Recommender System Trust and Safety

Khawar Murad Ahmed[1]
University of Utah, U.S.A., khawar.ahmed@utah.edu
Vishva Desai
University of Utah, U.S.A., vishva.desai@utah.edu
Thomas Greger
University of Utah, U.S.A., thomas.greger@utah.edu

Streaming and social media platforms like Netflix, YouTube, and Twitter use algorithms to make suggestions for content that the user might be interested in. They do this to keep the user engaged with the platform and keep them captive. The recommender systems use personal data that the user provided in the form of personal preferences or by previous viewings, purchases, likes, or retweets. This information is personal and may be of sensitive nature and therefore, could possibly be harmful to the user if such data were leaked. We are going to present the users' perception regarding trust and safety towards platforms that they are using.

1. Introduction

Over the past decade, as content has become easier to create, the problem of content curation for each user has become a problem that many platforms have attempted to solve. Currently, the most popular solution is using a recommendation system through personalized recommendations for each user based on their preferences. This is actively marketed as a feature by many platforms such as Netflix, Spotify, TikTok, and YouTube among many others. While personalized recommendations have made the user's life much easier by providing content to optimize the user's experience. However, there are a lot of downsides to the problem as well. The recommendation systems require a lot of data for optimal experience, amount of data which can risk de-anonymization if gotten into the wrong hands. In addition, because recommendation systems have so much control over what users see and do not see, there is also an open possibility for bias to occur.

Because of its great utility of recommending things, and also a major concern about privacy, it is clear that there is a trade-off that needs to be made with regards to the design of future personalized recommendation systems. In order to do that, user input is required with regards to the extent of trade off. The first step to learning about the trade off is getting an idea of how they view personalized recommendations in their current form. This paper will present user perception with regards to trust and safety. Specifically, the research question is as follows:

1) How do personalized recommender systems affect human behavior with respect to trust and safety according to user perception across different platforms?

In an attempt to answer that question, semi-structured interviews along with a survey were conducted. Semi-structured interviews were designed to get the user's perception with regards to their general view on personalized recommendations, and also their perceptions of platform-specific personalized recommendations. Platform-specific personalized recommendations (asking the users what they think about Spotify's recommendations and YouTube's recommendations separately) was important to inquire about because there is a chance that, for the user, what is acceptable to one user might not be important to another. Indeed, the findings showed that to be the case, which indicates that there is no singular answer to the utility to privacy trade-off, and that these decisions would differ for each use case.

2. Literature Review

Alkhatib [7] paper claims that the absurd outcomes are constantly being rewarded, and the general user perception around that (i.e.: Does the user think the recommendations they get are absurd?). This paper draws from

[1]All three authors contributed equally to this research

anthropological theories to apply them to algorithmic applications, although it does no such thing. Rather, it will use theory as an influence on data collection and interpretation. The big problem that ensues with using algorithms is that, oftentimes, absurd outcomes are rewarded. This problem also applies to recommendation systems, and is often cited as the cause of division created because everyone is fed different content based on their own personal preferences as determined by algorithm. As such, this paper provides an interesting framework through which we can examine the users' perceptions of such algorithms. It would be especially interesting to see whether the users feel that the relationship between them and recommendation systems is adversarial or friendly by nature, as this paper frames that relationship as inherently adversarial and something that hurts the user.

While Alkhatib's [7] work describes the state of the society with regards to recommendation algorithms, Seaver [9] provides a conceptual framework with regards to the primary purpose of recommendation algorithms. While we don't explicitly want to mention captivity in relation to recommendation algorithms, we do want to explore whether user perception backs up the notion of captivity. If it does, what about it makes them feel captive? This work does not speak much about user perceptions as much as it does about the primary purpose and the consequences of that purpose with regards to the material culture. Before discussing the user perceptions, it is important to mention the primary motive of the existence of recommendation systems. Seaver [9] mentions that most of the designers of recommendation systems use words like captivity and hooked. When it comes to user perception of these algorithms it is important to examine whether recommendation systems are perceived as an adversary (i.e.: something that users must fight to maintain their wellbeing) or a helper (i.e.: something that helps them sift through an extremely large catalog). How users perceive these algorithms on that high of a level will help the designers evaluate whether current metrics that help with the evaluation are accurate in terms of maximizing user trust and safety.

