Privacy Policies at the Crossroads: Public Perception and Engagement

Philipa Kolade
School of Computer Science
University of Guelph
Ontario, Canada
pkolade@uoguelph.ca

Srinija Battula
School of Computer Science
University of Guelph
Ontario, Canada
sbattula@uoguelph.ca

Vidhi Parekh
School of Computer Science
University of Guelph
Ontario, Canada
parekhv@uoguelph.ca

***Abstract*— Privacy policies tend to have problems that users struggle with. In this study, we highlight the importance of privacy policies, then we investigate the privacy policies of six different organizations by comparing them against each other. The privacy policies we chose are from two key industry sectors – the Entertainment sector and the healthcare sector. From our analysis, we are able to deduce instances that may present problems to users. Lastly, we conducted a survey to gain valuable insight on privacy receptions and the struggles users face in reading privacy policies. Our findings from 30 participants show that people still face difficulties in reading policies. Based on our findings, we recommend steps that can be taken to reduce the burden of digesting privacy policies.**

Keywords—Privacy Policy, GDPR, readability,

I. INTRODUCTION

Privacy has been a key concept since ancient times and has evolved alongside modern technologies. Today, privacy policies are crucial documents that outline how organizations collect, use, and share personal information [1]. Unfortunately, policies are often lengthy and filled with technical jargon, making them difficult for many users to comprehend. As a result, individuals frequently overlook reading them and remain unaware of the terms they are agreeing to [2].

A 2008 study [3] famously estimated that reading every privacy policy a user encounters would take 244 hours annually. Despite regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), challenges persist in effectively communicating the intentions of privacy policies. The rise of advanced technologies, including artificial intelligence, further complicates privacy management, introducing unique risks such as difficulties in exercising the "right to be forgotten."

This study investigates public perceptions of privacy policies, the challenges users face in understanding them, and the effectiveness of current policies in conveying their purpose. Through the analysis of survey responses and policy samples, we aim to provide actionable recommendations for enhancing the clarity and accessibility of privacy policies.

II. RELATED WORKS

In this section, we present a brief discussion of studies related to our project. Several studies [4] [5] have shown that users are worse at accurately deciphering information from full length policies than shorter length policies. Kelley et al. [4] report that users preferred shorter and tabulated policies while Earp et al. [5] states that users regard fuller length policies as more secure and detailed.

Multiple studies have shown the difficulty in interpreting privacy policies. Sumeeth et al. [6] discovered that privacy policies are sometimes only suitable for people with a post-graduate degree, and not average individuals. Similarly, Das et al. [7] conducted a study with 64 participants and determined that privacy policies are unsuitable for most youth.

III. PROBLEM STATEMENT

Since 2018, when the GDPR took effect, privacy policies have undergone significant changes. New requirements have been introduced, benefiting users (data subjects) by enhancing transparency and control over their data. Linden et al. [8] report a positive trend in users' experiences since the regulation's implementation. Although six years have passed since the GDPR became operative and it has effectively protected users' rights within the EU, privacy gaps and flaws remain in the implementation of privacy policy agreements.

IV. OBJECTIVES

This study addresses challenges in understanding and engaging with privacy policies, which are often seen as complex and tedious. This disconnect affects users' interactions with organizations. The research aims to provide clear insights to improve the design and implementation of privacy policies through the following objectives:

1. Understanding Public Sentiment on Privacy:
   As digital services become more prevalent, privacy concerns among users grow. This study will:
   a. Assess how users prioritize privacy in their online interactions.
   b. Determine whether people view privacy as relevant or outdated in today's connected world.
   c. Explore how users weigh their need for privacy against the convenience of digital services.
2. Assessing Engagement with Privacy Policies:
   Many users do not engage with privacy policies despite their importance. This analysis will:
   a. Investigate barriers that prevent users from reading them, such as complexity and length.
   b. Discover what motivates users to read privacy policies, such as mistrust of platforms.
3. Evaluating User Trust in Organizations and Their Privacy Practices:

User trust is crucial for interaction with digital services. This objective will evaluate:

a. The level of trust users has in organizations regarding privacy commitments.
b. How an organization's reputation affects users' trust.
c. Whether mistrust leads users to avoid platforms or encourages them to review policies.

4. Analyzing Preferences for Privacy Policy Presentation Formats:

Privacy policies vary in presentation style. This study will look at:

a. User preferences for detailed data lists versus summarized formats.
b. Demand for simplified policies that use plain language.
c. The trade-off between detailed transparency and accessible summaries.

