Issues in Information Systems
Volume 22, Issue 3, pp. 145-159, 2021

DOI: https://doi.org/10.48009/3_iis_2021_159-174

Current privacy policy attitudes and fair information practice principles: A macro and micro analysis

Jacob Klemovitch, *Undergraduate, Penn State University, jck40@psu.edu*
Lauren Sciabbarrasi, *Undergraduate, Penn State University, lms529@psu.edu*
Alan Peslak, *Penn State University, arp14@psu.edu*

Abstract

In an increasingly technology dependent and digitized world, the privacy of users' personal data is a growing concern. Unlike the European Union (EU), with their General Data Protection Regulation (GDPR) requirements, the U.S does not have any nationally accepted privacy policy standards other than guidelines in the Fair Information Practice Principles (FIPP). This puts the onus on companies to create ethical, clear, and transparent privacy policies. The incorporation and effectiveness of just these general non-binding FIPPs was the focus of our study. A literature review and developing, distributing, and analyzing a survey about the privacy policy attitudes and behavior and well as specific wording and contents of the Uber and Lyft privacy policies fulfilled our goals. The results and conclusions from this study found a disconnect from the guidelines found in the FIPPs and the respondents' expectations of privacy. A contrasting difference between older and younger age groups' behavior towards privacy policies was also discovered.

Keywords: Privacy, Privacy policies, Fair Information Practice Principles, Fair Information Practices

Introduction

Many people rely on smartphone applications, websites, and programs for their day-to-day activities, most of which have a common factor: each contains a privacy policy. These policies are written to disclose usage of private data by the application, website, or program. Past studies indicate that privacy policies have fundamental problems. Das (2015) studied the readability of privacy policies and found that after analysis of 64 youth centered privacy policies, all the policies are rated above the average reading level of adults in the U.S. The average reading level of US adults in 8 or 8th grade. Another study from Gerlach (2014) claims that privacy policies contents are an integral part of a business model and have a direct impact on monetization of information gathered. There is an monetary incentive for loose policies. Our case study was conducted with two specific goals, using general privacy policy questions and Uber and Lyft privacy policies as a basis for research. The first goal was to evaluate the effectiveness of privacy policies on informing consumers about the handling of their personal data. The second was an analysis of what the public expects a privacy policy to entail, compared to the realities of such policies.

Consumers are often unaware of what data are being shared and to whom. Consumers have differing thoughts and opinions on how they value privacy and what is acceptable for companies to do with their

collected data. Readability and assumed questionable motives of companies' privacy policies content are by and large left unaddressed by the current regulations in the U.S.

The most glaring issue of privacy policies, specifically in the U.S are the 'ambiguous' guidelines and requirements for companies to create policies. There is no overarching federal law specifically stating that all companies that collect data must post a privacy policy. The FTC (Federal Trade Commission) in 1998, released the universal guideline to privacy policies in *Privacy Online: A Report to Congress* called the Fair Information Practice Principles also known as FIPPs. Stating the five core principles of fair information practices (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. These 5 sections are recommended for privacy policies, although they are not explicitly required by law. It should be noted that there are other federal laws requiring privacy notices and specific standards such as Children's Online Privacy Protection Act, Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act which focus on the handling of data for children, health records and banking and financial records, respectively. These types of data handling are not the focus of this article.

In a 1995 law review, the basis of privacy in the United States, specifically states that "Privacy" is used as a catch-all term and is used from describing government intrusion in the bedroom to the inviolability of telephone communications and that the FIPPs falls under the broad label of privacy. Regardless of being under this label the standards are distinctly focused on maintaining integrity of personal information and fairness to individuals that the data relates, and specifically applies to the storage use and disclosure of personal information (Reidenberg, 1995). To determine the adequacy of privacy policies in informing the consumer as they currently exist the recommended principles are analyzed.

Notice/Awareness: "Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information." (Federal Trade Commission, 1998, p. 7). Essentially, the consumer needs to be informed if information is being collected, of what information is being collected, and where it will be going or what it will be used for.

Choice/Consent:" Choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — i.e., uses beyond those necessary to complete the contemplated transaction." (Federal Trade Commission, 1998, p. 8). The privacy policy should contain an option for people to opt out of data collection. Examples include limiting functionality of a given application or service, or suggesting to not use the service altogether if the consumer refuses to have their data collected.

Access/Participation: "It refers to an individual's ability both to access data about him or herself — i.e., to view the data in an entity's files — and to contest that data's accuracy and completeness" (Federal Trade Commission, 1998, p. 9). In other words, the policy needs to allow for a user to see their own data that have been collected by the service. This ensures data accuracy for the consumer and the service being provided, while providing transparency for the given service.

Integrity/Security: "Data must be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form." (Federal Trade Commission, 1998, p. 10). This principle gives guidance to what companies should

do for security of data. The overall concept is that data need to be secure through technical measures and physical ones.