Mohallick et al. [5] talk about privacy risks and the tradeoffs users make with news recommender systems and how systems use interaction history and preferences for the recommendations. This ties into how users perceive security when using the system. This work places emphasis on news recommendations whereas our work is more general to include media and product recommendations. News is unstructured data and different from recommendations for media and products. This is a tangential to our work since it provides one specific trade off that we can look into when it comes to user perception. Because of the massive amount of data, users more and more rely on recommender systems for providing relevant suggestions. Specifically with news, where data is unstructured, is timely, and interests can change quickly based on for example current sport events, this has become difficult. As a result, news recommendations are a bit more tricky when it comes to implementing privacy measures. Because of the abundant information, users are relying on recommender systems making relevant suggestions for them and for this they are giving up some privacy. The system's algorithm requires this personal and perhaps sensitive information to make relevant and sustained recommendations. As stated by the authors, there is a trade off to be made if we are to examine privacy with relations to recommendation qualities (which is defined by current metrics). If this information is leaked, it could put the user in danger, if the information is of sensitive nature, like political views and sexual orientation. As the Netflix Prize dataset [17] has shown, even if anonymized, datasets allowed for re-identification, and that could put users' privacy at risk. In the context of security, privacy is a major factor. In addition, O'Donovan et. al [1] explored trust from both perspectives, how it is perceived by users, as well as what the system can do to gain user trust. Harboth et. al [6] showed that privacy literacy has a negative impact on trusting beliefs of current data collection infrastructure. There is also a more extensive survey of privacy and security with regard to recommendation systems done by Himeur et al. [13] as well.

A lot has been written about gaining the trust of users as well as looking into the ethics of algorithmic recommendations. Winoto et. al [4] explored how recommendation algorithms can influence people's personal beliefs, and stated that it is important to consider the ethical impacts of that. Milano et al. [3] identified six ethical concerns: Inappropriate content, fairness, opacity, privacy, social effects, and autonomy and personal identity. For the scope of this study, inappropriate content was not extensively considered. Sullivan et. al [16] explored whether explanations would further aid in increasing user trust, and argued for setting that as an ethical standard. This claim is further supported by Kunkel et al. [8] which focused on the impersonal nature of recommendation algorithms, and how oftentimes humans tend to trust other humans with recommendations (even if less accurate) because there is a lot more trust when the recommendation comes with context. Shang et al. [14] also found there to be a positive correlation between explanations and utility after conducting a user study on human-readable explanations for the content that was recommended. To tackle these problems, Gupta et al. [15] proposed a conversational interface that could aid with explanations for the recommendations being given. There is also a study conducted by Burbach et al.

[12] that studies the user perception of different types of algorithms (ex: collaborative filtering, content based recommendation etc.), and also found that there were users who preferred different approaches for different products. Eskandanian et al. [13] explored how few people might heavily influence collaborative filtering. [Gorgoglione et. al [2] also studied the impact of recommendation systems on consumer purchasing behavior when using context-aware recommendations compared to other methods.

While this study does not extensively focus on addiction to different platforms, it is still a subject that poses a great deal of risk to the safety and trust of the users that use these platforms. Lukoff et al. [10] explore agency and independence with respect to recommendation algorithms, and more specifically, the UI of YouTube and found that the aggressive nature of YouTube UI takes away the sense of agency a user has. As explained in Qahri-Saremi et al. [11], addiction is already a big problem, with certain personality types being more vulnerable to addiction, recommendation algorithms add a new layer because of how easy it is to find new content.

3. Methods

In order to find answers to our research question, we collected data using interviews and online surveys. The interviews and surveys used similar questions to find out what the users' perception was regarding trust and safety with regard to recommendations made by the algorithms of the platforms they were using.

3.1 Interviews

To collect the data for our study, we used interviews and an online survey study. First, we performed semi-structured interviews. Participants were recruited using convenience sampling. Six participants were recruited. The interviews were conducted using Zoom video calls. We had an observer take notes during the interviews. For record keeping, we recorded the audio with the consent of the participants. The interview had a few generic questions regarding the safety and trust of online platforms and what platform the participants were using. Then we asked specific questions regarding trust and satisfaction with the recommendation for each of the platforms the participants indicated they were using (up to three maximum).

