AB testing Project Report:
The price for privacy - the causal effect between information and willingness to pay for privacy

Team 7
Christopher Weddle, Katian Harris, Laknath Gunathilake,
Ryosuke Kurematsu, Sanjana Parmar, Shrivatsan Ragavan

1. Executive Summary

The consciousness of consumers with regards to data privacy is slowly improving over the years, and this is especially true considering the increase in reported incidents of data breaches around the world. However consumers continue to practice unsafe behaviors online that cause loss of privacy. A hypothesis to explain this contradiction is the lack of sufficient information on the consumer's part. This gives rise to the question: does exposure to easily understandable information about data privacy entice customers to pay a premium for mobile applications offering premium privacy features?

To assess this, we implemented Randomized Control Trial (RCT) to obtain the causal impact of providing privacy information on the willingness of customers to pay a premium for enhanced privacy features in mobile applications. We had three treatment groups and one control group with the equal probabilities. We carried out the survey through Whatsapp and other social network services from November 18, 2021 to December 10,2021. The total responses are 224, and effective ones are 191.

The results of our regression analysis show no statistical significance and hence, we cannot find the causal effect. We also conducted a heterogeneous analysis using educational attainment, but were unable to observe the heterogeneous treatment effects.

2. Introduction

The general consumer awareness towards data privacy vulnerabilities has shown a steady growth in recent years. Recent surveys have found that as much as 65% of the respondents did not have confidence that their personal data is private.[1] Despite this awareness, there seems to exist contradictions in consumer's behavior in the mobile applications landscape. There exists vast literature exploring the possible rationales behind this privacy paradox. The explanations tend to vary from risk-benefit analyses, biased risk assessment and knowledge deficiency.[2]

The knowledge deficiency line of reasoning suggests that consumers' online behavior contradict their privacy attitudes as consumers lack complete information regarding the potential risks

[1] "Exploring Consumer Attitudes About Privacy - Future of Privacy Forum," *Https://Fpf.Org/* (blog), accessed December 10, 2021, https://fpf.org/blog/exploring-consumer-attitudes-about-privacy/.

[2] Susanne Barth and Menno D. T. de Jong, "The Privacy Paradox - Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior - A Systematic Literature Review," April 26, 2017, https://doi.org/10.1016/j.tele.2017.04.013.

associated with their behaviors in online platforms. However, human behaviour guided by bounded rationality and their general inability to process complex, technical information, could explain their paradoxical behavior.[3]

Our experiment aims to test this hypothesis of knowledge deficiency leading to paradoxical privacy behaviors. We wanted to understand if varying levels of information about data privacy had a causal relationship with a person's willingness to pay for privacy enhancing features. The growing demand for Privacy-as-a-Service in the current digital landscape suggests that there exists a possible positive correlation between awareness of privacy threats and willingness to pay for privacy enhancing services.[4]

The OECD privacy principles exists as a voluntary guideline for companies to follow with regards to data privacy. We leveraged this information to design a mock mobile application, which has a free version akin to the popular social media apps today, and paid tiers that give the users enhanced privacy preserving features. These features are based on the use limitation, collection limitation and individual participation principles of the OECD guidelines.[5]

Consumers, randomly split into treatment and control groups, would take part in a survey that introduces this mock mobile application. The treatment groups would be exposed to information about data privacy and privacy enhancing principles, while the control group would receive no information. The consumers would finally be presented with the option between the free version of the app and the paid versions that have better privacy.

Furthermore, to ascertain the negative impact of exposing the consumer to too much information, the experiment was designed to have three treatment groups. These treatment groups would differ in the amount of information they receive regarding data privacy, with treatment group 1 receiving minimal, surface level information and treatment group 3 receiving exhaustive information.

3. Experimental Design

The survey consists of four parts. The first part has three demographic questions about the participant. These questions ask for the person's age, their gender, and what their highest level of education is. The purpose of these questions is to see if there are differences in the treatment effect for different people through heterogeneous analysis.

The second part of the survey gives the participant information about InstaPro and the privacy features it offers. The participant is told what differentiates the free version from the paid version, and how much each additional privacy feature costs.

[3] Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *IEEE Security Privacy* 3, no. 1 (January 2005): 26–33, https://doi.org/10.1109/MSP.2005.22.
[4] Daniel Burrus, "The Privacy Revolt: The Growing Demand For Privacy-as-a-Service," *Wired*, March 23, 2015, https://www.wired.com/insights/2015/03/privacy-revolt-growing-demand-privacy-service/.
[5] "OECD Privacy Principles," accessed December 10, 2021, http://oecdprivacy.org/.

The third part consists of the treatment. 25% of the time, the participant will be placed in the control group, and will not see this third part at all. 75% of the time, the participant will be placed in one of the treatment groups and will receive additional information about data sharing policies and privacy guidelines(Appendix 1). The three possible treatment groups are:

- Treatment 1: Information about what data “free to use” apps share with third parties
- Treatment 2: The same information as treatment 1, plus information about OECD guidelines for Use Limitation, Collection Limitation, and Individual Participation
- Treatment 3: The same information as Treatments 1 and 2, plus an in depth explanation about how Use Limitation, Collection Limitation, and Individual Participation are implemented to keep user data secure

The fourth and final part of the survey asks participants to choose one of four options:

1. InstaPro with no add-ons, for free
2. InstaPro with No Sharing, for $1 / month
3. InstaPro with No Sharing and Metadata Collection Only, for $2/month
4. InstaPro with No Sharing, Metadata Collection Only, and Complete Control, for $3/month

To prevent the bias towards the first choice, we randomized the order of the four options.

For the survey implementation, we used Qualtrics to design and send the survey questionnaire. As a convenient survey, we distributed it through our network in CMU and other social networks like Whatsapp. The survey was carried out from November 18, 2021 to December 10, 2021.

4. Data

Data Exploration

We collected 224 responses from our survey. These responses include 191 completed surveys. The majority of our respondents are from the United States as shown in figure-1, and we also received several responses from individuals living in the South Asian region.