Enforcement/Redress: "Core principles of privacy protection can only be effective if there is a mechanism in place to enforce them." (Federal Trade Commission, 1998, p. 10). This section specifically addresses some of the ways for non-compliant companies to be penalized when not adhering to the other four principles. It gives the option for self-regulation through external audits and at the minimum making sure consumers' concerns are addressed. A second option includes private remedies, like creating private rights for consumers harmed by a company's privacy practices. Government enforcement, through criminal or civil penalty depending on the nature and severity of the issue or violation that has been committed, is an alternative option.

Literature review

There have been various studies on privacy policies, some of which include the user's understanding and retention of policies, the policies' length, analyzing user's privacy values and comparing that to the actions of the users. As mentioned in the introduction, the FIPPs are the basis of privacy policy development in the U.S, and are the primary focus of research.

The first core aspects of privacy policy research are the FIPPs. More specifically, are companies that are collecting data and have a policy, following the guidelines? A 2012 study regarding 30 Dow Jones companies' adherences to the Fair information practice principles, they found 43.33% of companies do not comply with the Choice principle in all aspects, and 66.67% do not fully comply with the Access principle. (Li, 2012). As the FIPPs are widely understood as the universal basis to privacy statements this is a significant percentage, especially in the context of the highest stock market value companies at the time.

The legal implications and effect of the Fair Information Practice Principles itself has been under analysis since its creation as well. In an Iowa law review of the FIPPs Reidenberg (1994) writes on the standards of personal information in the U.S.

> "There is a lack of transparency for the treatment of personal information, abundant secondary use of personal information, weak enforcement of fair information practice standards, and a misallocation of standard-setting responsibilities." (p.529)

This review was written prior to the report to Congress outlining the Notice, Choice, Access, Integrity and Enforcement guidelines but still holds true in the loose standards that were set for companies to adhere to in relation to data privacy. Recent law reviews have revisited the FIPPs and points out some of the negatives and positives to its approach to data privacy, a review from Maryland states that the FIPPs articulate desirable endpoints such as openness, security, data equality and accountability but fail to specify the design to facilitate actions to get to the desired endpoints (Hartzog, 2017).

As the standards for personal information data collection have remained relatively consistent through the digital age, this begs the question: do consumers today value their own personal information and privacy? A 2019 study illustrates the current level of concern and willingness to provide personal information to digital marketers (Facebook, Google) through a survey of 2,416 Americans, 70% of respondents reported feeling very concerned or somewhat concerned about their private data being collected, in addition 53% of their respondents stated that they had some understanding, limited understanding or no understanding of the information collected on them (Winegar, 2019,). These data speak for themselves suggesting that there is a wide concern for data privacy in the U.S. Large groups of individuals do not have a comprehensive

understanding of what data are being collected. The inherent issue builds off the pitfalls of the FIPPs and the history of poor standards in data collection, which breeds an inherently ambiguous privacy policy. The exact cause for the issue is the privacy policy itself.

Based on previously mentioned surveys and studies individuals have heightened interest in personal data security. The crux of the matter is a lack of understanding on what data are collected initially. Typical users might fall into this category by skimming or completely ignoring the privacy policy altogether. A study done in 2018 found that in studying users' demand for privacy, the individuals' intentions and motivation need to overcome barriers such the long and complicated language of policies, available time, and their own technical and cognitive ability to attain their desired understanding of online privacy (Rudolph, 2018). This language may be interpreted as if it is solely the user's own fault for lacking motivation to look out for their own wellbeing. Although instead of looking towards the user as the potential issue, policy readability, length and common standards for privacy policies may better be held responsible.

As evidenced by various sources regarding FIPP topics, the value of consumers' data privacy, and privacy policies, issues are evidently complex and compounding one another. Our testing methodology was designed with the underlying issues in mind, thus allowing for a clearer picture regarding privacy policies as a continuous worry for online consumers.

Methodology

Our study was conducted using a combination of privacy policy research driven areas and its goal is to answer the following questions:

At the Macro level:
Do consumers read privacy policies?
How do consumers value their personal privacy?
Is there a difference in behavior surrounding privacy policies based on demographics?
At the Micro level:
How does Uber and Lyft follow the fair information practices principles?
Are consumers familiar with Uber and Lyft privacy policies content?

Our research objective was to examine current privacy policy attitudes using both general questions as well as ones specific to a particular industry. In this way, we believe we could obtain a more comprehensive understanding of privacy policies and FIPP in use today.

Uber and Lyft Privacy Policies

Prior to preparing our survey, analyzed two specific privacy policies from competing companies. Uber and Lyft were prime candidates for this study to gauge their adherence to recommended FIPPs. These ride sharing services were chosen because of their popularity and mainstream qualities. Their services are dependent on using a phone application and as such, all their customers are presented with a privacy policy. Additionally, both applications use location tracking, collect personal data and process payments. As a first step, Uber and Lyft's policies were broken down from the perspective of Notice, Choice, Access, Security, and Enforcement.