3.1.1 Interview structure

We started the interview with a question of how the participants define personal recommender systems. For this question, we are trying to get the participant to start thinking about personalized recommendations and their workings at a high level. This is to make sure that we have a general idea of what the participant thinks of the inner workings of a personalized recommender system. Additionally, we asked the participants what platforms they were using that provide personal recommendation. Then for up to three platforms they were using, we asked them what their perception was regarding the recommendation and whether they trusted the platform. Also, we wanted to know if the personalized recommendations affected their time or money spent on the platform. For up to three platforms that the participants mentioned, we followed up with platform specific questions whether the recommendations were relevant and biased. We also asked them if they trusted the platforms with their personal information and if their personal safety would be at risk, if any of the data were leaked. We ended the interview with a general question about whether good recommendations are worth providing more personal data. This question was about trying to find out the participants' views on personal data collection and the extent to which they are comfortable sharing their personal data.

3.2 Result

During the interviews, there were a few topics that were consistently touched on several times. Before getting into the result, it is important to provide a little background on our participants. All six participants were in either undergraduate or graduate programs at the time of interviews. The platforms mentioned by our participants were streaming platforms such as Spotify and Netflix, social media such as Instagram, Youtube, and Tiktok, as well as ecommerce platforms such as Amazon. Given that, there are several prominent topics that came up that were addressed by most, if not all of the participants. Among those topics addressed was the nature of data, company size (which was a factor for both better and worse), echo chambers, as well as bias.

3.2.1 Company Size

For almost all of the participants, company size was a huge factor in determining how much they trusted each company with their data. Several participants mentioned that they would trust companies like Facebook (as referred

to by the participants) and Google with their data because of their sheer size. The participants mentioned that their trust came from the fact that these were very profitable companies that would have a robust cybersecurity infrastructure that would prevent massive leaks. This is the response of one of the participants to the question if they trusted Amazon:

> “I would say, yeah, i'd trust them just because it's a big enough company that, like, you know, with any kind of company that's going to fail, like or not fail, but be like as big as they are, They could be kind of, what's the term for it? They are more or less liable for some sort of security breach, possibly. So, but the data that I have on it is just be like debit card info. Not necessarily anything where anybody could steal my identity, I don't think.”

On the flipside, several participants were not at ease with the amount of data conglomerates like Google and Facebook (as referred to by the participants) had on them, and did not trust them. This is what one of the participants answered to a question regarding what type of data they would like to keep private:

> “I'd say for the most part, I value like data privacy. In terms of different things like my current location being shared with, you know, other entities um like my address, birthday, you know, stuff like that that kind of, I'm required to put in for you know security and privacy reasons, you know, I would assume that if that's the case, that it shouldn't be shared with like any other third parties. So in that term, I value that type of privacy. But in terms of like you know me liking certain like genres. Me like wanting to search certain things on social media like, I don't value that quite as much.”

Another participant said that no matter how strong the cybersecurity infrastructure, there is always a risk of leak. As a result, they would trust Netflix and Spotify a lot more because streaming companies would have less data about them. Size of the company factored into the safety as well, because more participants mentioned that their safety might be at risk if data is leaked, because Google or Facebook leak would mean a lot more personal data is in danger, as compared to Netflix and Spotify (one user mentioned that their music and show preference is public anyways).

3.2.2 Recommendation Quality

Most of the participants mentioned that some social media platforms, like Instagram and YouTube were very aggressive with their recommendations. Participants that used YouTube and Instagram said that clicking on one video would completely change their recommendations. Many of our participants were very concerned with that for two reasons. The first reason given was that their recommendation quality was worse. The second reason was that it presents a danger of falling down a rabbithole. Based on what the participants said, the researchers thought that it was similar to the theory presented by Seaver, which was basically that recommendation algorithms were a trap.
This is what one of the participants said:

> “…for Youtube and Instagram, it's a bit more fluid because it's like, maybe i'll search one video, and then for the next two or three days i'll, like, get a big like a kind of a conglomeration of videos related to that one video that I watched, which Isn't necessarily indicative of like what my actual preference might be. So it kind of eventually bounces out like, let's say, I watch more videos relating to that. But I'm not necessarily absolutely trusting of it, just because it relates it off like one small thing, and then pushes more of it on me.”