5. Providing Actionable Recommendations to Improve Policy Transparency and Usability:

This study aims to provide recommendations for organizations to enhance their privacy policies:

a. Creating strategies to simplify policy content while remaining compliant with regulations.
b. Suggesting ways to improve transparency about data-sharing practices.
c. Proposing user-friendly enhancements, such as visual aids and options for opting out of data sharing.

V. Methodology

This study aimed to understand public perceptions and engagement with privacy policies through a multi-faceted methodology. It included survey analysis, privacy policy evaluations, and the distribution of questionnaires to a diverse, global audience.

A. Privacy Policy Evaluations

We performed evaluations on the six privacy policies and extracted the points of concern in them. We chose the policies from these platforms; Netflix, Rakuten Viki, Serializd, DoctorC and MFINE. The first four represent platforms related to media streaming, and the latter two represent Health-related services.

B. Survey Design and Development

The survey was designed to collect quantitative and qualitative data on user perceptions and behaviors regarding privacy policies. It included 24 structured questions categorized as follows:

- Demographics: Questions on age, gender, education level, technical knowledge, and professional background, including experience in IT or privacy fields.
- Notions on Privacy: Exploration of the importance of privacy, attitudes toward current practices, and willingness to compromise privacy for convenience.
- Engagement with Privacy Policies: Inquiry into how often participants read policies, barriers to reading, and factors that prompt engagement.
- Trust in Organizations: Assessment of trust in organizations' ability to uphold privacy commitments.
- Policy Preferences: Comparison of two privacy policy excerpts (Sample A and Sample B) to identify user preferences for clarity, detail, and simplicity.

The survey utilized:

- Multiple-Choice Questions for quantitative data (e.g., "How often do you read privacy policies?").
- Open-Ended Questions for qualitative insights (e.g., "What prompts you to read a privacy policy?").
- Likert Scale Questions to measure agreement or importance (e.g., "How important is privacy to you?")

C. Policy Analysis

Four privacy policies of differing complexity were analyzed. In Section four (which spans Q15 - Q19) of our questionnaire, Netflix is represented by sample A and Rakuten Viki is represented by sample B. Section four covers data sharing practices by Netflix and Rakuten Viki. In Section five, Sample A (now representing DoctorC) categorized data collection, while Sample B (now representing MFINE) provided detailed lists. Section five focused on presentations of data collection. These excerpts were used to assess user comprehension and preferences.

D. Survey Distribution

The survey was digitally distributed to people through online platforms such as social media groups, email lists, and forums with privacy-conscious users. To encourage honest responses, anonymity was guaranteed. Sensitive information like names or specific identifiers were not collected.

VI. Policy Evaluations

A. Netflix vs. Rakuten Viki

In this section, we focus on features of Netflix's privacy statement and Rakuten Viki's privacy policy that are a cause for concern, or areas we found interesting. For this analysis, Section F of Netflix's privacy statement, which focuses on "Netflix Games" would not be discussed, because Rakuten Viki has no gaming features currently.

- General Overview

Netflix and Viki's Privacy statements are structured properly, with appropriate headings, bullet points, etc. Netflix is easier to navigate because it has a side panel, where you can easily jump to a section you are interested in and includes hyperlinks in the policy that redirect you to a section of the policy being referenced.

According to the Flesch-Kincaid readability test, which is based on the number of words, sentences, and syllables in a body of text, both policies are appropriate for individuals that are at least college graduates or professionals. They perform poorly with a score of 27 for Netflix and 28 for Rakuten Viki. Flesch-Kincaid tests have their limitations; however, they give an idea of how easy it is for an individual to read a document. Complexity makes the privacy policy meaningless and unfair to individuals who might be at a disadvantage due to age, reading disabilities, or other forms of neuro-divergence that might impact comprehension levels.

Rakuten Viki and Netflix require users to be above 18 or older to subscribe to their services but teenagers remain at risk of unknowingly compromising their privacy because the fences around account creation are typically easy to circumvent.

- Data collection

Both policies tend to use terms like 'such as' when describing the kinds of information collected by the

services, this term introduces ambiguity in what exactly is being collected because it is a vague quantifier [9]. The use of terms like 'such as' reduces specificity because some examples can be removed from the list of collected information. It can be used to avoid making comprehensive lists of collected data.