FIPPs Analyses

FIPPs Notice: Both Uber and Lyft privacy policies contained sections on what data they are collecting and how they are using the collected data. Uber's privacy policy contained the information essential to the Notice principle in two overall sections of the notice and four subsections. Notable qualities of their policy include a section indicating that if there were to be significant changes users will be notified through email or the app. Aside from the EU, the consumer's choice to continue using the application counts as their consent to any and all changes made to the policy. A similar statement is made in the Lyft policy and information that is required to fulfil the Notice principle were in four main sections and five subsections.

FIPPs Choice: The aspect of choice was also dedicated in one section in each the Uber and Lyft policies. The Lyft policy specifically names several data tracking functions that the user can opt out of such as email subscriptions, text messages, push notifications, location information, and cookie tracking. Notable data that the user does not have control over are the "do not track" feature on browsers and the retention of certain data when deleting an account for business purposes and legal reasons. Uber contained overall similar opt-out options for their service, the specific practices on cookies and the deletion of data were contained in separate sections which made the information difficult to find. The section on deletion of data specifies that data will be stored and used for seven years for purposes of safety, security, fraud prevention and detection, and research and development.

FIPPs Access: Both Uber and Lyft have less information respective to notice and choice. This principle largely builds on other principles such as Choice. The Uber policy specifically states that they enable Access and Control through in-device settings, device permissions, in-pp ratings pages and marketing opt-outs. Additionally, Uber allows users to request access to their data, deletion of their accounts, and/or that Uber restricts its processing of user data. Lyft provides one statement on this principle stating that the user has the ability to access and delete their information and exercise other data rights, such as California's privacy rights.

FIPPs Security and Enforcement: These two principles are the least focused in the Uber and Lyft privacy policies and most other privacy policies. Uber's policy highlights Enforcement by stating users can submit a concern or a complaint through Uber's help section. Lyft takes a similar approach where they have a section that users can contact them if there are questions or concerns related to the policy. Uber does not have a specific section on security. It does mention the use of collected data to improve the security of its apps or services, but otherwise has no specific statement of the protection of collected data. Lyft has a section dedicated to security of collected data in which they state they take reasonable efforts to keep data safe. but no security measures are 100% secure.

Overall analysis of FIPP in Uber and Lyft Policies: From our analysis of Notice, Uber and Lyft policies sufficiently cover what information they are collecting, and how they are using such data. This content makes up much of both privacy policies, although certain sections lack detail in how they use data, most notably in the Choice section. Through our analysis of Choice, it is found that the user is presented with a number of opportunities to limit data collection on them. When the option of Choice is not presented, both policies can be vague and confusing regarding what data are being retained and for how long. This is seen in both policies' statements on deletion of an account. Building from Choice, Access was another key area of analysis. Both policies mention and give a level of choice to Access their data. Both policies do provide adequate but not easily accessible ways for the consumer to access the personal information the apps have collected for most U.S users. Enforcement and Security are both integral to consumers' ability to maintain

data integrity, and report wrongdoing. These sections revealed that both Uber and Lyft do not have significant Enforcement on internal wrongdoings, or any third-party review on internal data practices. Additionally, mentions on data security only located in the Lyft policy, of which were vague and could be interpreted as a deniability of wrongdoing in terms of security breaches. The analysis from the FIPPs helped us focus on what the problematic areas are for these privacy policies and then helped us create the survey questions.

We also reviewed readability for each policy and found the Flesch-Kincaid grade level to be 13.9 for Uber and 11.1 for Lyft, well above the average readability for US adults.

Data collection

After analysis of both the Uber and Lyft policies based on the FIPPs, a survey through Qualtrics was created and distributed with proper Institutional Review Board (IRB) approval. The goal of conducting the survey was to attain a data set to gauge the public's reaction to some of the common concerns as privacy policies as a whole, their effectiveness, and Uber and Lyft specific practices addressed in their policies.

Survey questions can be broken down into three categories.

I. Respondents' expectation and understanding of common practices of privacy policies.
II. Respondent's overall value of their personal privacy.
III. Respondent's attitudes of Uber and Lyft specific questions on policy wording and practices.

All three categories of questions were distributed throughout the survey, with a total of 27 possible questions depending on which answers were received. Demographic questions such as age, occupation, and gender were also recorded to determine if there are any correlations between answers and demographics.

This survey was active from September 8th to September 23, 2020. There were several means of distribution for this survey, many results were obtained by directly sending a link to contacts and through Facebook and other social media sites. Another significant portion was obtained with the participation of professors sending the anonymous survey link to their IST classes. In total, 116 usable responses were recorded and analyzed to fulfill our research questions. All participants were 18 and older and were from the United States.