By aggressively altering the recommendation based on one click, it seems that the platform wants to have the user fall down the rabbit hole. Another participant said this when asked whether the recommendation affects their time spent on the platform:

> “Yea, I would say that they they do cause me to spend more time on the on the platform, eh, especially in relating to content. If if I’m looking up how to do something, and on YouTube and then you know another recommendation video comes up, em, that I may not have watched before, then, you know, you obviously watch that one. and then, you know, you spend more time. And as far as it being positive or negative, I would, I would probably lean more towards positive.”

This did not seem to be a problem when it came to streaming services. However, most of the users thought that there was a bias.

3.3 Survey

For the online questionnaire, we used Qualtrics to create and host the questionnaire. Similar to the interviews, we included generic questions at the beginning and then iterated over platforms that the participants were using. We included one attention question and also included demographic questions at the end so that we could cross check the answers with the information provided by Prolific. The study itself was administered on Prolific. We used the standard sample, because it would distribute the study to available participants and we did not have to wait as long for the responses. Since we were able to only get a small number of participants, we opted to only get participants in the United States. We ran a pilot of five seats to determine if our reward was sufficient and we were able to get good answers. Also we wanted to know if our time estimate of five minutes for the survey was adequate. GIven the five minute time for the questionnaire and the $25 budget, we were able to get 5 seats for the test study and 22 seats for our full study. We were able to accept 100% of the questionnaires and no bots were detected. The minimum recaptcha score was 0.90 (>= 0.50 means the responses are very likely from a human).

3.3.1 Survey structure

The survey questions were similarly structured as the interview questions because we wanted to receive comparable results from the survey participants as from the interview participants. We asked additional demographic questions at the end to see if we received a diverse pool of participants. Also, this was an additional measure to validate the quality of the respondents since this allowed us to cross-check the demographic answers given in the surveys with the demographic information provided by Prolific.

The design of the survey asked the participants to select two or more of the platforms we believed were most commonly used, but we also added the open to select ‘other’ and write in the platform name. Even though we have one participant in the test run of five questionnaire seats provide a custom platform name, none of the participants of the full run chose to do so. For a follow up or future research, we would provide more predefined platform names because we were missing out on responses for streaming platforms like Netflix or Spotify. Our focus of the questionnaire platforms was mainly on social media platforms.

4. Results

4.1 Interviews

We interviewed six participants using semi-structured interviews. The time varied between 31 and 48 minutes for the interviews. The demographic for our participants was skewed towards students only in the age range between 18 to 24 and 25 to 34. This was the result of using convenience sampling. For additional results or for future research, the researchers should look into recruiting a broader audience to receive a balanced sample for more representative results.

4.2 Survey

The survey responses of the full run included the responses from 22 participants. The demographic for age and occupation were diverse, see figure 2 and figure 3. The gender was not as diverse (see figure 4) because we were using the standard sample on Prolific which distributes the questionnaire seats to available participants. A balanced sample would have been possible, but it would have taken more time to collect the answers.

