

User Agreement Knowledge and Social Media Engagement

Braedon Richlen

Communication & Media Studies, St. Norbert College

COME 468: Mass Communication Theory

Dr. Valerie Kretz

April 7, 2023

Abstract

As media rapidly grows and advances, there is little knowledge about users' thoughts on Terms of Service and user agreements or if users read them. This research proposal includes a way to examine the relationships between the amount of personal information users submit about themselves and the time they spend reading user agreements or similar documents. An online experiment consisting of a manipulation group, a control group, and a third group is used for validation to examine how users submit their data to platforms. Research regarding this subject can be used for companies, future legislation, and media consumers.

Keywords: privacy, trust, engagement, terms of service, reading, user agreements, media

Obtained User Agreement Knowledge and Social Media Engagement

As technology advances, society is witnessing more and more invasions of personal privacy with online information. Invasions of a user's digital identity fall into four categories - identity (who a user is online), location, search query (what users search and navigate), and digital footprint (a record of what a user was doing). As people carry more wearable technology and include smart devices in aspects of their everyday lives, homes, and jobs, opportunities for others to collect more personal information increases (Chawdhry et al., 2022). These are not usually hackers, but rather everyday social media companies and platforms. Companies commonly partake in gathering and using GPS, app data and internet traffic. None of this information should come as a surprise to the general public as companies are required to disclose a Terms of Service (ToS) agreement or a similar document explaining why they will collect a user's data, and how it is used.

There are certain conveniences at play when using these companies for social media needs or technological needs in general, and because of these conveniences, users are willing to ignore the data collection practices of these companies to keep the convenience of having technology at their fingertips. While the internet does offer these conveniences, there is no way for users to control their data if they wished. When a breach of a company's data occurs, users of any platform or technology start to worry and engagement of social media platforms decreases (Bright et al., 2021). When users have a high amount of trust in a social media platform with their privacy and data, social media engagement is more likely to increase. Privacy concern is also higher for people who do not try and reduce their data online while it is lowest for those who actively try and reduce their data (Bright et al., 2021). The rest of this proposal will cover ways to improve privacy policies while reflecting on the history of protection efforts and data

leaks, ways users reduce their data online, and issues in privacy policies and ToS agreements such as readability.

History of Privacy Protection Events

Throughout history, there have been multiple breaches of online privacy, either by notorious hacktivist groups like Anonymous, or by companies themselves. One of the most popular data breaches of all time was the Facebook breach in March 2018, instigated by Cambridge Analytica. In this data breach, millions of users had their data on their profiles used for political ads motivated by ad tailoring (making ads specific to a target audience that would be most likely to interact with the ads). In response to this data breach, users felt like their privacy was violated by Facebook instead of Cambridge Analytica because Facebook failed to keep their personal information private, despite users agreeing to how their data was being used and Cambridge collecting the data based on users' public privacy settings. This movement on social media platforms was called the #deletefacebook movement, and social media was reevaluated in consumers' eyes as a whole, not just the Facebook company. Based on an adult multinational cross-sectional survey conducted in July and August 2017 with 4,684 respondents about privacy, trust in data institutions and trust in Facebook, researchers found when trust in Facebook increases, users have a higher level of trust in all data institutions (Rosenthal et al., 2020). Users that chose to not delete or "abandon" facebook decided to change their privacy settings and usage patterns in an attempt to regain control of access to their personal information (Bright et al., 2021). Information online flows in unpredictable ways in the eyes of the consumer, but the companies know exactly what data is collected and used. Because of this, it is impossible to remain anonymous online and to truly keep your data private, even with a private profile (Quinn & Papacharissi, 2018). In addition, individuals often think their online social network is smaller

and more close-knit than it actually is, or users forget to change their privacy settings after a network growth. Something as simple as this can lead to a data leak to unintended recipients.

Data Reduction

While privacy concern increases, trust in Facebook, trust in data institutions, and acceptance of information personalization significantly decreases (Rosenthal et al., 2020). As mentioned before, in order to combat these privacy concerns, users that feel their online data has been violated exhibit behaviors to reduce the amount of their online information in an effort to take control of their data. Despite the #deletefacebook movement, users are more likely to find coping mechanisms for social media usage and behaviors instead of not using the social media platforms altogether.

Users that understand what measures to take to truly protect their personal data are considered to be extremely privacy literate, while those who do not understand online privacy and data collection practices are privacy illiterate, but are less trusting of companies than those with a higher privacy literacy (Rosenthal et al., 2020). Those with a lower privacy literacy enact more privacy protections against people, such as blocking previous friends, making their profiles private, or untagging themselves from photos, while those with a higher privacy literacy take actions against data collection by companies by using a pop-up blocker, proxies or other advanced techniques (Quinn & Papacharissi, 2018). Apart from reducing their data, the only time people are comfortable with sharing more data with companies is for convenience, such as disclosing personal information for personal gain or personalized content.