Results

Age and Gender

The age and gender of our survey size could have a measurable impact on how questions were answered and is important on how this data set should be interpreted. The average age for the respondents is 31.4, with a median of 21 with a standard deviation of 17.0. The gender of 58.8% of respondents were female with the rest being male, preferred not to say or other. In several cases age played a measurable relationship to how certain questions were answered. Gender had no measurable impact in any question's responses.

As mentioned previously, the survey questions can be grouped into three categories this first section displayed below are the questions pertaining to the respondents' understanding of the common practices of

privacy policies. Some questions that proved to be unneeded or inconclusive are omitted from the possible 26 questions to keep the focus and length of this article concise.

Respondents understanding of common practices of privacy policies

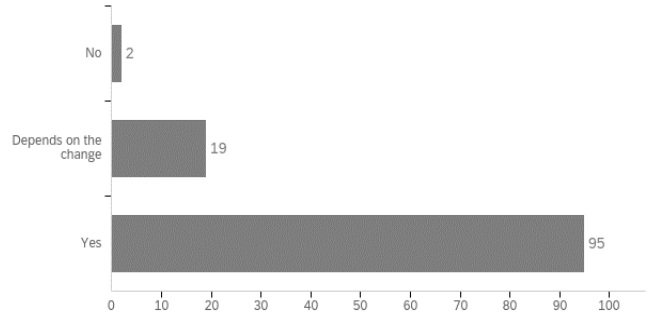

Figure 1 Q3 - If the terms of a privacy policy were to change, would you expect to be notified of these changes?

Q3: Most of the respondents would expect to be notified of a change, with a small but substantial minority choosing that it depends on what change was made. In the case of Uber, if the change is not deemed to be significant then users will not be notified. Although with both companies' users will be notified through the platform, or through email, which is standard practice for most privacy policies but is not something pointed out specifically in the FIPPs and is not explicitly required by law.

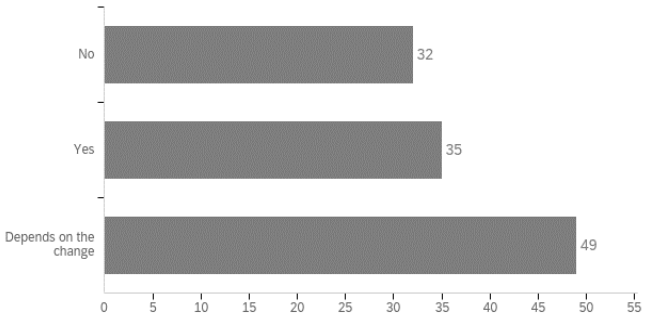

Figure 2 Q4 - Do you feel that "continuing to use an app after a privacy policy was changed" should qualify as consent to any and all changes made?

Q4: This question further builds on the previously discussed notification of a change. Where 42% of respondents chose that it "depends on the change made". The remaining respondents were essentially split between yes and no. In Uber and Lyft's case any use of their services after a change in privacy policy will count as consent to those changes made. This conflicting result indicates that privacy policies should define specific scenarios when continuing to use an app after a privacy policy was changed qualify as consent. Alternatively, they should consider not be using this practice at all.

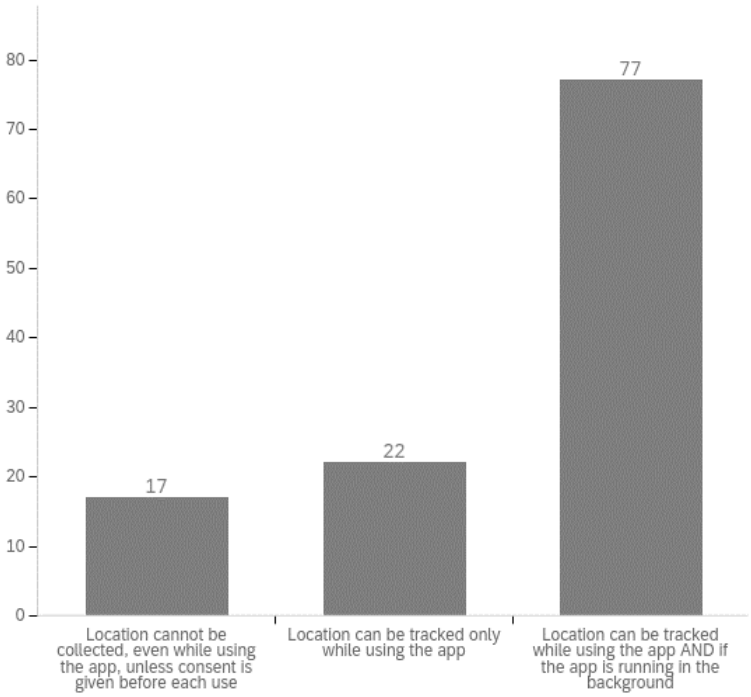

Figure 3 Q8 - Many phone apps use of location services. What is your current understanding of the scope of the use of "location services"?