- Data sharing

While it is not mandated by privacy frameworks like GDPR and CCPA, both policies do not provide specifics on who personal information is shared to. Netflix and Rakuten provide only the categories of the parties which data is shared with. (e.g., Service providers, Advertising companies etc.). Rakuten only provides the name of the party responsible for the processing of financial information in their policy.

- Privacy Rights

In Netflix's policy, privacy rights are explicitly stated, and they align with GDPR requirements. Users can access, rectify, and erase their information. Users have the right to data portability and to download a copy of their information. They can object to or restrict processing, and conditionally object to automated decisions being made about them. Users have the right to complain to data protection authorities about the processing of their data. These rights are possessed by all individuals making use of Netflix.

On the other hand, the rights of those using Viki are dependent on where they reside. It is not explicitly stated which countries/regions are allotted the rights listed in their policy, except for the United States, which has additional rights. Asides those in the United States, users do not have the right to object to their personal data being used for targeted advertisements. All users regardless of where they reside, cannot restrict or object to automated decisions being made about them.

- Cookies

Investigation of the third-party cookies used by both services revealed that Netflix uses a significantly smaller amount of third-party (15) and advertisement cookies (8), in total 23, while Rakuten Viki uses about 88 cookies in total from third party services. This indicates that Rakuten Viki might partake in extensive tracking. Further investigation into what each cookie does would be required to determine the extent and validity of tracking. For this project, we do not have the capability, mostly due to time, to delve into further investigation.

Another cause for concern is the lifespan of these cookies, The longest lifespan of third-party cookies used by Netflix is 729 days (about 2 years), while that used by Rakuten Viki is 20 years, which is exceedingly larger.

- Do Not Track signals

Rakuten Viki and Netflix do not respond to Do Not Track (DNT) signals, DNT signals are a privacy feature built into web browsers, while there is no legal requirement to respond to these signals, it ignores users' wishes to not be tracked and does not align with privacy by default requirements.

- Transfer of assets

Netflix states that in the event of an asset transfer, they will transfer personal information if the receiving party agrees to respect it similarly to the manner done in their existing policy. Rakuten Viki provides no assurances, except that they will try their best to ensure that the receiving party uses personal information in a way that matches their privacy policy.

A. TV time vs. Serializd

This report presents a detailed comparison of privacy policies of TV Time and Serializd. TV Time functions as a media-tracking platform with extensive user interaction, while Serializd is designed to facilitate reviews, ratings, and personalized media cataloging. The analysis focuses on privacy practices, user controls, data collection, and notable concerns to highlight similarities and differences between the two platforms.

- General Overview

Both TV Time and Serializd outline their privacy practices via dedicated sections on their platforms. These documents adhere to modern standards of clarity, using structured headings and bullet points for easier navigation. However, TV Time offers more comprehensive coverage on third-party integrations compared to Serializd, which prioritizes transparency in community engagement and content moderation.

- Readability & Accessibility

TV Time's policy is lengthier and provides detailed information on how user data is processed and shared with third parties. Serializd has a brief approach, emphasizing user-generated content and its storage without delving deeply into legal compliance. Neither of the documents meets readability standards for a general audience, making it difficult for users who are not good with technical terminology.

- Data Collection Practices

TV Time: Collects detailed behavioral data, including media consumption habits, device information, and interaction metrics. This platform also tracks preferences for personalized recommendations.

Serializd: Focuses more on explicit user submissions, including reviews, ratings, and platform interactions. It is transparent about the use of user-generated content but provides less details on data collection mechanisms like analytics and advertising tracking.

Key Concern: Both platforms rely on vague terms like "such as" when describing data categories, which reduces specificity and leaves room for interpretation. This lack of clarity is a potential issue for users looking for comprehensive understanding of what data is being collected.

- Data Sharing Practices

TV Time: Shares data with a wide range of third-party partners for advertising, and platform improvements. However, the policy only categorizes these partners without listing specific names, limiting transparency.

Serializd: Serializd shares less data with third parties and mainly uses data internally. It does not provide detailed information about external partners, which might mean it has limited third-party involvement or simply does not explain it clearly.

- User Rights and Privacy Controls

TV Time: Aligns with GDPR and CCPA frameworks, offering robust user controls. Users can access, correct, or delete their data, as well as opt out of certain types of data processing.
Serializd: Provides basic privacy rights but lacks detailing in controls, such as the ability to restrict specific data usage or portability options.

- Cookies and Tracking

TV Time: Has relatively huge cookie usage for personalization and advertisement purposes. Cookies are active for up to two years.
Serializd: It uses fewer cookies, mainly focusing on essential functions instead of advertising purposes.

