and hard to find as well as comprehend. There is no to very little distinction provided for the information collected by the entire platform versus just the voice assistant. While they do mention that they might use data shared by third parties with them to provide better personalization, there are very blurry boundaries for data sharing with these third-party platforms which is a serious concern

regarding profiling on these platforms. There is no clear documentation that prevents them from refraining from cross-platform exchanges of PII.

3.2 CURATING A LIST OF QUESTIONS FOR THE VOICE ASSISTANTS

After analysis of the privacy policies and taking a deep dive into the publicly disclosed categories that are used to profile users, the next step was to generate a list of questions that could be answered by the voice assistants and would be useful for supporting the main focus of the project. There were various criteria that needed to be looked into while curating this list.

Firstly, we investigated the type of questions that could directly be answered by the platforms without the need for the installation of third-party skills. This could be analyzed by interacting with the voice assistants and checking their home setup application for external (third-party) applications. Questions like "*Alexa, turn on the light*" or *"Alexa, set the heat to low in my car"* require additional skills to help execute the user request. After performing this experiment, we were able to come up with a list of questions that were independent of additional skills and could be used for the VAs using a routine setup.

Secondly, we wanted to segregate the type of questions that can be answered by the voice assistants without being connected to a phone interface and the type of questions that required a setup of a phone interface for productive usage. According to our analysis, Siri and Alexa require maximum support from the phone environment to be able to execute most of the user requests but are able to answer *"What, Who, Why"* questions that require a basic web search. It can provide almost all information once the setup is integrated with a phone interface and the requested data can be *"sent to phone"*. Certain questions like *"Send a text to my mom"* requires the setup of the user's voice so that the voice assistant can identify who the person is as well as set up relationship categories. The Google voice assistant was the most usable without a phone interface as it comes integrated with the android environment and presumably allows the exchange of data between platforms without extensive setup. While investing this criterion, we realized that although this segregation was necessary, it was more important to be able to replicate the real-life setup of voice assistants which are usually used in conjunction with phones and/or other smart devices.

Thirdly, an additional filter was added to recognize the questions that were meaningful to the event of profiling. Although voice assistants can be used to answer any type of question and perform other helpful everyday tasks, it was interesting to investigate queries like "*Recommend a shampoo for me*", "*Recommend a restaurant for dinner of two*" or "*Add item to my shopping list*" and analyze the results/ product recommendations returned by the voice assistants for the user than looking into queries like "*Set an alarm for 7.00 am*" or *"Play Yellow by Coldplay"*. Although, another line of thought for future work can be to investigate how and if the routines, user habits, and interests recorded by the voice assistants are used to profile users (for instance, early risers versus late risers).

3.3 IDENTIFICATION OF TARGET TAGS

3.3.1 DISCLOSED TAGS ON AMAZON

Before researching profiling trends, we wanted to identify the sensitive tags that we would use to give direction to our project. In order to achieve this goal, we had to research the disclosed categories on the various platforms.

Amazon used Interest Based Ads referred to as personalized or targeted ads. They show interest-based ads to display features, products, and services that might be of interest to users. They follow the Self-Regulatory Principles for Online Behavioral Advertising developed by the Digital Advertising Alliance. Information used to show interest-based ads -

1. Interactions with Amazon sites, content, and services.
2. Do NOT use identifying information - name, email
3. Cookies, pixels

Amazon works with third parties, such as advertisers, publishers, social media networks, search engines, ad-serving companies, and advertising companies working on their behalf, to improve the relevance of ads. In providing users with interest-based ads they do not associate their interactions on unaffiliated sites with information that on its own identifies the user, such as name or email address, and Amazon does not provide any such information to advertisers or to third-party sites that display their interest-based ads. Advertisers and other third parties may **assume** that users who interact with or click on an interest-based ad or content are part of the group that the ad or content is directed towards (for example, users in a particular **geographical area** or users who purchased or browsed for **classical music**). Some third parties may **provide** Amazon **pseudonymized information about the user** (such as **demographic information** or sites where you have been shown ads) from offline and online sources that we may use to provide you with more relevant and useful advertising. Third-party advertisers or advertising companies working on their behalf sometimes use cookies in the process of delivering content, including ads, directly to the user's browser or device, and **they may automatically receive an IP address when this happens**. Amazon does not provide readily available information they collect on users and one must request Amazon to provide the information collected by the platform which takes about 30 days to be sent over by the company per data request.