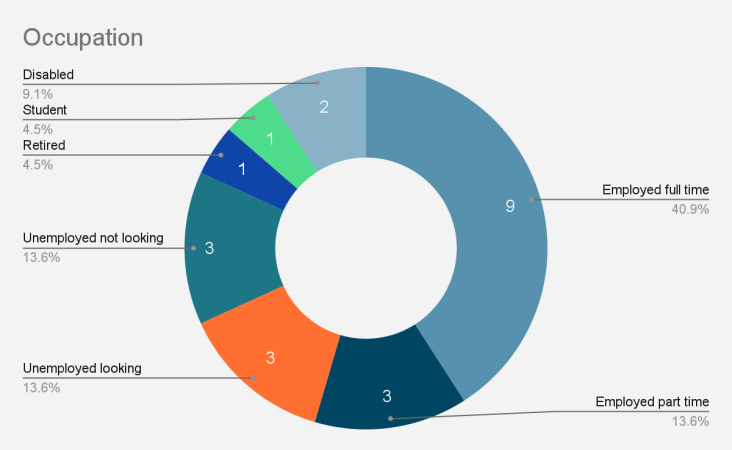


Figure 1: Responses to question regarding bias in the recommendation

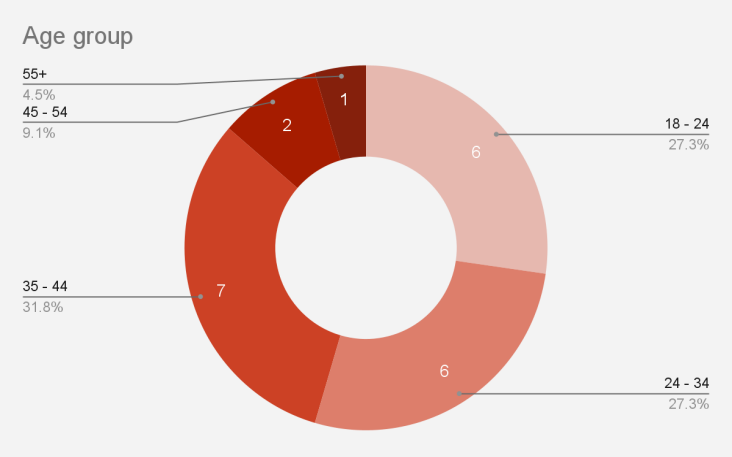


Figure 2: Responses to question regarding bias in the recommendation

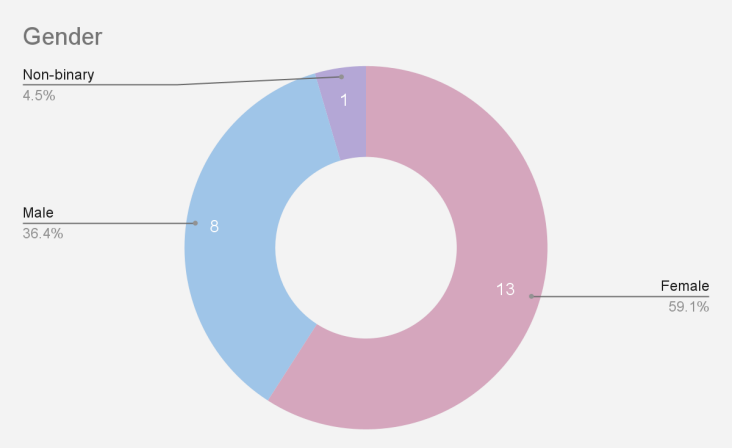


Figure 3: Responses to question regarding bias in the recommendation

4.3 Analysis

After the analysis of the interview, the authors selected certain trends that were visible from the interview data. Based on that, a survey was designed and conducted on Prolific as a way to see if the trends observed during the interview

data were generalizable to a more general audience. In particular, the authors were looking for trends regarding general bias, data privacy, and safety with regards to time or money spent because of the personalized recommendations. In order to get more granular information, participants were asked the same six questions for every app they selected. The platforms used by the participants are shown in figure 4.