- Do Not Track Signals

Neither platform responds to Do not Track (DNT) browser signals, which talks about user choice and privacy-by-default principles. Although not required by law, ignoring this feature aligns with common industry practices that do not prioritize user choice.
Key Concerns gotten from the analysis of TV time and Serializd's policies include:

- Data Transparency: Both platforms need to improve clarity and granularity in their privacy disclosures, particularly regarding third-party data-sharing practices.
- User Accessibility: The policies are not user-friendly for younger or non-technical audiences.

VII. Key Findings and Insights from Survey

A. Demographics and context

Respondent Overview: The respondents reflected a diverse and informed sample group:

- Age Distribution:
  Largest group: 18-24 years (47%)
  Second largest: 25-34 years (27%)
- Gender:
  Respondents were split almost evenly, with 50% Men and 47% Women, and 3% Prefer not to disclose their gender.
- Education Levels:
  The group was highly educated, with 68% holding bachelor's degrees and 25% with master's degrees. Minimal participation from those with secondary education or no formal education.
- Technical Knowledge:
  Respondents rated their technical knowledge as Good (47%), Excellent (23%), or Average (27%).

B. Country Representation

Respondents represented diverse geographies, with 57% from Canada, followed by participants from the USA, UK, India, Kenya, and Nigeria.

C. Privacy Concerns and Perception

1) Importance of Privacy:
80% of respondents rated privacy as Extremely Important, showcasing a strong belief in the fundamental value of privacy. However, 33% believed that privacy is becoming irrelevant in the modern world due to pervasive data collection and tracking practices, which reflects a growing sense of resignation among users who feel their personal data is already compromised. Even though 97% of our respondents rated privacy as extremely important or somewhat important, 23% claimed they would still use a service or application with shady privacy policies. This information tracks because most participants said they were undecided on if they could trust organizations to uphold their end of Privacy agreements. Shady policies might not matter to them because they lack sufficient confidence in organizations.

a) Main concerns about Privacy Policies:

b) Complexity and Length:

Many privacy policies are too long, dense, and filled with technical jargon, which makes it inaccessible. One of the participants suggests they would prefer a summarized version of policies.

- Mandatory Acceptance:
  Users feel they lack control, as agreeing to privacy policies is often required to use essential services.
- Transparency Issues:
  Privacy policies are perceived as vague about data-sharing practices, particularly with third parties.

D. Engagement with Privacy policies

→ Frequency of Reading

- 33% of respondents rarely read privacy policies, and 20% never read them.
- Only 7% always read policies, while 23% sometimes engage with them and 17% often read them.

→ Motivations for Reading Policies :
When respondents did read policies, their motivations included:

- Lack of Trust: If a platform or service seemed suspicious or had a poor reputation.
- Curiosity About Data Sharing: Understanding what data is collected and with whom it is shared.
- Personal Impact: Policies perceived as directly affecting well-being or security.
- Length: Shorter lengths inspire some to read policies.

E. Trust and Decision making

1) Trust in Organizations

- Only 33% of respondents trusted organizations to honor their privacy policies.
- The majority (57%) were unsure, reflecting a significant trust deficit.

2) Decision-Making Based on Privacy Policies

- 68% of respondents said privacy policies influence their choice of platforms.
- However, 46% said they would avoid services entirely if privacy policies appeared sketchy or unclear.

This demonstrates that while users value clear and transparent policies, they are often willing to compromise privacy for convenience or necessity.

F. Preferences for Privacy Format

1) Simplification Needs

A resounding 93% of respondents preferred simplified policies with less technical terms. Be it whether you are an IT professional or not, whatever your age be or how much education and technical knowledge you have, everyone prefers a simplified version of these policies with less technical terms because it is much easier to understand. Suggestions included:

- Short summary of key points.
- Plain language explanations.
- Visual aids like diagrams or bullet points.

2) Detailed vs. Grouped Data Presentation

- 79% preferred detailed data lists (MFINE's policy) over grouped categories (DoctorC's policy). Detailed formats were perceived as more transparent and trustworthy, even if they required more effort to read.
- 21% preferred grouped categories, citing simplicity as a major advantage.

This indicates a trade-off: while users value transparency, simplicity is critical to improving engagement..

G. Data Sharing Concerns

1) What Concerns Users Most?