AUDIENCE TARGETING METHODS ON AMAZON DSP

Amazon DSP (Demand Side Platform) is a dynamic, programmatic advertising tool that uses AI and automation to discover niche audiences and serve audiences with relevant ads at the right time. Amazon's DSP allows higher capabilities, including audience insights,

customizations, and advanced automation. The opportunity to buy audio ads, display ads, and video ads on both Amazon and off-site also makes this tool a worthwhile investment.

- ***Behavioral Targeting:*** Focuses on customers who have carried out specific activities (like browsing your category over the past 30 days or clicking a specific listing). Advertisers often use behavioral targeting to generate more awareness.

- ***Lifestyle Targeting****:* Shows ads to relevant people who habitually buy from a particular category. Lifestyle targeting will concentrate on customers who are similar to your existing ones or interested in brand-relevant categories.

- ***Demographic Targeting*****:** Refers to targeting based on age, gender, yearly income, or location. Best for top-of-funnel/awareness stage.

- ***Device Targeting***: Advertisers can target ads to specific device users like Android or Apple phones, desktop users, etc.

- ***In-market Targeting:*** In-market defines people in the market for specific products or services. It is a more refined version of lifestyle targeting.

- ***Contextual Targeting****:* Advertisers can choose to display ads to audiences based on the user's browsing behavior.

- ***Remarketing***: remarketing targets consumers who were close to purchasing a product or competitive product. In most cases, these customers abandoned their basket or added a product to a wish list. There are many types of remarketing targets available:

    - ***Pixel-Based Remarketing*** re-targets shoppers on Amazon who visited your brand's website.
    - ***ASIN Remarketing*** re-targets shoppers who viewed your product on Amazon but didn't complete a purchase.
    - ***Purchased ASIN Remarketing*** re-targets shoppers who bought one of your products previously.
    - ***Brand Halo Remarketing*** targets shoppers who viewed other products from your brand.
    - ***Similar Product Remarketing*** re-targets shoppers browsing similar products to yours.

- ***Audience Lookalike:*** Targets customers who share similarities with your current customers.
- ***Advertiser Audiences****:* Uses third-party data as well as Amazon data.

3.3.2 DISCLOSED TAGS ON GOOGLE

Google uses *Audience Targeting* where audiences are made up of segments or groups of people with specific **interests, intents, and demographic** information, as **estimated** by Google. Users are allocated into audience categories for targeting on third-party websites and apps based primarily on their activity on third-party websites and apps. Users are allocated into audience categories for targeting on Google's own products based primarily on their activity on these products. Google has audience segment types to use for targeting the given audience

- ***Affinity -*** Reach users based on what they're passionate about and their habits and interests.

Custom segment inputs

Reach people based on	Inputs	Audience type
Interest or behaviors	Keywords	Enter interests, in the form of keywords or phrases, that represent your ideal customer. Your ads will reach people likely to be interested in or with purchase intent for your keywords based on their behavior and activities, such as apps they use or the type of content they browse or search for online. When you enter interests or behaviors, you have a choice of how Google should interpret the inputs. • People with any of these interests or purchase intentions (This is the default) • People who searched for any of these terms on Google properties (such as Google.com and YouTube). Only on campaigns running on Google properties. On other campaigns, they will be used as interests or purchase intentions.
People who browse websites similar to	URLs	Enter website addresses (URLs) that your ideal customer might visit. Your ads will reach people who browse websites similar to the URLs you enter. **Note**: This doesn't mean your ads will show on those URLs.
People who use apps similar to	Apps	Enter the names of apps that you think your ideal customer might use. Your ads will reach people who download and use apps similar to the ones you enter. **Note:** This doesn't mean that your ads will show on those apps.

- ***Detailed Demographics***: Reach users based on long-term life facts.
- ***Life Events*:** Reach users when they are in the midst of important life milestones.
- ***In-market:*** Reach users based on their recent purchase intent.
- ***Your data segments:*** Reach users that have interacted with your business.