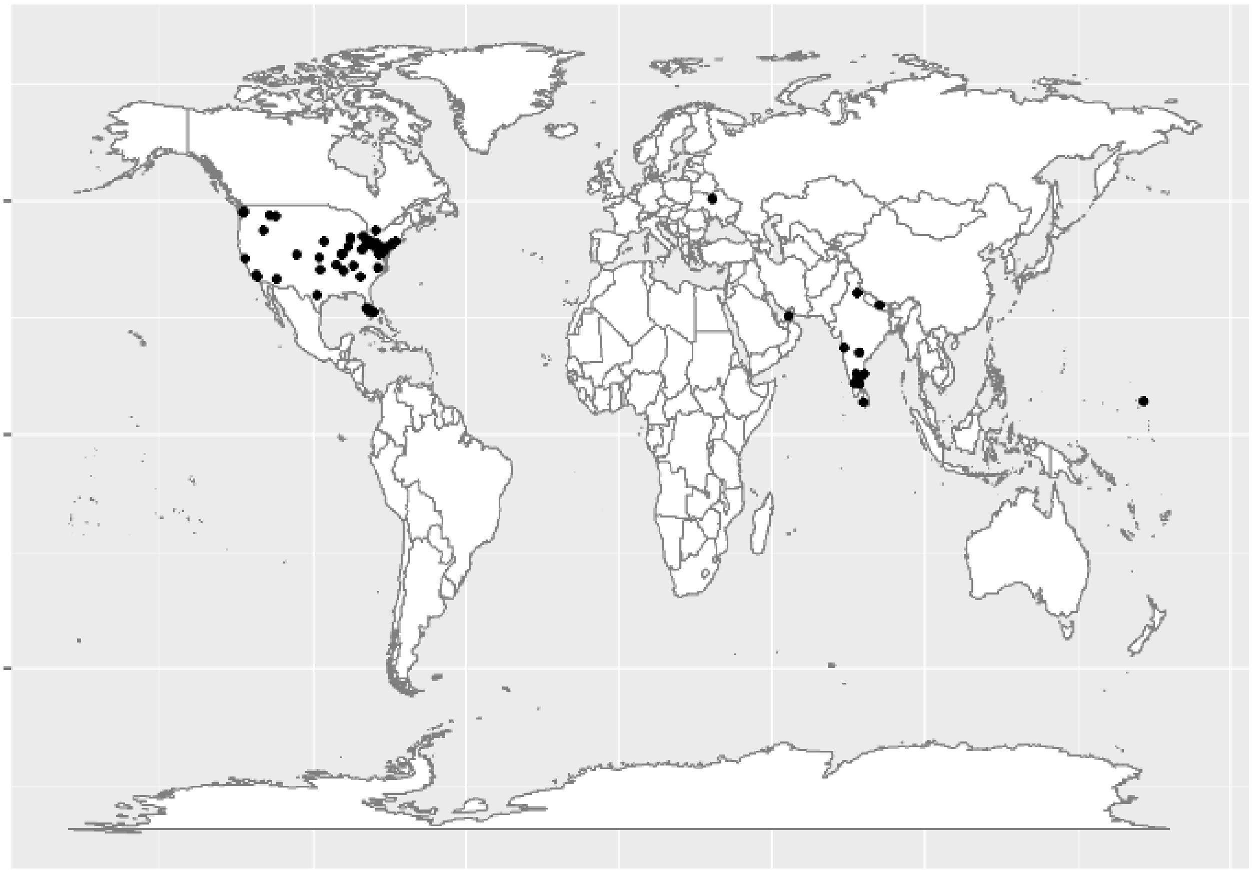


Figure (1)

Our treatment group consisted of 152 subjects, and the control group had 39. Figure-2-A shows the distribution of the treatment and control group, and Figure 2-B shows the distribution of the 149 treatment subjects across the three treatment groups. Our treatment group has more subjects compared to the control group. This allocation was intentional and part of our survey design. Since we had three subgroups within our treatment that received varying degrees of information, we wanted to ensure that each of the subgroups is assigned an adequate number of subjects.

The sample we collected included 95 female respondents, 95 male subjects, and one respondent that identified as Non-binary/third gender.

Most of the respondents in our survey had completed a four-year college degree. In addition to that, over 50 individuals had completed a Master's Degree or a Ph.D. The age distribution is shown in Figure-5 (displays that most of the subjects were between the age of 25-29 followed by those who are 35 or more

It is also evident from figures 4 that the age and educational attainment of subjects between the control and treatment groups are similar in characteristics although different in proportions. This is to be expected since we allocated more individuals to the treatment groups