Participants identified the following as the most sensitive data types to share:

- Addresses
- Health conditions
- Financial details
- Tracking information (e.g., GPS location)

This is an open-ended response question, only 11 out of 30 have answered this question. However, out of these 11 responses, 9 responses were found to be from people working as IT professionals. "Almost everything" and "location/address" being highlighted. This might be because they have heightened awareness of data misuse risks, and their understanding of how personal information can be tracked and exploited.

2) Clarity on Data Sharing

46% of respondents felt policies lacked clarity on how data is shared with third parties. Users want explicit details on "What data is shared, Who the recipients are, and The purpose of sharing."

Out of 30 participants, who have responded to the collection of usage patterns question regarding healthcare service providers policies, 15 said yes, they are comfortable, 14 said no and one is unsure about it. Responders who are IT professionals and have education of master's/bachelor's level has rated themselves as "Excellent" in technical knowledge skills, are found to be the ones who said "YES". This might be due to their better knowledge in data collection and processing, perceiving risks accurately and being familiar with privacy safeguards. We can safely say that educational background and field of professional affects the trust of users in these policies.

H. Suggestions for Improvement

Respondents provided actionable feedback for improving privacy policies:

1) Transparency:

Clearly list all third-party recipients and explain the purpose of data sharing.

2) Trust Indicators:

Use trust scores or compliance badges (e.g., GDPR certification) to reassure users.

3) Format Enhancements:

Summarize key terms with bullet points. Include diagrams or visual aids to break down complex content.

4) User Control:

Offers opt-out options for data sharing. Simplify data management interfaces to empower users.

Insights from Policy Excerpts (Doctor C and MFINE)

DoctorC (Grouped Data Categories):

Strengths: Simple and scannable.

Weaknesses: Perceived as vague and lacking depth.

MFINE (Detailed Lists):

Strengths: Transparent and comprehensive.

Weaknesses: Time-consuming to read.

Finding: Transparency outweighs simplicity, but users still demand policies that balance the two.

VIII. RECOMMENDATIONS

1. Simplify Privacy Policies
   a. Use plain, concise language to reduce complexity.
   b. Summarize key terms using bullet points and infographics.
2. Increase Transparency
   a. Clearly disclose data-sharing practices, including specific third-party recipients.
   b. Offers opt-out mechanisms for data-sharing practices.
3. Build User Trust
   a. Highlight compliance with frameworks like GDPR or CCPA.

b. Introduce trust indicators, such as historical transparency scores.

4. Adopt Visual Formats
    a. Incorporate flowcharts, diagrams, or interactive dashboards for policy navigation.
5. Educate Users
    a. Launch campaigns to inform users about their privacy rights.
    b. Provide easy-to-follow onboarding guides that summarize policy terms.

IX. Limitations

Due to time constraints, we were not able to document our evaluation of DoctorC and MFINE. To not make our questionnaire too bulky, we restricted the number of excerpts to assess people on. The excerpts used in our questionnaire covered only four policies.

X. Conclusion

This study highlights a gap between the intended purpose and actual effectiveness of privacy policies. While these policies aim to protect users and inform them about their data rights, many find them complex and hard to understand. Despite this, 79% of users consider privacy important, although younger demographics feel it is becoming less relevant in today's data-driven world.

- Low Engagement: The survey shows that 36% of people rarely read privacy policies, and 18% never engage with them. Key reasons include long length, unclear language, and the perception that acceptance is mandatory. This perception weakens the effectiveness of these policies.
- Trust Issues: Only 32% trust organizations to uphold their privacy commitments, reflecting doubts about data handling and clarity surrounding data sharing.
- Desire for Simplicity: Most respondents prefer simpler policies with clear summaries and direct disclosures. A significant 93% want less jargon, and 79% seek detailed explanations of data collection.
- Call to Action: Organizations and regulators must prioritize clear and trustworthy privacy policies. Regulation frameworks like GDPR and CCPA should evolve for better transparency.
- Moving Forward: By simplifying language and enhancing transparency, organizations can create meaningful privacy policies that build trust and improve user engagement. Collaborative efforts are essential to empower users and transform privacy policies from bureaucratic documents into effective safeguards for user rights.

References

[1] J. B. Earp, A. I. Anton, L. Aiman-Smith, and W. H. Stufflebeam, “Examining Internet Privacy Policies Within the Context of User Privacy Values,” IEEE Trans Eng Manag, vol. 52, no. 2, pp. 227–237, May 2005, doi: 10.1109/TEM.2005.844927.