- ***Website and app visitors****:* Reach people who have visited your website and/or apps.
- ***Customer Match****:* Reach your existing customers based on your CRM data.
- ***Similar segments***: Reach new users with similar interests to your website visitors or existing customers

It was interesting to observe how Google provides extensive CSVs for *In-market segments, Affinity categories*, and *Detailed demographics*. While they provided categories and subcategories on multiple interest topics they do not dive deep into categories like *"Dating Services"* which appears as the only single entry without subcategorization in their in-market CSV and raises questions on what kind of data is collected under this interest category when they claim they do not collect/ use the information to identify someone's sexual orientation which is directly related to this category.

246	/Consumer Electronics/Game Consoles/Sony PlayStation	YES	YES	YES	YES	NO	YES
247	/Consumer Electronics/Game Consoles/Xbox	YES	YES	YES	YES	NO	YES
248	/Consumer Electronics/Home Theater Systems	YES	YES	YES	YES	NO	YES
249	/Consumer Electronics/Mobile Phone Accessories	YES	YES	NO	YES	NO	YES
250	/Consumer Electronics/Mobile Phones	YES	YES	YES	YES	NO	YES
251	/Consumer Electronics/Mobile Phones/Android Phones	NO	NO	YES	YES	NO	YES
252	/Consumer Electronics/Mobile Phones/iOS Phones	NO	NO	YES	YES	NO	YES
253	/Consumer Electronics/Power Adapters & Chargers	NO	YES	NO	NO	NO	YES
254	/Consumer Electronics/Televisions	YES	YES	YES	YES	NO	YES
255	/Dating Services	YES	YES	YES	YES	NO	YES
256	/Education	YES	YES	YES	YES	NO	YES
257	/Education/Foreign Language Study	YES	YES	YES	YES	NO	YES
258	/Education/Post-Secondary Education	YES	YES	YES	YES	NO	YES
259	/Education/Post-Secondary Education/Arts & Design Education	YES	YES	YES	YES	NO	YES
260	/Education/Post-Secondary Education/Business Education	YES	YES	YES	YES	NO	YES
261	/Education/Post-Secondary Education/Cosmetology Education & Training	YES	YES	YES	YES	NO	YES
262	/Education/Post-Secondary Education/Health Care Education	NO	NO	NO	YES	NO	YES
263	/Education/Post-Secondary Education/Health Care Education/Nursing Education	NO	NO	NO	YES	NO	YES
264	/Education/Post-Secondary Education/Technology Education	YES	YES	YES	YES	NO	YES
265	/Education/Primary & Secondary Schools (K-12)	YES	YES	YES	YES	NO	YES
266	/Education/Study Abroad Programs	YES	YES	YES	YES	NO	YES
267	/Education/Test Preparation & Tutoring	YES	YES	YES	YES	NO	YES
268	/Employment	YES	YES	YES	YES	NO	YES
269	/Employment/Accounting & Finance Jobs	YES	YES	YES	YES	NO	YES
270	/Employment/Career Consulting Services	YES	YES	YES	YES	NO	YES
271	/Employment/Clerical & Administrative Jobs	YES	YES	YES	YES	NO	YES
272	/Employment/Education Jobs	YES	YES	YES	YES	NO	YES

It was also of intrigue for us to look into the *"News & Politics"* category in the affinity_categories CSV which further lead us to question what kind of profiling can be done based on the political interests of a user and does that lead the algorithm to expose the user to biased information on the topic. For instance, does the google news feed or youtube recommendations get affected by someone's political inclination, and if that can be used to further drive them to the other extreme of the category? The category *"Luxury Shoppers"* was another point of interest as we wanted to investigate if there was a distinction in the recommendation of products and results based on someone's income status inferred by the algorithm.