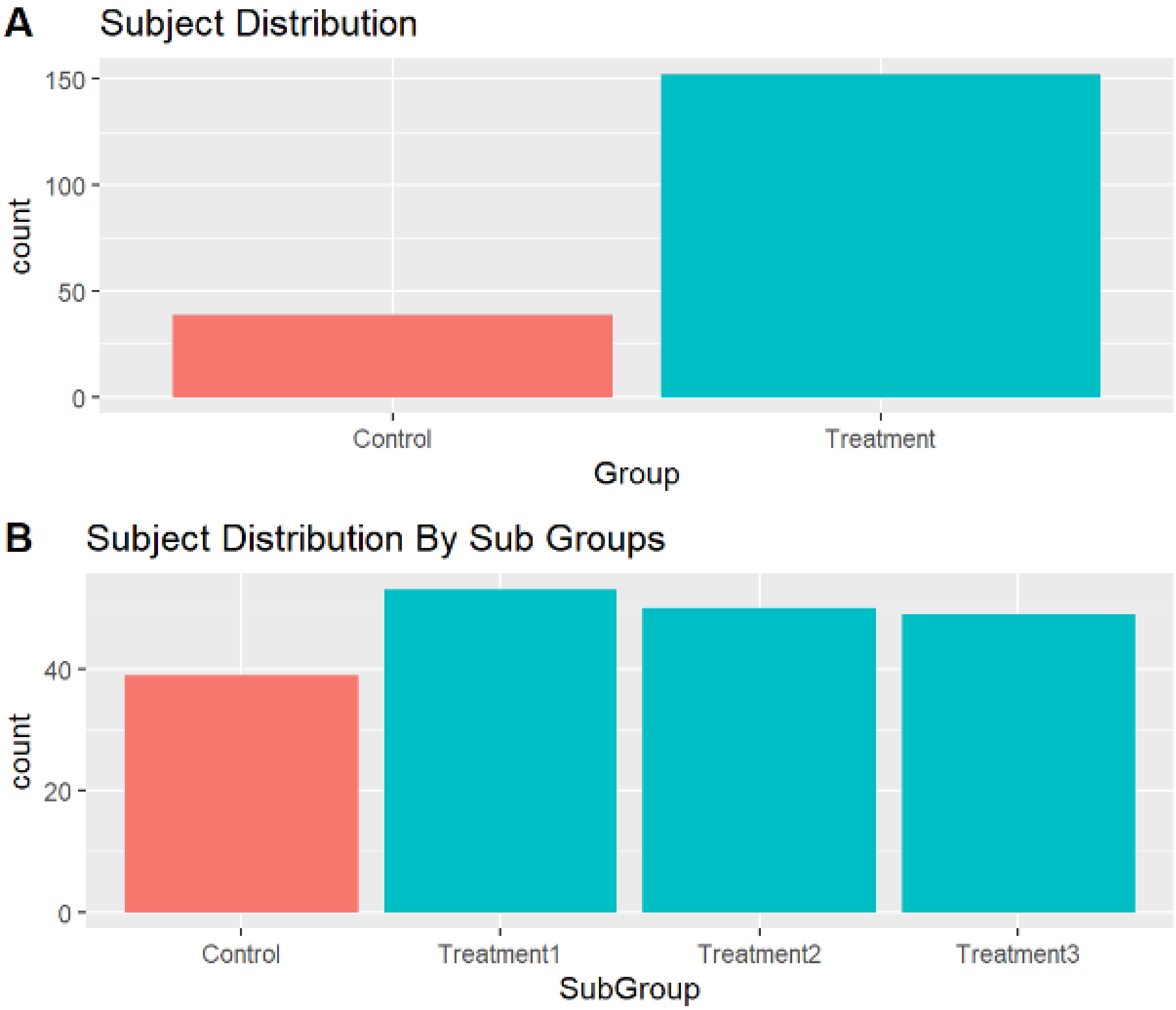


FIgure (2)

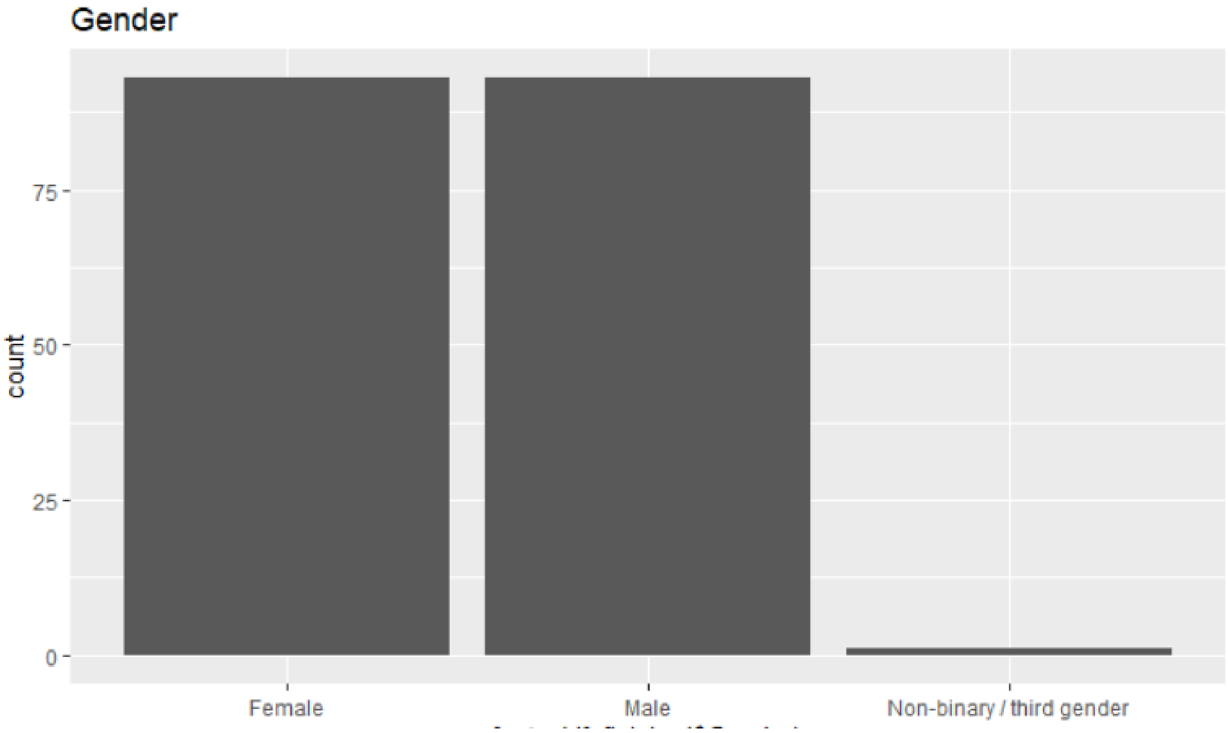


Figure (3)

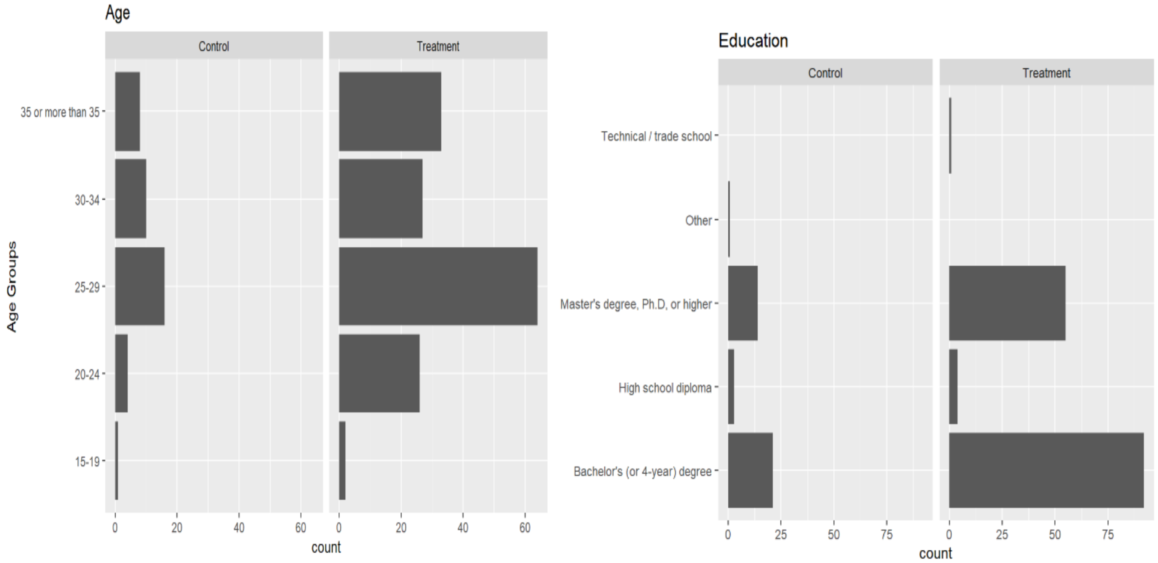


Figure (4)