[2] J. Woodring, K. Perez, and A. Ali-Gombe, “Enhancing privacy policy comprehension through Privacify: A user-centric approach using advanced language models,” Comput Secur, vol. 145, Oct. 2024, doi: 10.1016/j.cose.2024.103997.

[3] A. M. Mcdonald and L. F. Cranor, “Database Nation: The Death of Privacy in the 21st Century,” 2001. [Online]. Available: http://www.is-journal.org/

[4] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, “Standardizing privacy notices,” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA: ACM, Apr. 2010, pp. 1573–1582. doi: 10.1145/1753326.1753561.

[5] J. B. Earp, M. Vail, and A. I. Anton, “Privacy Policy Representation in Web-based Healthcare,” in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07), IEEE, Jan. 2007, pp. 138–138. doi: 10.1109/HICSS.2007.445.

[6] M. Sumeeth, R. I. Singh, and J. Miller, “Are Online Privacy Policies Readable?,” International Journal of Information Security and Privacy (IJISP), vol. 4, no. 1, pp. 93–116, 2010, doi: 10.4018/JISP.2010010105.

[7] G. Das, C. Cheung, C. Nebeker, M. Bietz, and C. Bloss, “Privacy Policies for Apps Targeted Toward Youth: Descriptive Analysis of Readability,” JMIR Mhealth Uhealth, vol. 6, no. 1, p. e3, Jan. 2018, doi: 10.2196/MHEALTH.7626.

[8] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz, “The Privacy Policy Landscape After the GDPR,” Proceedings on Privacy Enhancing Technologies, vol. 2020, no. 1, pp. 47–64, Jan. 2020, doi: 10.2478/popets-2020-0004.

[9] V. Belcheva, T. Ermakova, and B. Fabian, “Understanding Website Privacy Policies—A Longitudinal Analysis Using Natural Language Processing,” Information (Switzerland), vol. 14, no. 11, Nov. 2023, doi: 10.3390/info14110622.

[10] “DoctorC - Making Healthcare Affordable and Accessible,” *Doctorc.co.in*, 2024. https://doctorc.co.in/privacy-policy/ (accessed Dec. 10, 2024).

[11] “Privacy Policy – mfine,” *mfine*, 2024. https://www.mfine.co/privacy-policy/ (accessed Dec. 10, 2024).

[12] “Privacy Statement | Netflix Help Center.” Accessed: Nov. 26, 2024. [Online]. Available: https://help.netflix.com/legal/privacy

[13] “Watch Korean Dramas, Chinese Dramas and Movies Online,” *Rakuten Viki*. https://www.viki.com/legal/privacy

[14] “Keep track of what you watch | TV Time,” *TV Time*, 2024. https://www.tvtime.com/privacy (accessed Dec. 10, 2024).

[15] S. FAQs, “Serializd | FAQs,” *Serializd.com*, 2023. https://www.serializd.com/about (accessed Dec. 10, 2024).

APPENDIX:

a) Introduction

- How old are you?
- What is your gender?
- What country do you reside in?
- Have you worked in a field related to IT/Privacy?
- What is the highest level of Formal education you have completed? (if other, please specify)
- How would you rate your Technical Knowledge?

b) Notions on Privacy

- How Important is Privacy to you?
- Do you believe Privacy is dead/Irrelevant in modern times?
- Would you use a service or application even though their privacy policy seems sketchy or shady?

c) Engagement with Privacy Policies

- How often do you read Privacy Policies?
- What typically prompts you to read a privacy policy? (i.e Good qualities they may have)
- Do you trust organizations to honor their privacy policies?
- How do you think we can improve Privacy Policies?

d) Netflix and Rakuten Viki

- Which is more understandable?
- What do you think could be added to the data-sharing sections of policies to build more trust?
- Do you feel these policies provide enough clarity on who your data is shared with? Required to answer.
- Would you prefer an option to opt-out of data sharing with third-party advertisers when using media platforms
- If two platforms offered similar services, but had different data-sharing practices, would their policy influence your choice of platform?

e) DoctorC and MFINE

- Which policy is clearer about personal information collection?
- Are you comfortable with platforms collecting your usage patterns on their websites or applications (e.g time, frequency, and duration of use)
- Would you prefer simplified versions of these policies that focus on key points with less technical terms?
- Which type of information do you find most concerning to share with healthcare platforms? Single line text.
- Do you prefer policies that list all collected data individually (like sample B) or group it categorically (like sample A)