/Media & Entertainment/TV Lovers/Documentary & NOnfiction TV Fans	YES	YES	YES	YES	NO	YES
/Media & Entertainment/TV Lovers/Family Television Fans	YES	YES	YES	YES	NO	YES
/Media & Entertainment/TV Lovers/Game, Reality & Talk Show Fans	YES	YES	YES	YES	NO	YES
/Media & Entertainment/TV Lovers/Sci-Fi & Fantasy TV Fans	YES	YES	YES	YES	NO	YES
/Media & Entertainment/TV Lovers/TV Comedy Fans	YES	YES	YES	YES	NO	YES
/Media & Entertainment/TV Lovers/TV Drama Fans	YES	YES	YES	YES	NO	YES
/News & Politics	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers/Avid Business News Readers	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers/Avid Local News Readers	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers/Avid Political News Readers	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers/Avid World News Readers	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers/Entertainment News Enthusiasts	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers/Men's Media Fans	YES	YES	YES	YES	NO	YES
/News & Politics/Avid News Readers/Women's Media Fans	YES	YES	YES	YES	NO	YES
/Shoppers	YES	YES	YES	YES	NO	YES
/Shoppers/Bargain Hunters	YES	YES	YES	YES	NO	YES
/Shoppers/Luxury Shoppers	YES	YES	YES	YES	NO	YES
/Shoppers/Shopaholics	YES	YES	YES	YES	NO	YES
/Shoppers/Shoppers by Store Type	YES	YES	YES	NO	NO	YES
/Shoppers/Shoppers by Store Type/Convenience Store Shoppers	YES	YES	YES	NO	NO	YES
/Shoppers/Shoppers by Store Type/Department Store Shoppers	YES	YES	YES	NO	NO	YES
/Shoppers/Shoppers by Store Type/Grocery Shoppers	NO	YES	YES	NO	NO	YES
/Shoppers/Shoppers by Store Type/Superstore Shoppers	YES	YES	YES	NO	NO	YES
/Shoppers/Value Shoppers	YES	YES	YES	YES	NO	YES
/Sports & Fitness	YES	YES	YES	YES	NO	YES

The detailed-demographics CSV provided vague sub-categorization on the collection of information on the *"Homeownership Status"*, *"Marital Status"*, and *"Parental Status"* of the user. Noticing the inconsistencies in the full disclosure of categories in previous data by Google, we presume that there is further subcategorization of these categories which is not available in these documents.

	A	B	C	D	E	F	G
11	/Employment/Company Size/Small Employer (1-249 Employees)	NO	YES	YES	YES	YES	YES
12	/Employment/Company Size/Very Large Employer (10k+ Employees)	NO	YES	YES	YES	YES	YES
13	/Employment/Industry	NO	YES	YES	YES	YES	YES
14	/Employment/Industry/Construction Industry	NO	YES	YES	YES	YES	YES
15	/Employment/Industry/Education Sector	NO	YES	YES	YES	YES	YES
16	/Employment/Industry/Financial Industry	NO	YES	YES	YES	YES	YES
17	/Employment/Industry/Healthcare Industry	NO	YES	YES	YES	YES	YES
18	/Employment/Industry/Hospitality Industry	NO	YES	YES	YES	YES	YES
19	/Employment/Industry/Manufacturing Industry	NO	YES	YES	YES	YES	YES
20	/Employment/Industry/Real Estate Industry	NO	YES	YES	YES	YES	YES
21	/Employment/Industry/TechNOlogy Industry	NO	YES	YES	YES	YES	YES
22	/Homeownership Status	NO	YES	YES	YES	YES	YES
23	/Homeownership Status/Homeowners	NO	YES	YES	YES	YES	YES
24	/Homeownership Status/Renters	NO	YES	YES	YES	YES	YES
25	/Marital Status	NO	YES	YES	YES	YES	YES
26	/Marital Status/In a Relationship	NO	YES	YES	YES	YES	YES
27	/Marital Status/Married	NO	YES	YES	YES	YES	YES
28	/Marital Status/Single	NO	YES	YES	YES	YES	YES
29	/Parental Status	NO	YES	YES	YES	YES	YES
30	/Parental Status/Parents	NO	YES	YES	YES	YES	YES
31	/Parental Status/Parents/Parents of Grade-Schoolers (6-12 years)	NO	YES	YES	YES	YES	YES
32	/Parental Status/Parents/Parents of Infants (0-1 years)	NO	YES	YES	YES	YES	YES
33	/Parental Status/Parents/Parents of Preschoolers (4-5 years)	NO	YES	YES	YES	YES	YES
34	/Parental Status/Parents/Parents of Teens (13-17 years)	NO	YES	YES	YES	YES	YES
35	/Parental Status/Parents/Parents of Toddlers (1-3 years)	NO	YES	YES	YES	YES	YES
36							
37							

Furthermore, in the previous version of the Google interface, if we wanted to look into our personal tags on the platform, one could navigate to

Manage your Google account ➡️ Data and Privacy ➡️ Your information

and this would display an extensive list of tags the algorithm thinks you are interested in. An example of the deluge of tags can be found in my personal tags document on google (some tags have been removed from this document in the interest of privacy).
NOTE: the major part of this project was done using the old interface of this google page.