Comparing the Control and Treatment group willingness to pay

We wanted to explore whether the average willingness to pay for privacy features is different between the overall treatment group and the control group. To do this, we extracted the dollar amounts respondents specified in their selection in the survey and created a column corresponding to each observation. The figure-5 shows that the average willingness to pay for all treatment groups was slightly higher than the control group. However, this difference is not statistically significant as evident by the overlapping confidence intervals between the two bars.

Next, we looked at the average willingness to pay between the control and the three treatment groups. It is evident from Figure 6 that the average willingness to pay is very similar between the control group and treatment groups 1 and 2. However, treatment group 3 that received in-depth information about the use and collection limitations have a slightly higher willingness to pay, although this difference is not statistically significant as evident by the overlap of confidence intervals between the four groups.

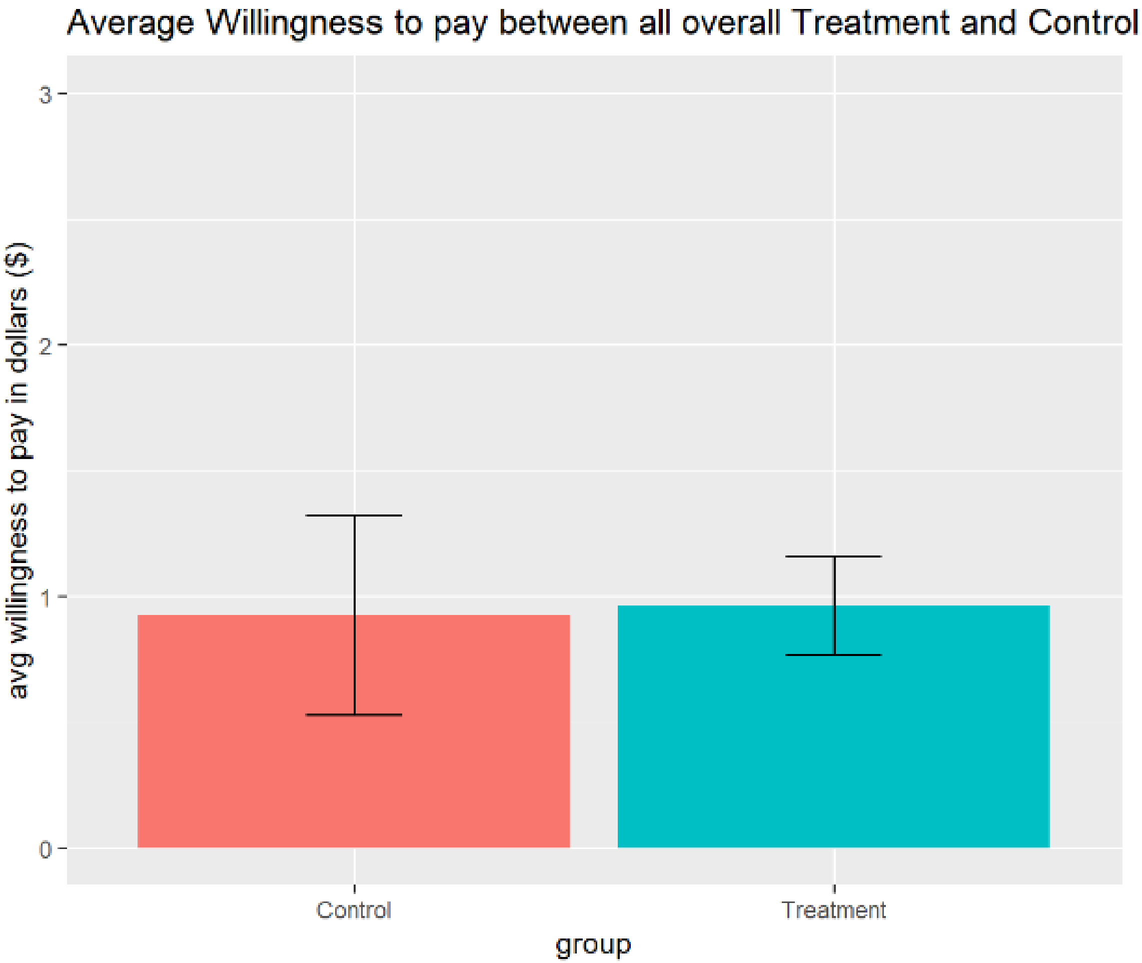


Figure (5)