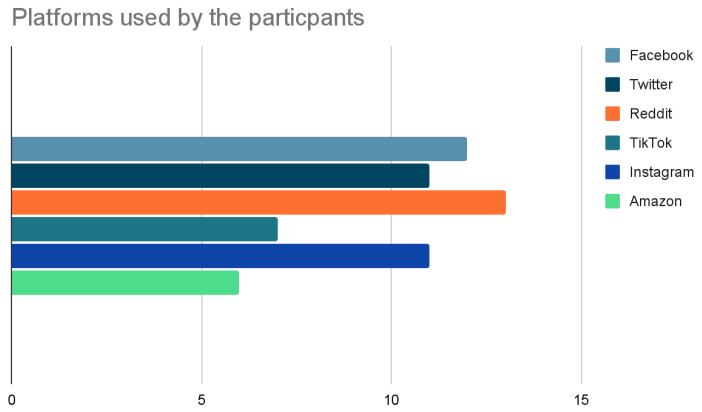


Figure 4: Platforms used by the participants

4.3.1 Bias

Breaking down the analysis on a single app basis, the survey participants felt that some apps were much more biased than others. According to the participants, apps such as Instagram, Amazon, Facebook, and Tiktok were considerably more biased than others. This finding was largely consistent with what the interview participants had said with regards to the topic. The only part that cannot be corroborated in this case is what each survey participant perceived the definition of bias to be. This is particularly interesting because, purely by observation, these apps very aggressively utilize personalized recommendations as part of their in-app experience as compared to others. Twitter has both a home (recommended) feed and chronological feed as options, but it must be pointed out that even home feed only orders tweets by accounts followed (and a few promoted tweets in between). Reddit also utilizes membership in subreddits to curate content for the user. Based on that, it can be inferred that because of the perception of bias, users don't trust a personalized recommendation heavy curation system. This was only based on 22 participants (with even less participants for single platform analysis), and a survey with more participants needs to be conducted in order to reach that conclusion. The participants' responses with regard to bias are shown in figure 5.

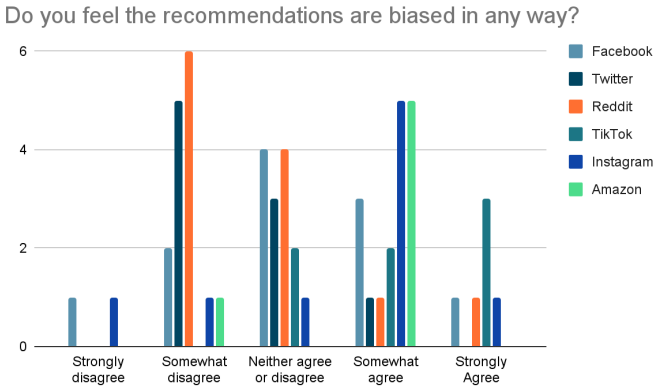


Figure 5: Responses to question regarding bias in the recommendation

4.3.2 Data Privacy

During the interview, a lot of participants stated that, in most cases, their personal safety would not be at risk if there was a data leak that happened. The exceptions were largely centered around large conglomerates, such as Amazon and Meta products (Facebook and Instagram). This finding was partially corroborated by the survey that we took. For Amazon, 50% of respondents stated that there would be a moderate risk or greater if there was a data leak, and 6 out of 11 said the same for Facebook. However, only 3 out of 9 would say the same for Instagram (which is the same as Twitter). That is particularly interesting because Facebook and Instagram are owned by the same company, so this finding can also suggest that context knowledge has a lot to do with perceptions. The participants' responses are shown in figure 6.

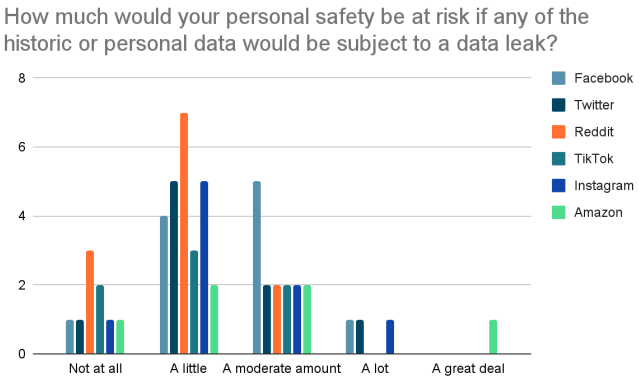
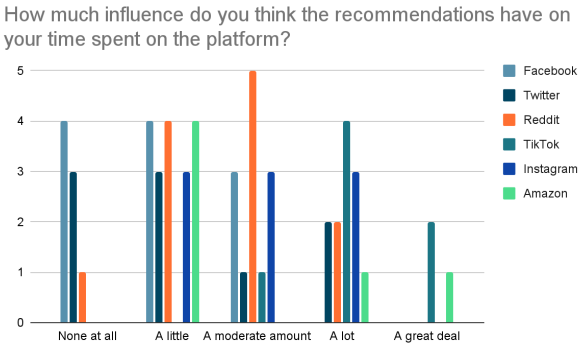