In the new interface, this page has been reconfigured to lead the users to their personalized ads category which displays the *Gender, Age,* and *Location* as provided by the user upon account creation as well as *"Categories used to show you ads"* with *relationships, household income, industry, education, employer size, homeownership* and *parenting* tags listed within it. Another feature of this new update is that the user can manually go in and change the assumption made by the algorithm in case it has been inferred incorrectly in the system.

Manage your Google account ➡️ Data and Privacy ➡️ Personalized ads ➡️ My ad center

3.3.3 INTEREST TAGS FOR THE RESEARCH

Due to the constrained time frame, we decided to focus our research on the Google platform as it was the easier and almost immediate observation of the categorization of users on the platform. In order to perform experimentation, we needed to narrow our focus to the following tags:

- ***Household income -*** to analyze differences in the recommendations of products, google news feed, youtube recommendations as well as targeted advertisements on all of the above platforms based on the inferred income level of the user.
- ***Gender / Sexual Orientation -*** to make distinctions in search results based on the inferred gender / sexual orientation of the user. An interesting research question was to observe if there was enough inferring information that can be gathered from the search results of the VA which could prove our hypothesis that the platform indeed does collect and categorize users based on their dating life (sexual preference) which is enlisted as a *"sensitive"* category on google. Another trend we wanted to zero in on was whether recommendations and search results are biased based on gender and if yes, how they could be potentially used other than for purposes of targeted advertisements.
- ***Relationship Status*** - to analyze what assumptions are made by the platform depending on the relationship status of the user. It again closely ties into the sexual orientation interest question. We wanted to look into what inferences are made based on the searches performed by the user. For instance, "*Book a table for two*" or "*Plan a trip to Mexico*" could be used to infer if the user is

single, engaged, or married. It also closely ties into the *parental status* tag of the user.

Overall, we also wanted to observe the compounding effects of tags like demographics, interests, industry, parenting, homeownership, etc on these categories as we presume that inference about categorizing a user to fit a box in the above-mentioned categories comes from a lot of assumptions made by the algorithm based on the usage by the user.

3.4 GENERATING INTEREST PERSONAS

Keeping our interest tags in mind, we decided to experiment with two personas revolving heavily around income categorization on the platform. In order to perform successful experimentation on the same, we needed to come up with a list of questions that could be used to train the algorithm based on the persona.

3.4.1 INTEREST PERSONAS FOR THE EXPERIMENT

We wanted to observe trends of profiling for users coming from different income backgrounds. Therefore, we created two personas - the *luxury* persona and the *Common* persona.

The characteristics of the *luxury* persona we had in mind before starting experimentation were:-

- Age: 42 years
- Gender: Female
- Income: High-income
- Marital Status: Single
- Demographics: United States

The characteristics of the *common* persona we had in mind before starting experimentation were:-

- Age: 22 years
- Gender: Male
- Income: Middle-income
- Marital Status: Single
- Demographics: Asia

There were some general assumption questions curated for the personas based on age groups and characteristics.

3.4.2 QUESTIONS FOR INTEREST PERSONAS

In order to generate training questions, the first step was to correctly identify the probing questions for the experiment. Probing questions were a list of neutral questions that should not in theory produce a biased result or tag if asked on a freshly created platform.

Questions like *"Recommend a watch", "Recommend good skin care products", "Apartments in Boston"*, etc. should generate results that are unbiased. For the two personas, we were trying to investigate - *Luxury* and *Common* - the training questions would be more targeted at the persona in question. For instance, the luxury persona may ask the voice assistant "*Show me deals on Rolex/ Garmin*" while the common persona may query "*Show me deals on budget-friendly watches/Fitbit*".