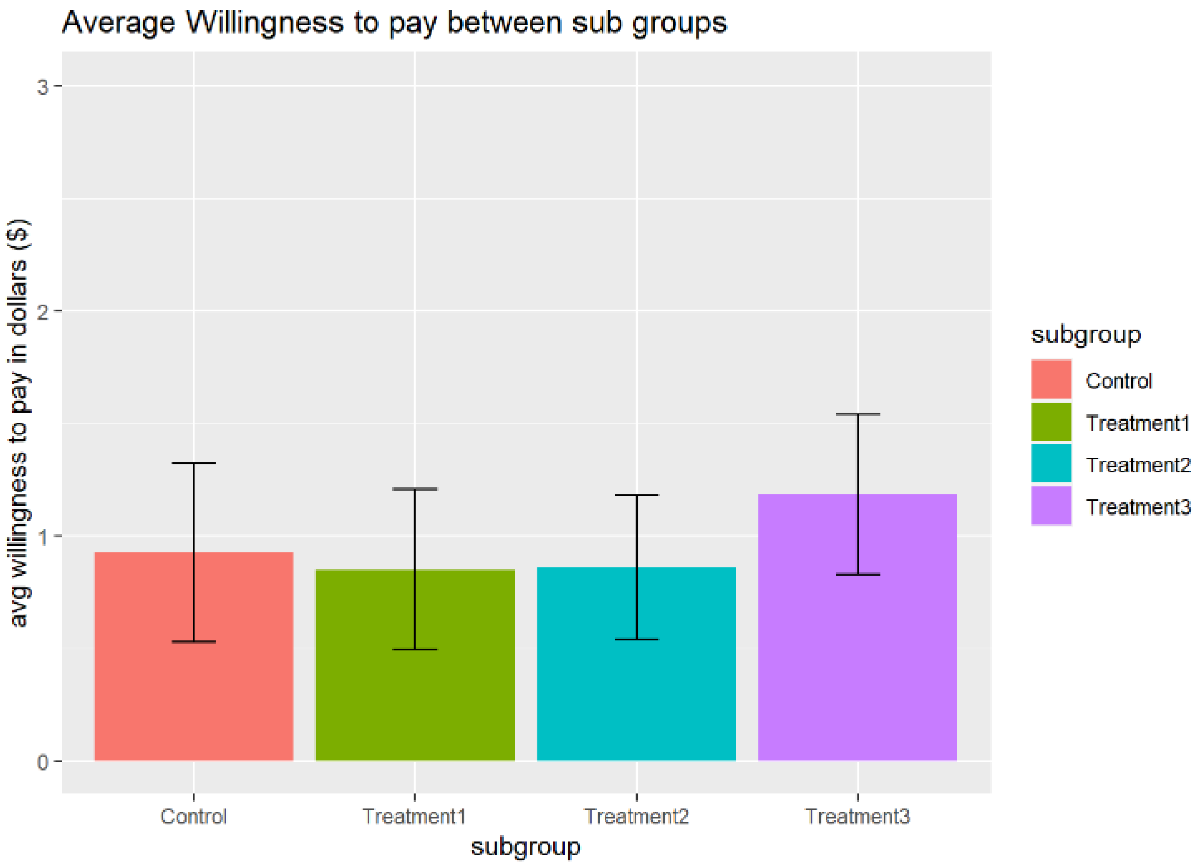
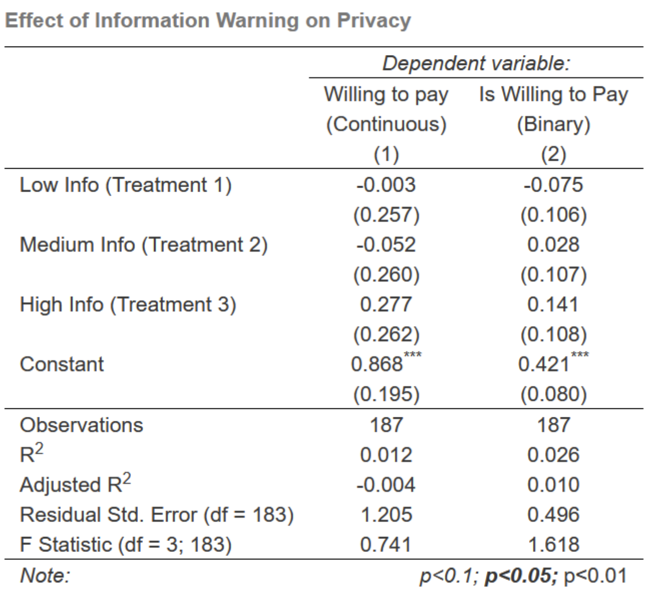


Figure - (6)

5. Results of Analysis

From our analysis we found no statistically significant difference between the control and treatment groups, suggesting there is no effect of informing people about lack of privacy in apps on them choosing to pay for premium privacy services. This is true for both the binary and continuous version of the dependent variable. The coefficients of those willing to pay a premium at all for privacy is not statistically significant regardless of the treatment. Although noticeably the treatment group with the largest coefficient is the one with the most information. Suggesting those in treatment group 3 are the most likely to pay a privacy premium. The same is true for the continuous dependent variable. The people willing to pay the most for