Q8: Respondents appeared to be largely in touch with the regular practices when it comes to location services. 66% of respondents chose the standard collecting location data while the app is in use and in the background. In the case of Uber and Lyft location information is collected by default, in both applications location data can be disallowed although Lyft specifically states that "it may impact Lyft's ability to provide you our full range of features and services" (Lyft privacy policy).

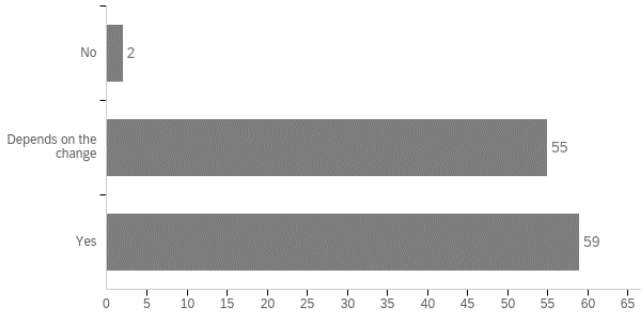

Figure 4 Q5 - Would you opt out of the collection of personal data when using an app, even if it results in "changes in the availability and functionality" of the app?

Q5: This question is largely an extension from question 8, to determine if respondents would give up features for privacy. The results indicate that half of the users need specific information on what features they are losing, and the other half would turn off data collection by default. As previously discussed, Lyft does explain that turning this off functionality will be lost, but does not go into specific detail.

Respondents overall value of personal privacy

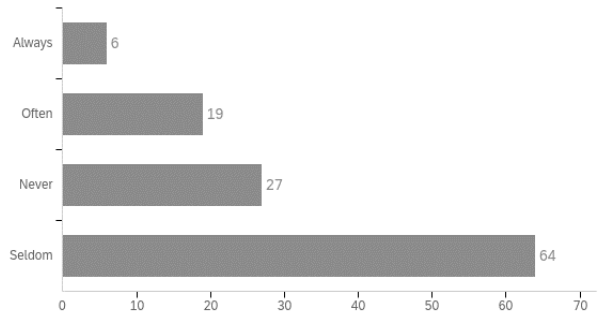

Figure 5 Q1 - Have you ever read a privacy policy of any online source or app?

Table 1 Ever Read a Privacy Policy

Q1: Have you ever read a privacy ...	Student	Other
Always	1.8%	8.6%
Often	12.5%	20.7%
Seldom	50.0%	58.6%
Never	35.7%	12.1%
Total	100.0%	100.0%

Q1: This question is a baseline to the remaining interpretations on the survey, and to attain a general feel for how much experience this pool of respondents has with privacy policies. 55% of respondents said they had seldom read a policy, and an additional 23% said they had never. This is significant because a large portion of the respondents have little experience with policies and may not be aware of the common practices presented in many policies. As you can see in the table, there is a large difference in responses from students versus non-students.

Table 2 Q6 - On a scale of 1-5: how important is the privacy and confidentiality of your data?

Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
Value (1-5)	1.000	5.000	4.379	0.877	0.770	116

Table 3 Q7 - On a scale of 1-5: how important is optimal and efficient functionality of an app?

Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
Value (1-5)	2.000	5.000	4.586	0.617	0.380	116

Q6/Q7: These questions directly recorded the respondents personal rating of privacy and how much attention they give to the functionality and efficiency of an application. The averages between the two values shows that efficiency and functionality of an application was universally held to a high standard by our respondents with an average rating of 4.59. Where privacy was also held to a high regard but was slightly lower with an average of 4.38.

