

PRIVATE OR PUBLIC PROFILE:
EXPLORING THE LINKS BETWEEN PRIVACY STATUS AND TRUST ON INSTAGRAM

Student Name: Jing Reilly
Student Number: N00173983
Supervisor: Robert Griffin
April 2020
Word Count: 6264

This thesis submitted as a requirement for the degree of MSc in Cyberpsychology,
Dun Laoghaire Institute of Art, Design and Technology, 2020

Declaration

This Thesis is entirely my own work, and has not been previously submitted to this or any other third level institution.

Jing Reilly

Word Count: 6264

Acknowledgements

The completion of this course and research project could not have been possible without the support of my husband and also my son who learned how to pronounce the word Cyberpsychology from the age of four.

Over the past year and a half, I have been fortunate to meet many like-minded professionals and dedicated lecturers who selflessly shared their knowledge and experience. I do hope that many of us will remain in contact and that our paths will cross again in the future.

I would also like to express my appreciation to my supervisor, Mr. Robert Griffin who has always been there for me whenever I faced a challenge. His sincerity and professionalism have inspired me to bring this project to completion.

And last but not least, my friends who have been listening to me forever about this course and the Thesis. I really look forward to seeing them soon. None of us ever imagined that we would be finishing our Thesis in a middle of a global pandemic caused by Covid-19. While most people are in lockdown and social distancing themselves, I found this situation brought its own additional challenges. Thanks to the advanced technologies and online platforms, we can still do what we love and connect with the ones we love.

This course has definitely changed the way I see technology and behaviour online. The next important thing is to continue this journey and use Cyberpsychology to help more people to make better decisions every day.

Table of Contents

DECLARATION	II
ACKNOWLEDGEMENTS.....	III
ABSTRACT.....	1
LIST OF ABBREVIATIONS	2
INTRODUCTION.....	3
RATIONALE	3
LITERATURE REVIEW.....	5
THIS STUDY.....	10
METHODOLOGY.....	12
DESIGN.....	12
PILOT STUDY	13
PARTICIPANTS	13
APPARATUS.....	14
MATERIAL	14
ETHICS	14
RESULTS	16
DESCRIPTIVE DATA	16
SPSS REPORTS	18
DISCUSSION	23
OVERVIEW OF FINDINGS	23
IMPLICATIONS.....	23
LIMITATIONS.....	25
EVALUATION	26
FUTURE RESEARCH	27
CONCLUSION	27
REFERENCES.....	28
APPENDIX A.....	33
APPENDIX B.....	37
APPENDIX C	38
APPENDIX D.....	43
APPENDIX E	44
APPENDIX G.....	49
APPENDIX H.....	51
APPENDIX I	54
APPENDIX J	56
APPENDIX K.....	57
APPENDIX L	60

Abstract

There were an estimated 2.95 billion social media users in 2019 (Clement, 2020) and every user has at least one user profile. User profiles are important as an extended core self into the online world and they also contain personal information. Increasingly, users become more aware of the privacy concerns associated with their profiles and social media platforms also enable users to control the access of their information by allowing them to change the privacy status.

The outcome of having a public or private profile isn't just about the potential risks or positive impact, it is linked with the user's trust. This research, which looked at a total of 58 participants, showed that users on Instagram with private profiles have a higher level of trust than users with public profiles. A possible explanation for this was linked to the CPM theory and findings which identifies that privacy boundaries have a positive effect on trust.

The second part of the study used an online experiment. Two random groups were created with one group exposed to six mocked-up public profiles and the other group exposed to six mocked-up private profiles. Although results failed to show any significant difference between trust and the profile privacy intervention, the results indicated that users with PTP had an increase in trust post intervention, regardless of what profiles they were exposed to.

This research showed that profile privacy status is an important topic which closely links to the evolving issues on privacy concerns and a user's trust. Future research is required to explore other potential impacts and influencing factors to help to deepen our understanding of how to help users and businesses to make the right decisions about their profile.