The ideology was to first observe the recommendations on probing questions. After that, every persona must be trained using the training questions (observe the change in tags). This should be followed up with retesting queries using probing questions to observe distinctions in recommendations for the different personas.

3.4.3 SETUP FOR THE EXPERIMENTATION

In order to minimize contamination, all queries for the personas were made on freshly generated accounts. Also while creating new accounts, we refrained from specifying the gender and income status of the user but did provide the date of birth and location of the user. Click on *"Prefer not to say"* for both the prompted questions for income and gender while creating accounts.

Probing questions were tested on a blank account with no searches. New accounts were made for the luxury and common personas as well and only training questions were initially used for the searches. Moreover, all questions asked were using the voice assistant and not through a direct google search. We also made accounts in Amazon using the same user id for google so both accounts are associated with the respective persona. Searches were made over a period of 1.5 weeks to train the luxury and the common persona using the training questions. The probing questions were queried on the profiles following the training period.

In order to observe changes in tags, we created new accounts for luxury and common personas separate from the ones previously created following the same specification. After using training questions on the profiles for the given time period, we conducted experiments to see if we could change the assigned tags by the algorithms, for instance, if we wanted to change the income tag from a high-income to a low-income tag. We needed to make dedicated searches with the accounts for at least three-four days to observe changes in tags.

3.5 EXPERIMENTATION FINDINGS

Some general assumptions are made by Google as soon as one creates an account based on voluntary information provided by the user. For instance, we observed tags of *marital status* pop up on the tags page upon account creation based on the age provided by the user. For the age group of 18- 24 years, the algorithm sets the tag to *Single* while for a higher age group(35-44 years) it sets the tag to *Married.* Also, if you use the id to create a business/ sellers page, it automatically assumes the gender of the user to be *Male* in the absence of other searches.

Analyzing the results on the probing account: When making queries using a voice assistant on a freshly created platform with zero searches, the recommendations and results returned were uninteresting and did not suggest any particular tags of interest. Some of the results returned were consistent with what I would personally get on my own voice assistant suggesting contamination. An example of this would be "*Recommend a protein powder for gym*" which returned the search result of the supplement I use and buy routinely. Also, no special tags were generated while querying the probing questions other than the *income tag* "*Average or lower income"* and accessory unlabeled interest tags.

Analyzing the results on the Luxury persona: While making queries using the training questions of the Luxury persona, the income tag of *"Moderately High"* household income was generated. Also, the Homeownership status tag assumed the persona was a "*Home Owner".* Although, gender neutral or a good balance of female: male-biased questions were asked to the voice assistant, the appearance of the high-income tag was accompanied by a gender assumption of *"Male"* even though certain queries included "*Show me directions to the nearest salon*" or "*Recommend the latest Rhode line for women*" which are more affiliated with a female audience. Moreover, making neutral (probing) queries like "*Find apartments in Boston*" returned search results of properties that could be bought on sites like zillow.com or "*Recommend me a shampoo*" returned high-end brands like OlaPlex for the user. Querying *"Apartments to rent in Boston"* returned search results of apartments in high-priced areas of Downtown and Back Bay.

Analyzing the results on the Common persona: While making queries using the training questions of the Common persona, the income tag of *"Average to low income"* household income was generated. Also, the Homeownership status tag assumed the persona was a "*Home Renter".* Although, gender neutral or a good balance of female: male-biased questions were asked to the voice assistant, the user was profiled as a "Female" even though searches were neutral and included queries tilted towards a male audience. Moreover, making neutral (probing) queries like "*Find apartments in Boston*" returned search results of properties that could be rented rather than bought, and "*Recommend me a shampoo*" returned brands like Dove and Neutrogena for the user. Querying *"Apartments to rent in Boston"* returned search results of apartments in areas of Dorchester and Jamaica Plain.