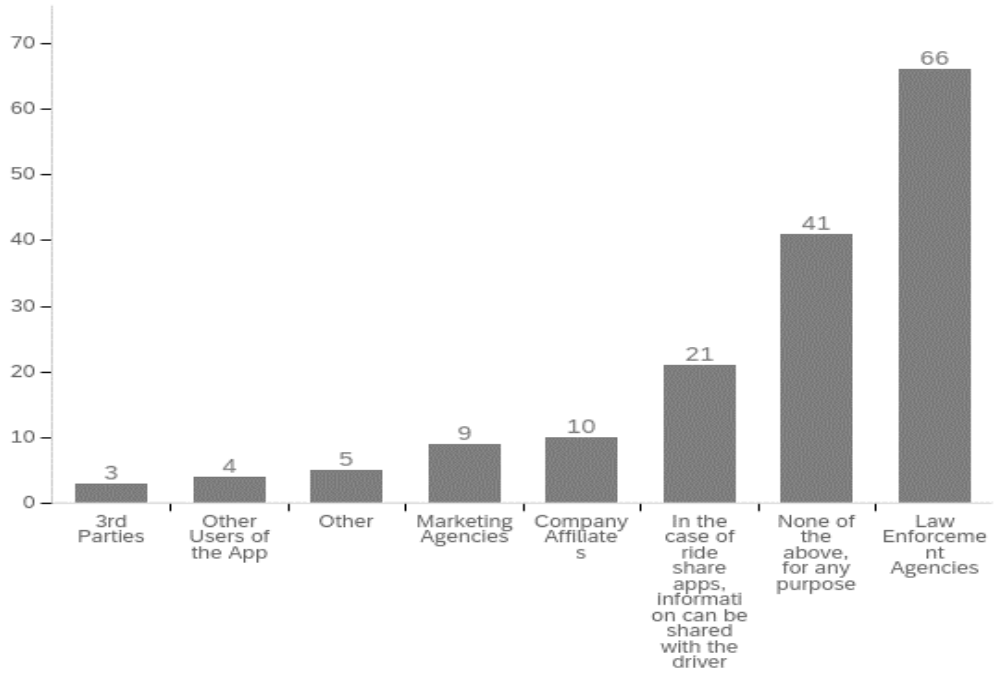

Figure 6 Q13 - What parties would you be okay with your data being shared with, for either your safety, the public's safety, marketing purposes, or a personalized experience? (select all that apply)

Q13: This question again is to record the respondents rating of privacy through asking what information is acceptable to give to whom. The most popular choice was law enforcement agencies where through comparison by age showed that a wide range of ages chose this response. Where on the contrary "None of the above for any purpose" averaged significantly higher. The last notable comparison are the remaining responses which collectively averaged a lower age than the average age of our respondents which is 31 years old.

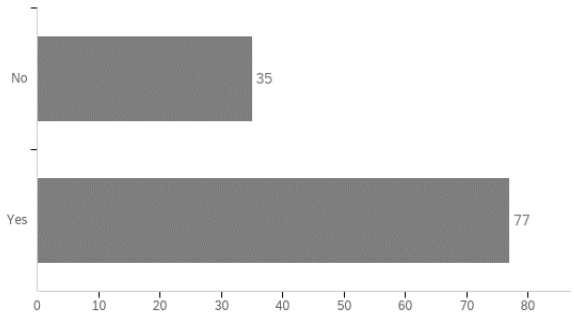

Figure 7 Q18 - Do you plan on reading privacy policies in the future?

Q18: This question is a reflection to gauge any effect on the previous questions in the survey which highlighted Uber and Lyft practices and other general privacy policy questions. A large majority of 68% chose that they do now plan on reading privacy policies in the future. The remaining portion of respondents choosing no showed to be the younger age group of the respondents at the average age of 22.5.

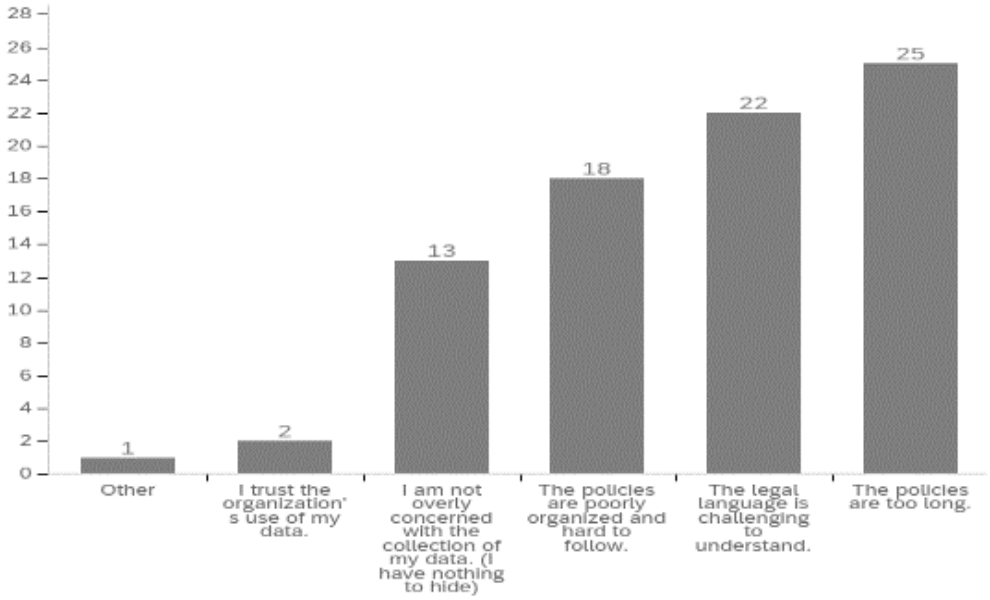

Figure 8 Q24 - Why do you choose not to read privacy policies? (select all that apply)

Q24: This question was only asked to those who chose seldom or never on Question 1. The results reflect what many other surveys on privacy policies have shown in the past including length and complexity. There were no noteworthy or conclusive demographics on this topic because of the limited survey size.