Readability of ToS

Currently no laws exist that govern the complexity or understandability of any legal contract including Terms of Service and Privacy Policies, but these are necessary to retain user

trust (Yerby & Vaughn, 2022). A privacy policy is a contract, and companies making the diction extremely high-level is the equivalent of a company not letting people read their documents before making them sign them. In order to truly protect personal information, users must become aware of what the ToS actually says before inputting all of their information on an online profile. Of course, most users do not read the ToS because companies are required to be extremely specific, so most user agreements are written in legal jargon not capable of being understood by the general public, and they are confusing. One company, Neopets, provides a means to delete/reject trackers, but they do not provide an explanation or instructions on an opting-out procedure, making it impossible for users to keep from sharing their data (Venger, 2017). Because of the unreadability of ToS agreements, they are often ignored by consumers (Chawdhry et al., 2022). It is more convenient to skip past the ToS because it is quicker, and users often want to feel the gratification of using the app past the sign-on pages.

Concerns for privacy risks are disregarded for convenience and connectedness. When information about the contents of privacy policies are actually given to users, they are not too keen on continuing to use the service. In a previous study, users were asked about the privacy collection practices of some of their platforms. When informed about what the companies actually collected for data or used the data for, 49.57% of participants stated they plan on making changes in how they use the device/technology, yet 87.2% percent of respondents showed a high degree of privacy concern (Chawdhry et al., 2022). This shows that most of the respondents were unaware of the privacy practices of that particular platform. On top of this, more than half of Pew Survey respondents held wrong assumptions about the purpose of privacy policies, proving most people do not even know what the privacy policy or ToS actually means (Venger, 2017).

On top of the other readability issues, users cannot read the privacy policies if they do not exist. App store companies such as Google and Apple allow developers to submit policy links without checking to see if the links are valid or if they actually lead to the privacy policy. Close to 50% of the apps in the Google Play Store do not have working privacy policies (Alamri et al., 2022). Apart from there not being a privacy policy available, occasionally, users do not have a chance to read one before their data is collected. This collection of user data before consent is known as data leakage and in an analysis of 2,000 apps in the Google and Tencent app stores, it was found that 155 apps had data leakage or potential data leakage, and 716 apps had data acquisition before user permissions were granted before user consent to the privacy policy occurred (Liu et al., 2022).

Research

Currently, there is little data focusing on the difference between the actions of those who read the user agreements and continue to use the app without reading the ToS agreements. The closest theory that represents digital privacy management is the Communication Privacy Management (CPM) theory. Typically occurring in relationships, it discusses how people feel that they are the owners of their information, and in relationships, set and maintain boundaries around their information. Turbulence is created when a party feels their information has been breached. This relates to concepts presented in this proposal because relationships exist between used social media platforms and their users (Petronio & Child, 2020). When a company decides to not have a user as a consumer anymore, companies will use the phrase “ending our relationship” and when a company violates the user’s privacy, backlash occurs. This includes the response from Facebook users following the Cambridge Analytica data breach. CPM theory can

be used to further examine how users manage their data and view their relationship with online platforms, specifically those managing personal data.

The goal of this research proposal is to figure out if those that spend more time reading the terms of service will have less engagement on social media, and will be less likely to share more information about themselves online. This is necessary in order to examine whether users are being taken advantage of, and why they continue with information-disclosing practices despite their knowledge of privacy practices.

H1: Those who spend greater time reading the Terms of Service will have less personal data submission on social media.

H2: Those who do not have access to the Terms of Service will have the same level of personal data submission as those who have access to the terms of service, proving the tendency to not read the ToS.

H3: When the key points of the ToS are shown to participants, they will decide to decrease the amount of data they originally submitted before they viewed the ToS summary.

Method

Participants

The participants of this study (at least one-thousand final responses) will be anyone that is familiar with using social media platforms and technology in general. The intended age of the participants will be anyone who is above the age of 18. This is because of the complicated readability of the terms of service agreements. Children are not able to read these agreements which means adults are the only ones that can participate in the experiment. At the same time, adults are the only ones who have experience using technology and can figure out without adult help how to navigate social media platforms. I would like to use snowball sampling in order to reach a wide range of participants for different demographics. I am aiming for the same

representation of demographics, excluding those under the age of 18. The actual online experiment platform where participants respond is the last thing needed to conduct this research.