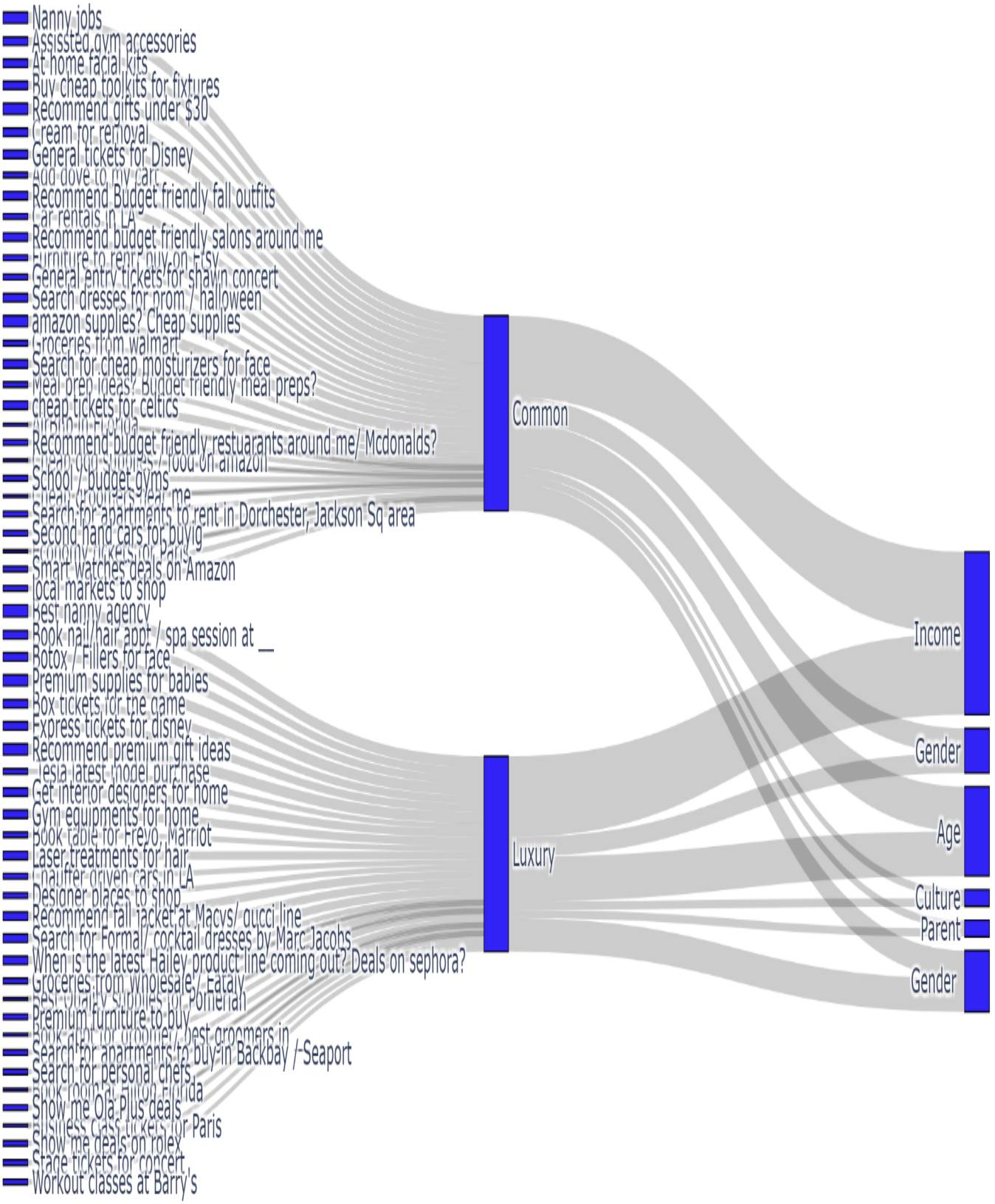
Observing the trend of results returned from the voice assistants upon the query and the tags generated for each persona was a strong indication of profiling by the algorithm based on searches done by the persona.

Analyzing the changes in tags for the personas: Experimentation performed on the persona accounts leads to the generation of tags based on the assumed characteristics of a persona. It was interesting to observe that the given tags can be changed based on dedicated searches performed by the users. The income status for the luxury persona was changed to *"average to low income"* after 3 days of dedicated searches for rental options on a budget, looking for cheap options of products, and finding budget-friendly options for most query questions. It is more tricky to change tags for gender identification and requires more time which needs to be determined with further experimentation. Another interesting observation was that if the algorithm was confused about the gender identity of the user, it completely removed the gender tag from the list of labeled tags which again might be interesting to look into in the context of the LGBTQ+ community.