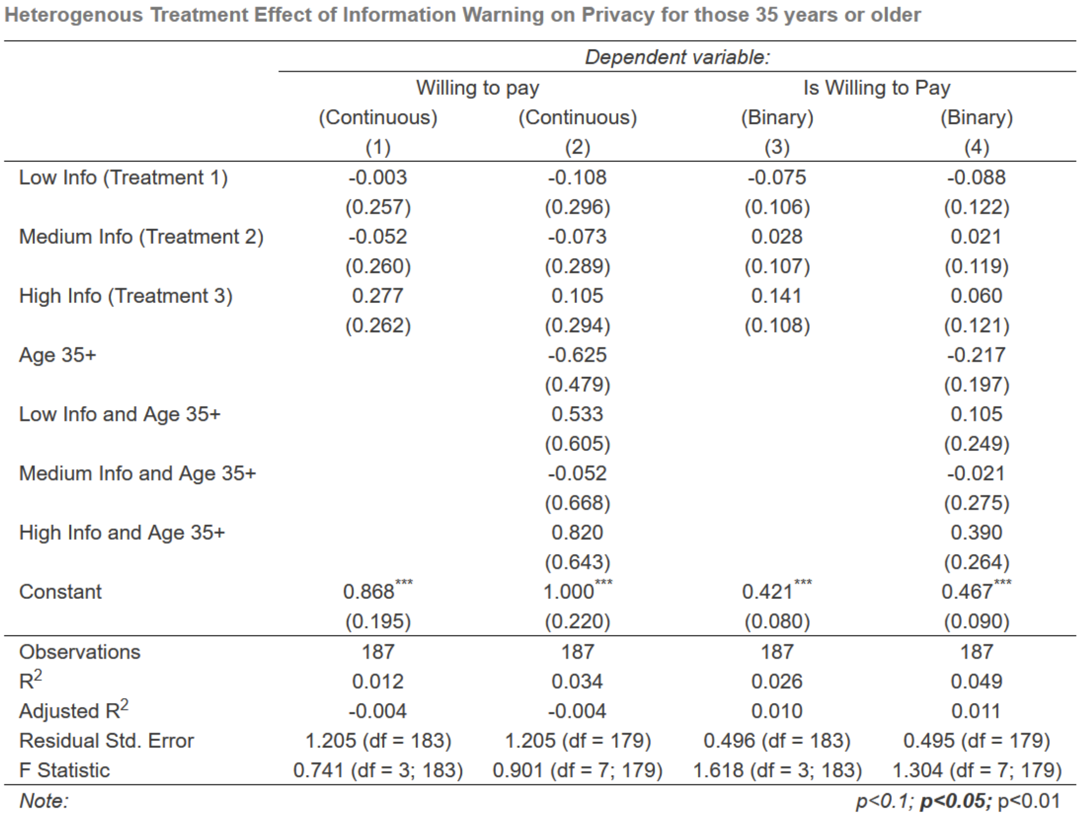


Effect of Information Warning on Privacy

	Dependent variable:	
	Willing to pay (Continuous)	Is Willing to Pay (Binary)
	(1)	(2)
Low Info (Treatment 1)	-0.003	-0.075
	(0.257)	(0.106)
Medium Info (Treatment 2)	-0.052	0.028
	(0.260)	(0.107)
High Info (Treatment 3)	0.277	0.141
	(0.262)	(0.108)
Constant	0.868***	0.421***
	(0.195)	(0.080)
Observations	187	187
R^2	0.012	0.026
Adjusted R^2	-0.004	0.010
Residual Std. Error (df = 183)	1.205	0.496
F Statistic (df = 3; 183)	0.741	1.618
Note:		*p<0.1;* ***p<0.05;*** p<0.01

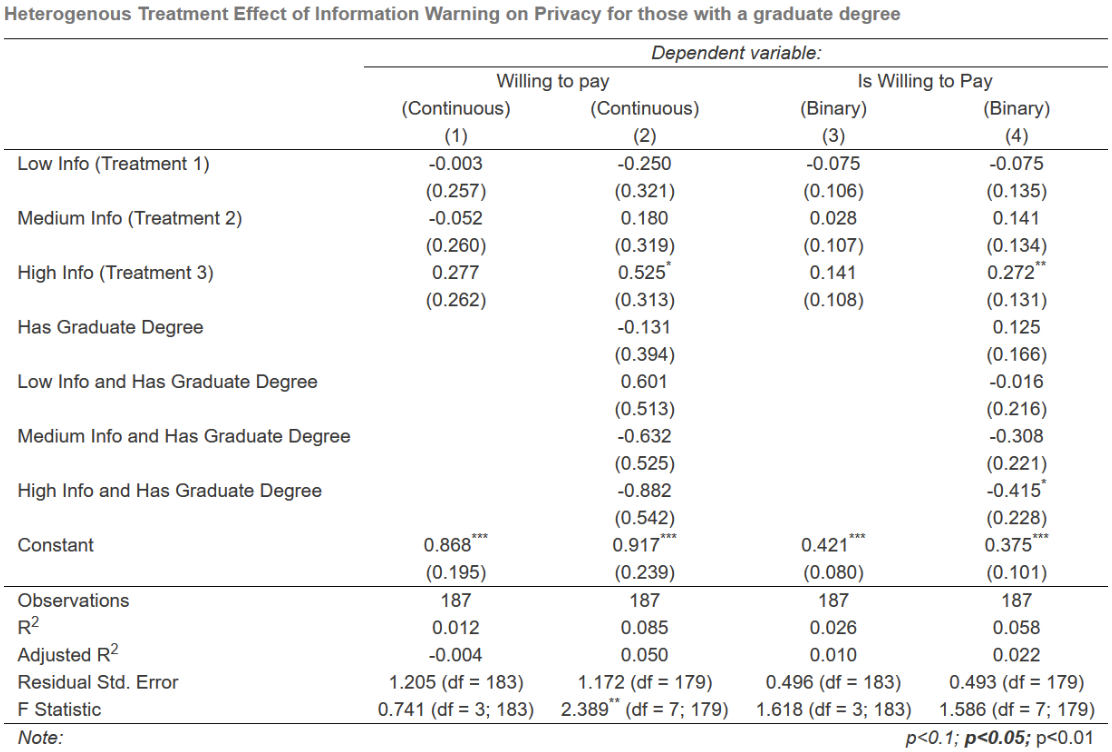
privacy are those who were given the most information about how to maintain their privacy on this app. On average, people in treatment group 3 were willing to pay $0.28 more for privacy than those in the control group who were willing to pay $0.87 (on average). Although our sample size was smaller than we had hoped we also looked at heterogeneous effects for both age and education.

We found no significant effects in either. Below are the regression outputs for both. 35 years old is the cutoff because that is the age where generation X begins and millennials end. We wanted to see if there was a difference in treatment effects based on generation. Older people are generally less familiar with technology and the internet so it would follow that those older are perhaps more concerned about privacy than those who are younger and willing to pay a premium for it. We did not find this in our results. Similarly we thought those with more education may also be more privacy conscious but once again found no evidence of heterogeneous treatment effects. Below are the regression tables.



Heterogenous Treatment Effect of Information Warning on Privacy for those 35 years or older

	Dependent variable:			
	Willing to pay		Is Willing to Pay	
	(Continuous)	(Continuous)	(Binary)	(Binary)
	(1)	(2)	(3)	(4)
Low Info (Treatment 1)	-0.003	-0.108	-0.075	-0.088
	(0.257)	(0.296)	(0.106)	(0.122)
Medium Info (Treatment 2)	-0.052	-0.073	0.028	0.021
	(0.260)	(0.289)	(0.107)	(0.119)
High Info (Treatment 3)	0.277	0.105	0.141	0.060
	(0.262)	(0.294)	(0.108)	(0.121)
Age 35+		-0.625		-0.217
		(0.479)		(0.197)
Low Info and Age 35+		0.533		0.105
		(0.605)		(0.249)
Medium Info and Age 35+		-0.052		-0.021
		(0.668)		(0.275)
High Info and Age 35+		0.820		0.390
		(0.643)		(0.264)
Constant	0.868***	1.000***	0.421***	0.467***
	(0.195)	(0.220)	(0.080)	(0.090)
Observations	187	187	187	187
R^2	0.012	0.034	0.026	0.049
Adjusted R^2	-0.004	-0.004	0.010	0.011
Residual Std. Error	1.205 (df = 183)	1.205 (df = 179)	0.496 (df = 183)	0.495 (df = 179)
F Statistic	0.741 (df = 3; 183)	0.901 (df = 7; 179)	1.618 (df = 3; 183)	1.304 (df = 7; 179)
Note:				*p<0.1;* ***p<0.05;*** p<0.01