Uber and Lyft specific policies

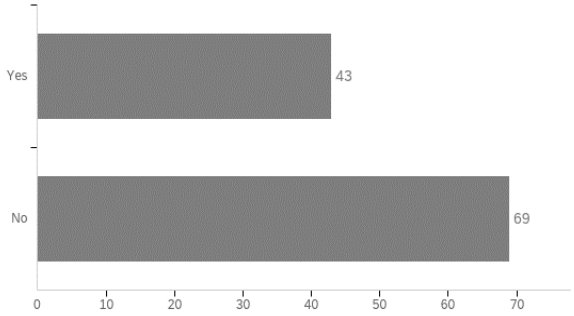

Figure 9 Q11 - Are you aware that your data, located in another individual's "address book/contact list", can be shared with Uber and Lyft without your direct consent?

Q11: This question such as the others in this section are to expose the respondents of the practices of Uber and Lyft listed in their privacy notices. Alternatively, they are also to remind Uber and Lyft users of information that they may have once read or have been exposed to. In this case, the majority of respondents were not aware of this current practice. Demographics did not show any significant relationship between age and response.

Table 4 Q12 - Both Uber and Lyft have the right to share (and sell in some cases) your data with various sources to create a profile about you. In general, are you comfortable with this?

Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
Please select a number	1.000	5.000	2.155	1.426	2.034	103

Q12: Respondents were overwhelmingly uncomfortable pertaining to the practices of Uber and Lyft sharing and, in some cases, selling their data. The average is very low at a 2.15 out of 5, the lowest results found on this survey.

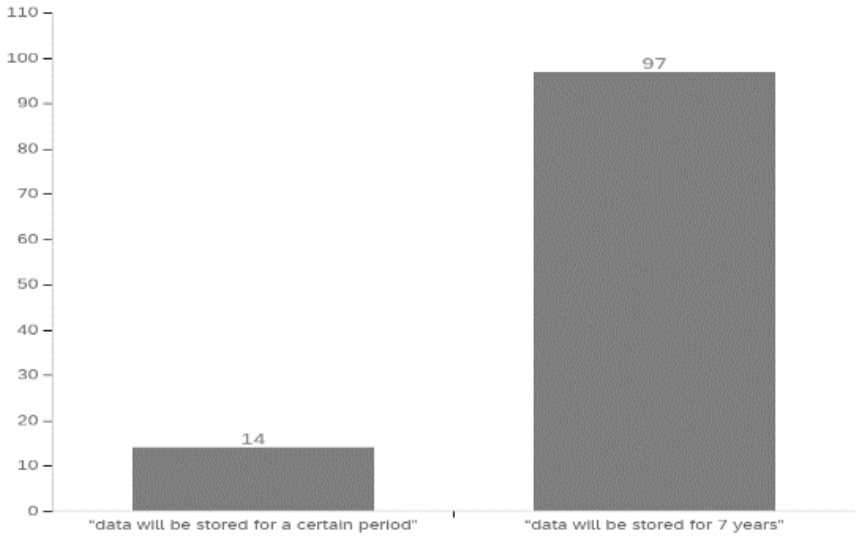

Figure 10 Q15 - Both Uber and Lyft keep data on file after deletion for research and development purposes. Which of the policy's wording do you prefer?

Q15: As seen at other parts on this survey such as the analysis on Q5 and Q8 the respondents do prefer choices with specificity. This is once again illustrated here with the overwhelming majority choosing the specific policy wording contained in the Uber privacy policy data will be stored for 7 years.

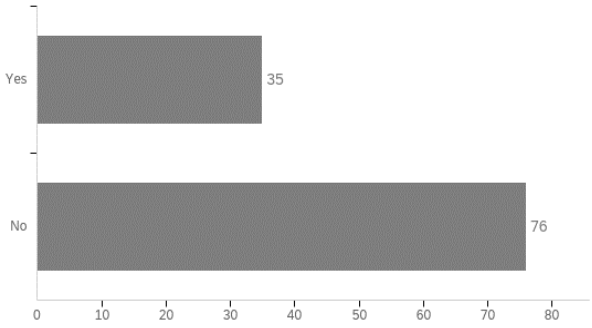

Figure 11 Q16 - In regard to policy enforcement, both Uber and Lyft indicate that any concerns can be sent to "HR and the Help Center". As a user, do you feel that this an adequate enforcement strategy to keep companies accountable for data security?

Q16: Policy enforcement as highlighted in the FIPPs is very important to maintain data integrity, and to hold privacy at a high standard. Uber and Lyft have chosen self-enforcement in order to maintain their standards. The majority of respondents did not agree with the HR and Help center as enforcement of wrongdoings being sufficient to keep the companies accountable.