SANKEY DIAGRAM

(shows the relationship between Questions, Personas, and Tags)

- Link to GitHub: Here
- Link to Code For Sankey: Here
- Link to Jupyter Notebook: Here
- Link to CSV for code: Here


Nanny jobs
Assissted gym accessories
At home facial kits
Buy cheap toolkits for fixtures
Recommend gifts under $30
Cream for removal
General tickets for Disney
Recommend Budget friendly fall outfits
Recommend budget friendly salons around me
General entry tickets for shawn concert
Search dresses for prom / halloween
amazon supplies? Cheap supplies
Search for cheap moisturizers for face
cheap tickets for celtics
Recommend budget friendly restuarants around me/ Mcdonalds?
School / budget gyms
Search for apartments to rent in Dorchester, Jackson Sq area
Second hand cars for buyig
Smart watches deals on Amazon
local markets to shop
Best nanny agency
Book nail/hair appt / spa session at _
Botox / Fillers for face
Premium supplies for babies
Box tickets for the game
Express tickets for disney
Recommend premium gift ideas
Get interior designers for home
Gym equipments for home
Laser treatments for hair
Designer places to shop
Recommend fall jacket at Macys/ gucci line
Search for Formal/ corktail dresses by Marc Jacobs
When is the latest Hailey product line coming out? Deals on sephora?
Premium furniture to buy
Search for apartments to buy in Backbay /-Seaport
Search for personal chefs
Show me Ola Plus deals
Show me deals on rolex
Stage tickets for concert
Workout classes at Barry's
Common
Luxury
Income
Gender
Age
Culture
Parent
Gender

3.6 SEPARATE DISCUSSION

In a separate experiment performed during the mid-term elections, an interesting finding was that if the user made the algorithm believe that they were more conservative than liberal, the Google News feed and YouTube recommendation for videos to watch changed based on this inference. Also, the news articles were by publishers who are publicly known to be more biased towards a certain line of thinking. This would be interesting to further investigate the exposure of the users to articles/videos based on their interests which might be dangerously skewed and fuel conflicts among different ideologies.

3.7 LIMITATIONS OF METHODOLOGY

While conducting experiments, we suspect possible contamination of our results for the project. This might be due to the linkage of all accounts to a singular mobile number and operator. We also suspect that the results could have been polluted due to the usage of the same IP address as well as the same voice assistant and laptop used during the creation and maintenance of the said accounts. The experimentation was performed only once for the personas which do not provide a reliable basis to make strong claims. Moreover, the setup and process do not provide scalability for multiple personas at this point as all searches and observations were made manually. Furthermore, all experimentation was done on the previous interface of google which is significantly different from the new interface.

In order to overcome these shortcomings, we should reconduct the experiments using completely different numbers, devices, and IP addresses for each persona to reduce the risk of contamination. Furthermore, the experiments need to be repeated multiple times with the new interface to reproduce similar results and confirm the findings to make stronger claims supporting our hypothesis. We should also investigate how we can scale our project to create and observe profiling trends on multiple personas to further solidify our findings and outcomes. Moreover, we need to perform similar experimentations with Alexa and Siri and look for trends of profiling to be able to further confirm our findings.

4. CONCLUSION

In summary, we have suggested evidence that voice assistant interactions lead to user profiling. These profiling activities can be compounded and associated with other data, for instance, basic searches on search engines, maps, reminders, and lists, maintained by the user. Overall, a lot of information can be collected by these platforms and used in conjunction with multiple platforms to infer the categorization of the users. The sensitive data collected and

inferred might be shared with less trustable third-party apps which might be used to deanonymize users and threaten their privacy. Moreover, targeted information for the users may create a bigger wedge in the knowledge and exposure of users which would not normally be the case in the absence of profiling. These profiling trends can not only be observed in product recommendations while making dedicated searches but also in advertisements on various platforms, video recommendations on platforms like YouTube, and news articles shown to different kinds of users which are prime educational tools and knowledge resources for most people today. Therefore, in the absence of well-defined laws and policies for protecting user data, information shared about the user by voice assistant interactions raises serious concerns about the privacy protection of its users.