Heterogenous Treatment Effect of Information Warning on Privacy for those with a graduate degree

	Dependent variable:			
	Willing to pay		Is Willing to Pay	
	(Continuous)	(Continuous)	(Binary)	(Binary)
	(1)	(2)	(3)	(4)
Low Info (Treatment 1)	-0.003	-0.250	-0.075	-0.075
	(0.257)	(0.321)	(0.106)	(0.135)
Medium Info (Treatment 2)	-0.052	0.180	0.028	0.141
	(0.260)	(0.319)	(0.107)	(0.134)
High Info (Treatment 3)	0.277	0.525*	0.141	0.272**
	(0.262)	(0.313)	(0.108)	(0.131)
Has Graduate Degree		-0.131		0.125
		(0.394)		(0.166)
Low Info and Has Graduate Degree		0.601		-0.016
		(0.513)		(0.216)
Medium Info and Has Graduate Degree		-0.632		-0.308
		(0.525)		(0.221)
High Info and Has Graduate Degree		-0.882		-0.415*
		(0.542)		(0.228)
Constant	0.868***	0.917***	0.421***	0.375***
	(0.195)	(0.239)	(0.080)	(0.101)
Observations	187	187	187	187
R^2	0.012	0.085	0.026	0.058
Adjusted R^2	-0.004	0.050	0.010	0.022
Residual Std. Error	1.205 (df = 183)	1.172 (df = 179)	0.496 (df = 183)	0.493 (df = 179)
F Statistic	0.741 (df = 3; 183)	2.389** (df = 7; 179)	1.618 (df = 3; 183)	1.586 (df = 7; 179)
Note:				*p<0.1;* ***p<0.05;*** p<0.01

6. Limitations and Future Work

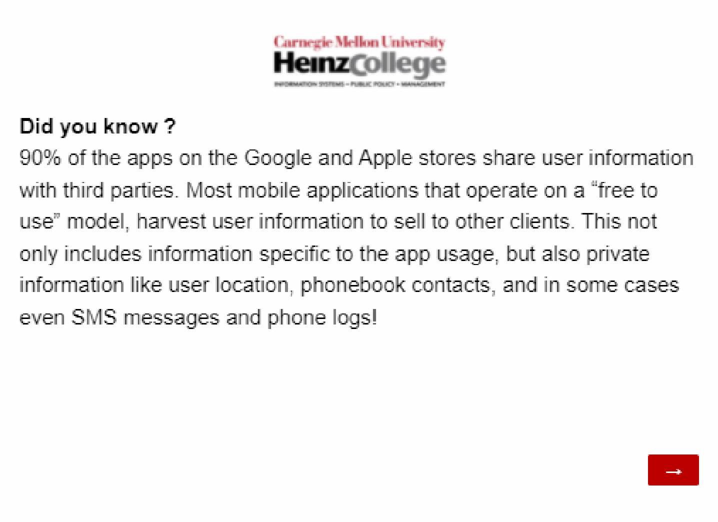
- **Loss of Features Assumption**
  There exists an assumption that data privacy in mobile apps have a tradeoff with functionality. While we have ensured that there is no difference in the functionality promised between free and paid tiers, other than privacy related features, users may assume that better privacy comes with reduced functionality. This assumption, if widely present among a large number of the respondents, then the results of the study may be biased
- **Experimental Design Limitations**
  We just used our connection heavily related to CMU students to collect data, so demographic characteristics such as educational attainment were biased.
  This experiment is convenient sampling, so we cannot generalize the result of our analysis, which means our result has low external validity. To keep the external validity, we have to clearly define the target population we are interested in and randomly choose the samples.
  We used several Whatsapp groups in which many people are duplicated, so there might be responses from the same person. This would ruin the survey result.

Future Work : This study was conducted as a pilot, with limited scope and resources. We recommend expanding the scope of the study to include a wider audience with greater demographic spread. The survey design and the information presented in the treatment groups can also be updated with inputs from experts in the privacy field. In addition to the information gap theory, this experimental design can also be leveraged to test other hypotheses that might potentially explain the privacy paradox in online consumer behaviors.

Appendix

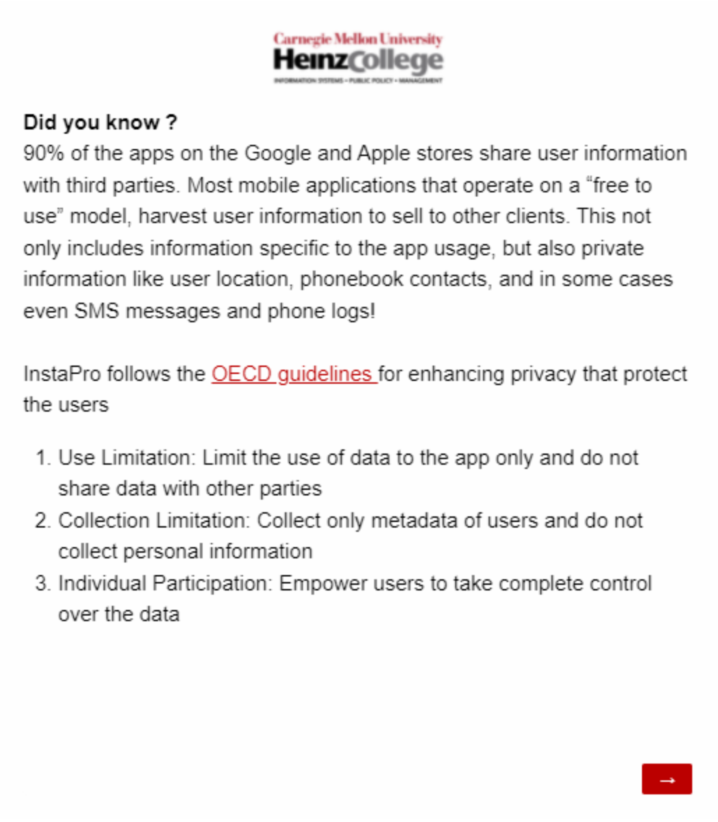
1. Privacy instructions as interventions

Treatment group 1


Carnegie Mellon University
Heinz College
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Did you know ?
90% of the apps on the Google and Apple stores share user information with third parties. Most mobile applications that operate on a "free to use" model, harvest user information to sell to other clients. This not only includes information specific to the app usage, but also private information like user location, phonebook contacts, and in some cases even SMS messages and phone logs!