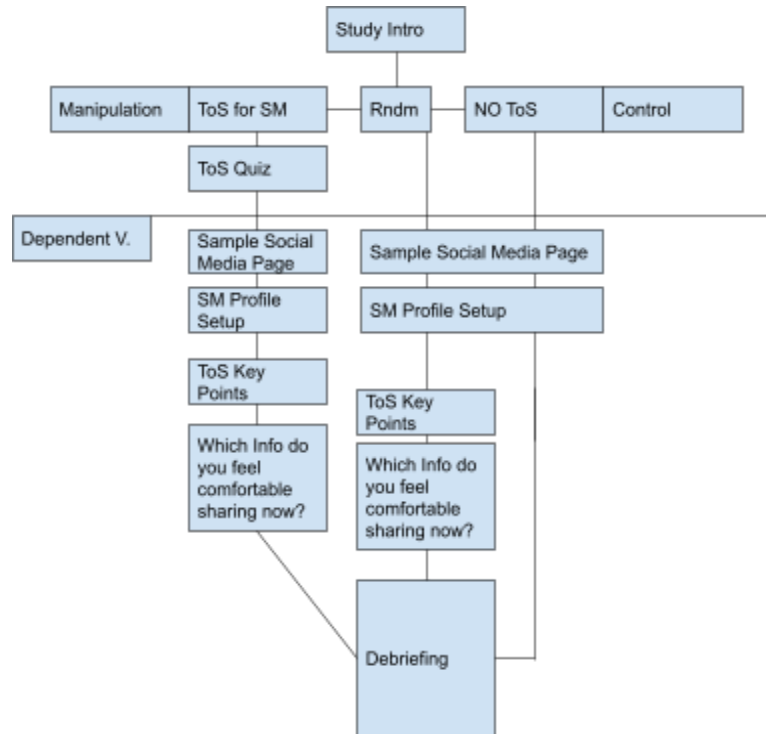
Materials

One of the materials that can be used in the experiment is a sample social media page. This will be made as an original document, not mimicking an original platform. The new original document will be used to immerse the participants in an online environment that is similar to the media they already use. Second, user agreements / privacy policy agreements are crucial to the research. This agreement must be drafted specifically for this study because it must be noted for both of these resources that any material used for this study should be original to the study to prevent existing platform bias.

Procedure

For the procedure, I would start with an online experiment made on qualtrics. The template provided at the end of this proposal is created from a blank survey, and it randomizes participants into 3 groups. A better way to visualize this is to look at the experiment on qualtrics that is attached at the bottom of this proposal, or one could follow the flowchart showing how the experiment was built. The flowchart is attached directly below in Figure 1.

Fig. 1



I would start with the introduction to the study and what participants should expect, along with ensuring that the data is confidential. After that, I would randomize participants into three groups - the manipulated group, control group and validation group. For the manipulation group, I would show them the terms of service for the sample social media platform and have the time spent reading the page timed to rule out those who did not read the ToS eliminated. After the ToS, the manipulated group will have a quiz about the information on it. If they fail, they will be sent to the ToS key points and then to start the dependent variable when finished. The control group will not have access to the ToS, but they will be sent to the dependent variable immediately. The validation group will have the same steps as the control group, but with an added option of changing the data they would like to submit after viewing key points of the ToS.

All three groups will be shown a sample social media page. Then, after reading, all groups will start selecting the data they feel comfortable sharing in the sample social media page

block. After that, the validation group will be sent to a block of information on how their data will be used by the company. These participants will be asked if they would like to switch which information they share with the company and why they would like to switch which information is shared. After, they will be sent to a demographics section, and the end of the experiment. A third group will go straight from the profile set-up page to the end of the survey. During the end of the survey, demographic information will be recorded along with what/who referred them to the survey, and why they chose to input or not input the information they did.

Measures/Data Analysis

The first thing I would do before analyzing the data is to scrub the dataset for missing/incomplete data, removing the answers of participants that did not finish the experiment, providing for more accurate conclusions. Then, for each section of the experiment in qualtrics, I would summarize the sections by averaging out responses for better visualization and understanding. This experiment will prove or disprove that people who know about the privacy policies of social media companies will be less willing to input their personal data, and those that do not know about the privacy policies will be more willing to input their data. The “why” question will also be analyzed and open-ended to see why people chose to input their data based on them seeing or not seeing the ToS, or changing their answers after the ToS was shown to them after the initial input.

When it comes to testing the hypotheses, I would test H1 by running a Pearson correlation between time spent reading the ToS and the amount of personal data submitted by participants. If there was a statistically significant negative correlation, H1 would be supported, proving as users actually read and obtain knowledge from the ToS, they are more likely to submit less personal data. If the chart does not show a downward trend, then H1 is not supported.