Figure 6: Responses to question regarding personal safety if there were a data leak

4.3.3 Time and Money Consumption

Majority of Tiktok and Instagram users pointed out that those apps increased their time spent on that platform as compared to others listed on our survey. This was a relatively new finding as this did not come up very often in the interviews. Once again, it is an interesting finding that most participants said this about two platforms that very heavily rely on personalized recommendation for their in-app experience. This goes in line with Seaver's [9] captive theory that the primary reason for personalized recommendations is to keep the users hooked in the app. A study with more participants is necessary to further substantiate this claim. The participants' responses regarding time and money spent on the platform are shown in the graphs in figure 7a and 7b.



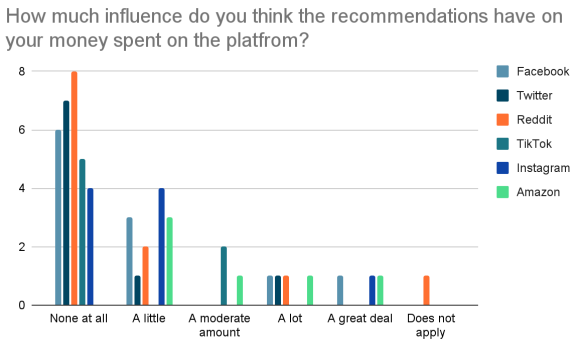


Figure 7a (left) and 7b (right): Responses to question regarding influence on time (left) and money spent (right)

5. Limitations

One of the main limitations of the research process is the lack of participants for online surveys. With only 22 participants, there is a limited amount of data to analyze. This lack of data can lead to skewed results and make it difficult to draw refined conclusions from the survey. Additionally, there are limited options for entertainment applications in surveys, such as Netflix or Spotify. These applications are often seen as more engaging for participants. With more focus on social media applications, entertainment/e-commerce applications take a back seat

which are widely used by the larger demographic. In the interviews, the process is limited by the participant demographic which is closely clustered by age and occupation. This can lead to inaccurate results and can prevent obtaining the data needed to accurately answer the research questions. Overall, the lack of participants in surveys, participant demographics in interviews, and limited options for entertainment applications in surveys can be major limitations of the research process. These limitations can prevent the researchers from obtaining the necessary data and lead to inaccurate results.

6. Conclusions

Trust and safety perception are two of the most important factors when it comes to using applications. It is not only dependent on the size of the company or the reputation of the app but also on the data collection practices that the company follows. People are generally more accepting of data collection for quality recommendations, but it is crucial to ensure that the data collected is only used for the purpose it is intended for. Financial data and location tracking are two types of data that should be off-limits, as they are personal and sensitive to the user. Applications for music are generally the most trusted, as people are aware that the data collected is used to provide better recommendations and not to exploit the user. However, this perception changes drastically when the application is owned by a large conglomerate. People have less trust in these apps, as they are aware that the company may use the data collected for their own gain, instead of just providing better recommendations. Therefore, it is important for companies to ensure that the trust and safety of their users are not compromised in order to maintain the trust of their users.

Acknowledgments

We would like to thank Professor Kate Isaacs and Josh Dawson for their guidance during the course of this project and their valued feedback on the assignments. Also we would like to thank the unnamed members of the class who provided feedback on various phases of the project during the inter-group draft feedback sessions in class.

REFERENCES

[1] John O'Donovan and Barry Smyth. 2005. Trust in recommender systems. In Proceedings of the 10th international conference on Intelligent user interfaces (IUI '05). Association for Computing Machinery, New York, NY, USA, 167–174. https://doi.org/10.1145/1040830.1040870

[2] Michele Gorgoglione, Umberto Panniello, and Alexander Tuzhilin. 2011. The effect of context-aware recommendations on customer purchasing behavior and trust. In Proceedings of the fifth ACM conference on Recommender systems (RecSys '11). Association for Computing Machinery, New York, NY, USA, 85–92. https://doi.org/10.1145/2043932.2043951

[3] Milano, S., Taddeo, M. & Floridi, L. Recommender systems and their ethical challenges. AI & Soc 35, 957–967 (2020). https://doi.org/10.1007/s00146-020-00950-y