Treatment group 2

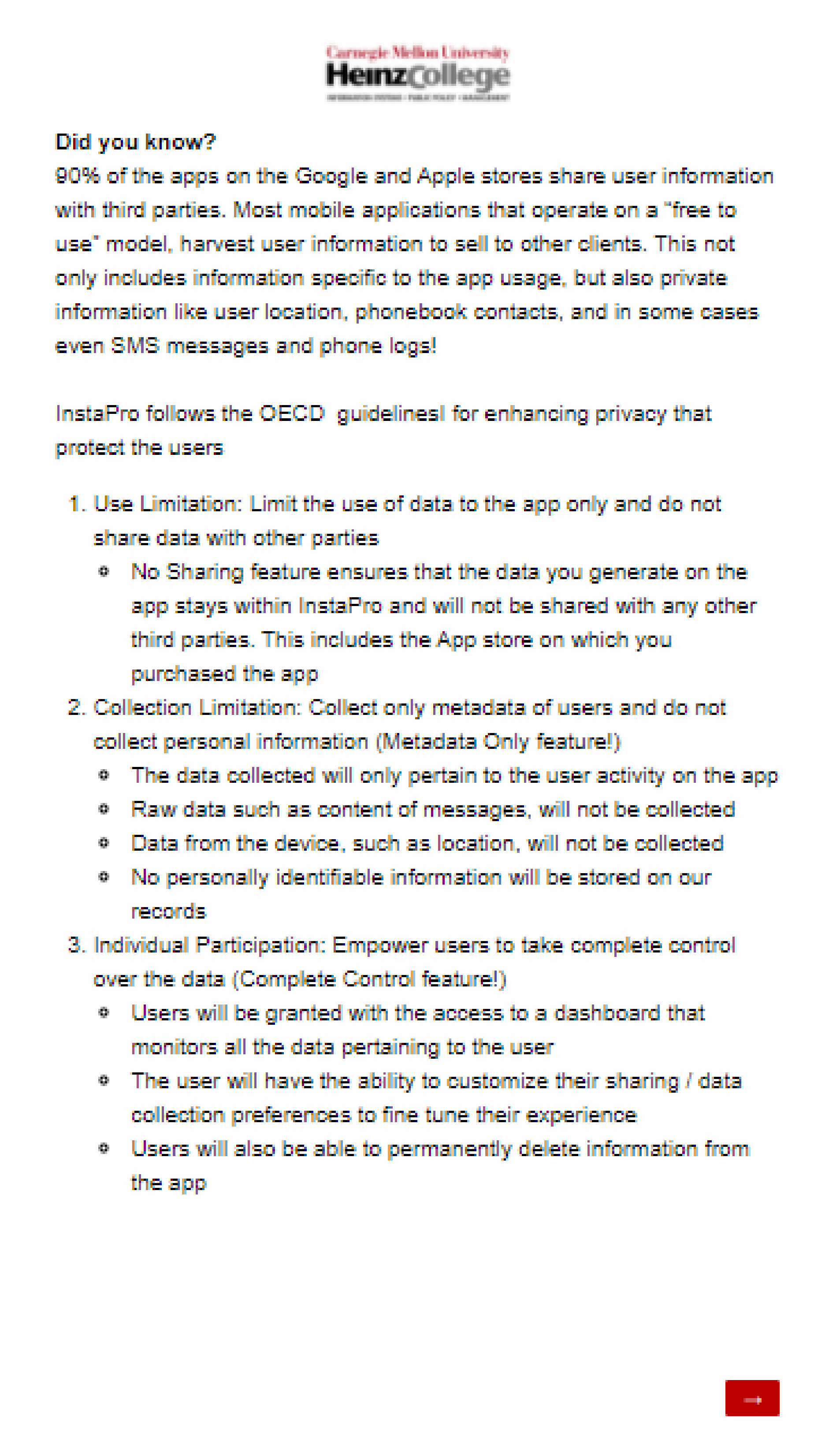

Carnegie Mellon University
Heinz College
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Did you know ?
90% of the apps on the Google and Apple stores share user information with third parties. Most mobile applications that operate on a "free to use" model, harvest user information to sell to other clients. This not only includes information specific to the app usage, but also private information like user location, phonebook contacts, and in some cases even SMS messages and phone logs!

InstaPro follows the OECD guidelines for enhancing privacy that protect the users

1. Use Limitation: Limit the use of data to the app only and do not share data with other parties
2. Collection Limitation: Collect only metadata of users and do not collect personal information
3. Individual Participation: Empower users to take complete control over the data

Treatment group 3



Carnegie Mellon University
Heinz College

Did you know?
90% of the apps on the Google and Apple stores share user information with third parties. Most mobile applications that operate on a "free to use" model, harvest user information to sell to other clients. This not only includes information specific to the app usage, but also private information like user location, phonebook contacts, and in some cases even SMS messages and phone logs!

InstaPro follows the OECD guidelinesl for enhancing privacy that protect the users

1. Use Limitation: Limit the use of data to the app only and do not share data with other parties
   - No Sharing feature ensures that the data you generate on the app stays within InstaPro and will not be shared with any other third parties. This includes the App store on which you purchased the app
2. Collection Limitation: Collect only metadata of users and do not collect personal information (Metadata Only feature!)
   - The data collected will only pertain to the user activity on the app
   - Raw data such as content of messages, will not be collected
   - Data from the device, such as location, will not be collected
   - No personally identifiable information will be stored on our records
3. Individual Participation: Empower users to take complete control over the data (Complete Control feature!)
   - Users will be granted with the access to a dashboard that monitors all the data pertaining to the user
   - The user will have the ability to customize their sharing / data collection preferences to fine tune their experience
   - Users will also be able to permanently delete information from the app