In order to test H2, I would use an Independent t Test/Parametric Test between those who have access to the ToS and those who do not have access to the ToS, and the amount of data submitted by both of these groups. If these two groups look the same when compared, H2 would be supported proving people do not read the ToS or privacy policy documents before submission of data occurs, regardless of if the ToS was present or not. A Pearson Chi-Square test is necessary in order to test H3. This will compare two groups, the control group and data reduction group, where only one group has the option to decrease their data after their original submission after being shown the key points of the ToS, providing a smaller, more understandable version of a standard ToS/privacy policy. If the participants in this group decrease the amount of data they chose to submit, and there is a statistically significant negative correlation from final data submission and data submitted before ToS, H3 will be supported, proving if people actually read how their data is used, they will feel less comfortable submitting data.

Discussion

For results, I expect to see all three hypotheses proved true. I believe that most of the participants in the manipulation will not read the ToS, or they will skip past it as soon as possible. For those in the control group, I believe all data submitted by the control group will match the same data as the manipulation group. Most of the data submitted will be from those who spent the least amount of time watching the terms of service. Some of the participants may read the entire terms of service or spend a vast amount of time doing so, but I believe they will be outliers and most of the participants will view for 30 seconds or less. The third group, branched off of the control group, will be responsible for proving H3, and I think that once people see how their submitted data is being used, they will not want to submit their data,

proving that people who submit their data are people do not know how their data is being used, or are unsure of the information presented in the ToS.

Although this study has not been conducted, I expect some limitations. First, readability of terms of service documents proves an issue. Those in the manipulated group who have the terms of service may not be able to read or understand the document if they wished. This would then make them similar to the control group, and the difference cannot be measured between the two main groups in these cases. This proposal also does not include all ages, so although teenagers are major users of social media, they cannot be included in the study due to the readability of the ToS. If an existing company's ToS/Privacy Policy is used for the experiment, users may already know the risks associated with the company and the user's information and may feel uncomfortable submitting information, interfering with results in both the control, reevaluation and manipulation groups. If this study is conducted in the future, I recommend drafting up a Terms of Service agreement of a company users are not familiar with or sample, with a similar set of terms.

Sample Experiment URL:

https://snc.qualtrics.com/jfe/preview/previewId/fd853e97-4e59-4851-9f72-dd52e96f4f5a/SV_b44zIPS89qHjaVU?Q_CHL=preview&Q_SurveyVersionID=current

References

- Alamri, H., Maple, C., Mohamad, S., & Epiphaniou, G. (2022). Do the Right Thing: A Privacy Policy Adherence Analysis of over Two Million Apps in Apple iOS App Store. *Sensors* (14248220), 22(22), 8964. <https://doi.org/10.3390/s22228964>
- Bright, L. F., Lim, H. S., & Logan, K. (2021). “Should I Post or Ghost?”: Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing*, 38(10), 1712–1722. <https://doi-org.snc.idm.oclc.org/10.1002/mar.21499>
- Cain, J. A., & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society*, 24(12), 2705–2724. <https://doi-org.snc.idm.oclc.org/10.1177/14614448211000327>
- Chawdhry, A., Poullet, K., & Pinchot, J. (2022). Internet of things: Measuring data privacy concerns of users. *Issues in Information Systems*, 23(4), 94–110. https://doi.org/10.48009/4_iis_2022_109
- Liu, K., Xu, G., Zhang, X., Xu, G., & Zhao, Z. (2022). Evaluating the Privacy Policy of Android Apps: A Privacy Policy Compliance Study for Popular Apps in China and Europe. *Scientific Programming*, 1–15. <https://doi.org/10.1155/2022/2508690>
- Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of Communication Privacy Management theory. *Current Opinion in Psychology*, 31, 76–82. <https://doi.org/10.1016/j.copsyc.2019.08.009>

Rosenthal, S., Wasenden, O.-C., Gronnevet, G.-A., & Ling, R. (2020). A tripartite model of trust in Facebook: acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology*, 23(6), 840–864.

<https://doi-org.snc.idm.oclc.org/10.1080/15213269.2019.1648218>

Quinn, K., & Papacharissi, Z. (2018). The Contextual Accomplishment of Privacy.

International Journal of Communication (19328036), 12, 45–67.

<https://search-ebscohost-com.snc.idm.oclc.org/login.aspx?direct=true&db=ufh&AN=139171388&site=ehost-live&scope=site>

Venger, O. (2017). Internet Research in Online Environments for Children: Readability of Privacy and Terms of Use Policies; The Uses of (Non)Personal Data by Online Environments and Third-Party Advertisers. *Journal of Virtual Worlds Research*, 10(1), 1–15. <https://doi-org.snc.idm.oclc.org/10.4101/jvwr.v10i1.7227>

Yerby, J., & Vaughn, I. (2022). Deliberately confusing language in terms of service and privacy policy agreements. *Issues in Information Systems*, 23(2), 138–149.

https://doi.org/10.48009/2_iis_2022_112