[4] Winoto, P., Tang, T. (2014). The Ethics of a Recommendation System. In: , et al. Web-Age Information Management. WAIM 2014. Lecture Notes in Computer Science(), vol 8597. Springer, Cham. https://doi.org/10.1007/978-3-319-11538-2_26

[5] Itishree Mohallick and Özlem Özgöbek. 2017. Exploring privacy concerns in news recommender systems. In Proceedings of the International Conference on Web Intelligence (WI '17). Association for Computing Machinery, New York, NY, USA, 1054–1061. https://doi.org/10.1145/3106426.3109435

[6] David Harborth and Sebastian Pape. 2020. How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies: The Case of Tor. SIGMIS Database 51, 1 (February 2020), 51–69. https://doi.org/10.1145/3380799.3380805

[7] Ali Alkhatib. 2021. To Live in Their Utopia: Why Algorithmic Systems Create Absurd Outcomes. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 95, 1–9. https://doi.org/10.1145/3411764.3445740

[8] Johannes Kunkel, Tim Donkers, Lisa Michael, Catalin-Mihai Barbu, and Jürgen Ziegler. 2019. Let Me Explain: Impact of Personal and Impersonal Explanations on Trust in Recommender Systems. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 487, 1–12. https://doi.org/10.1145/3290605.3300717

[9] Seaver, N. (2019). Captivating algorithms: Recommender systems as traps. Journal of material culture, 24(4), 421-436. https://doi.org/10.1177/1359183518820366

[10] Kai Lukoff, Ulrik Lyngs, Himanshu Zade, J. Vera Liao, James Choi, Kaiyue Fan, Sean A. Munson, and Alexis Hiniker. 2021. How the Design of YouTube Influences User Sense of Agency. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21).

Association for Computing Machinery, New York, NY, USA, Article 368, 1–17. https://doi.org/10.1145/3411764.3445467

[11] Hamed Qahri-Saremi, Isaac Vaghefi, and Ofir Turel. 2022. Addiction to Social Networking Sites and User Responses: Toward A Typological Theory and its Relation to Users' Personality Traits. SIGMIS Database 52, 4 (November 2021), 65–91. https://doi.org/10.1145/3508484.3508489

[12] Laura Burbach, Johannes Nakayama, Nils Plettenberg, Martina Ziefle, and André Calero Valdez. 2018. User preferences in recommendation algorithms: the influence of user diversity, trust, and product category on privacy perceptions in recommender algorithms. In Proceedings of the 12th ACM Conference on Recommender Systems (RecSys '18). Association for Computing Machinery, New York, NY, USA, 306–310

[13] Yassine Himeur, Shahab Saquib Sohail, Faycal Bensaali, Abbes Amira, Mamoun Alazab, Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives, Computers & Security, Volume 118, 2022, 102746, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102746

[14] Ruoxi Shang, K. J. Kevin Feng, and Chirag Shah. 2022. Why Am I Not Seeing It? Understanding Users' Needs for Counterfactual Explanations in Everyday Recommendations. In 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22). Association for Computing Machinery, New York, NY, USA, 1330–1340. https://doi.org/10.1145/3531146.3533189

[15] Akshit Gupta, Debadeep Basu, Ramya Ghantasala, Sihang Qiu, and Ujwal Gadiraju. 2022. To Trust or Not To Trust: How a Conversational Interface Affects Trust in a Decision Support System. In Proceedings of the ACM Web Conference 2022 (WWW '22). Association for Computing Machinery, New York, NY, USA, 3531–3540. https://doi.org/10.1145/3485447.3512248

[16] Emily Sullivan and Philippe Verreault-Julien. 2022. From Explanation to Recommendation: Ethical Standards for Algorithmic Recourse. In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (AIES '22). Association for Computing Machinery, New York, NY, USA, 712–722. https://doi.org/10.1145/3514094.3534185

[17] James Bennett and Stan Lanning. 2007. The Netflix Prize. Netflix released a dataset containing 100 million anonymous movie ratings. https://web.archive.org/web/20070927051207/http://www.netflixprize.com/assets/NetflixPrizeKDD_to_appear.pdf