Conclusions

There are various conclusions that can be drawn from the data set that was collected and the analysis of the results conducted in the previous section. Although the main goal of this study was to answer initial research questions, from our results and surrounding studies about privacy policies and the FIPPs it is evident that

they are not adequate to provide guidelines that consumers will agree with. For example, under the analysis of Q4, Q5 and Q15 the data show that consumers highly prefer specificity in regard to making choices about their privacy and their interpretation on what data are being collected and how they are being used. Other studies have found similar information when comparing the specificity, length, and visibility of a privacy policy. Specificity was found in by Capistrano (2015) to be the most important factor in consumers' perceptions of importance to deciding to share personal information. Furthermore, from our analysis, it was found that both Uber and Lyft generally followed the FIPPs. In particular instances, meeting the FIPPs requirements was not enough for the respondents such as seen in Q16. A significant portion of our respondents did not agree that self-enforcement was a sufficient way of data security accountability for a company dealing with personal information. Finally, respondents were mostly unaware of the Uber and Lyft's practices that are stated in their respective privacy parties. Overall, the data found in our research and others call for the potential need for reworking or replacement of FIPPs with clear specific and consistent rules for data privacy.

The demographics under analysis of the value of respondents' privacy revealed some interesting trends. The results for Q1 and Q18 show many of the younger respondents in the age range of 18-25 stated that they never read privacy policies and after taking the survey also said they would continue not reading privacy policies. On the contrary in Q13 many of the respondents that skewed older stated that they did not want to reveal any information to anyone for any purposes. This indicates that the older respondents are much more defensive about their personal information than the younger respondents. In both questions (Q1 have you ever read and Q18 plan to read in future) younger respondents sided contrary to most of the remaining respondents. The data do show a conflicting result in terms of demographics when looking at Q6 and Q7 where there was no statistical difference in demographic and respondents both valued privacy and efficiency of an application in a high regard. The statistical difference in the young age groups value of privacy should be a focal point to future works of research.

The last conclusion that can be drawn from this data is if consumers read privacy policies. Based on the respondents' answers on Q1 with the majority stating they seldom or never read privacy policies in most cases, consumers do not read said policies. Some of the reasons why consumers choose not to read these policies are answered under the analysis of Q24 with most respondents stating the policies are too long, complicated and unorganized, and also difficult to understand. Many studies have shown each of these to be problematic when it comes to privacy policies. Studies on policy length specifically show that shorter privacy policies lead to a higher retention of information for those that exert the required effort to retain and understand policies (Meier, 2020). A shorter privacy policy combined with the previously discussed changes to the FIPPs would address most of the general barriers on privacy policies and would improve privacy policies effectiveness on informing consumers.

Contributions and Limitations

This research had some limitations in terms of data collection and sample size. More specifically the sample size was a limited number at 116 results, more results may have resulted in different results or conclusions. Along the same lines of survey results, the population that was surveyed was largely localized along the east coast of the U.S most results coming from Pennsylvania and New Jersey. It is possible the limited diversity of the results may have impacted results as well. Further work is recommended in other areas of the US as well as Europe. For this reason, the data was compared with similar surveys, our data did corroborate with similar works of research with similar survey questions. Despite the limitations of the survey, this study contributes to the field of privacy policies, the FIPPs and the value of consumer privacy.

The analysis of the FIPPs on the Uber and Lyft privacy policies demonstrates how the guidelines are not fully adequate even when companies are following the standards set by the FIPPs. Further research on alternatives to the FIPPs in the U.S are an opportunity. The collected survey results and data is valuable to understanding consumers' value of privacy, and the resulting demographics data particularly in age groups sets the basis for further research. The contribution to theory is the successful approach in examining both specific privacy policies as well as general privacy policy concepts.

References

Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, *42*, 24-31.

Das, G., Cheung, C., Nebeker, C., Bietz, M., & Bloss, C. (2018). Privacy policies for apps targeted toward youth: descriptive analysis of readability. *JMIR mHealth and uHealth*, *6*(1), e3.

Federal Trade Commision. (1998, Jun) Privacy Online: A report to Congress.
Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems*, *24*(1), 33-43.

Hartzog, W. (2016). The Inadequate, Invaluable Fair Information Practices. *Md. L. Rev.*, *76*, 952.

Li, Y., Stweart, W., Zhu, J., & Ni, A. (2012). Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment. *Communications of the IIMA*, *12*(3), 5.

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. Media and Communication, 8(2), 291-301.

Reidenberg, J. R. (1994). Setting standards for fair information practice in the US private sector. *Iowa L. Rev.*, *80*, 497.
Rudolph, M., Feth, D., & Polst, S. (2018, July). Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. In *International Conference on Human-Computer Interaction* (pp. 587-598). Springer, Cham

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? a preliminary investigation. Journal of Consumer Policy, 42(3), 425-440.