List of Abbreviations

Social Media Site	SNS
Public Profile	PCP
Public Profile Owner	PCPO
Private Profile	PTP
Private Profile Owner	PTPO
Trust Score before Intervention	Trust 1 or T1
Trust Score after Intervention	Trust 2 or T2
Change in Trust Score (T2-T1)	Trust 3 or T3
Public Profiles Intervention Group	Group 1
Private Profile Intervention Group	Group 2

Introduction

Rationale

It's unquestionable that Social Media plays an important role in modern society. For many people, using social media is a daily activity. It offers a way of sharing and obtaining information; it is a source of entertainment and a communication channel to people both personally and professionally. There were an estimated 2.95 billion social media users in 2019 (Clement, 2020) and this number is projected to increase to 3.43 billion by 2023. Every social media user is required to have a user profile that can describe a lot of information about the user. Information such as their characteristic, identity, interests, professional affiliations, status, recent activities, pictures and geographic locations. Sharing or not sharing this information can potentially lead to good and bad outcomes. For example, having a public profile means that more people will be able to see your profile and your posts. On one hand, it means that your posts can potentially reach wider audiences and make a bigger impact; but on the other hand, it makes it easier for people to access your information without you knowing.

Users are becoming increasingly aware of the issues associated with privacy. A European wide survey showed that 72% of people are either fairly or very concerned about their privacy. (Eurobarometer, 2010). To address privacy related concerns, policy makers rolled out a European wide General Data Protection Regulation (GDPR) in May 2018. GDPR is a new regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Social Media Sites (SNSs) have also been enhancing their platform privacy features to allow users to better control the visibility and accessibility of their own data. (The Verge, 2019). Funding has been made available to improve privacy and cybersecurity. In 2019, a total of €233.36 million was made available by the EU for security and privacy related research projects (Europa, 2019a).

While privacy concern is growing, users' behaviours are changing too. In 2015, a research showed that 57% of people had tried to change their privacy settings (European Commissions, 2015, p. 91). Privacy settings is a feature on SNS that allows you to control who sees information about you (Cambridge Dictionary, 2019). Changing profile privacy settings is a common step that an individual user takes to control their visibility. However, the switch from one status to another has somehow created other phenomenon on SNS. For example, the memes (See Appendix A for examples) are created by users to demonstrate certain attitude change towards people who have a private profile or changed to private profile. Memes, defined as cultural units that spread from person to person (Shifman, 2013), can be an idea, behaviour, style, or usage that spreads from person to person within a culture. Another example of behaviour shift is users changing their profile to private in order to gain more followers. Some account owners have been seen switching from public to private account so the content they post can't not be viewed unless you follow them (See Figure A7). This has become a strategy to increase audiences. (Alvarez, 2020)

Privacy is particularly important to self-disclosure and trust. They all share complexity by nature. McKenna, Joinson, Reips & Postmes (2007) explained that privacy is a prerequisite for disclosure, and yet, the process of disclosure serves to reduce privacy. The main motivation for creating a profile on SNS is the possibility to easily share information with selected contacts or the public, either for professional or personal purposes. However, where disclosure fulfils the fundamental needs for social connectedness and belonging and is intrinsically rewarding (Tamir & Mitchell, 2012), it also carries risks, security concerns and potentially losing information because users' gave up some level of privacy and personal control by sharing information with people. Privacy and trust are closely linked according to previous research (Tang & Liu 2015). Trust in social media is a popular topic for researchers and its practical significance can help users collect relevant and reliable information on SNS. Trust is a critical issue in both online and offline disclosures of personal information. On one hand, we use self-presentation on SNS to establish trust; on the other hand, SNS have been blamed for contributing to the lack of trust. (Irish Times, 2019).

An idea emerged for this study to explore the links between profile privacy status and trust to help to understand this complex relationship. In particular, two questions arose: Does profile status indicate a profile owner's level of trust? In other words, do users with public profiles (PCP) have more or less trust than users with private profiles (PTP)? When users are continuously exposed to either PCP or PTP, does it affect a user's trust? "According to Tsay-Vogel, Shanahan and Signorielli (2018), "The persistent exposures to self-disclosure behaviours may in turn cultivate one's world view." These are the questions being addressed by this research.

Instagram was selected to be the SNS for this study because it has a large number of users and also two distinct profile privacy settings: Public and Private.

Literature Review

- CPM Theory

Communication Privacy Management (CPM) theory describes when and how people decide to share information about themselves and has provided a good theoretical base for this study. (Hahn, 2018). CPM theory has long existed but its popularity is growing among researchers in the context of social media studies. From the perspective of CPM theory, to protect one's privacy, a person would set privacy boundaries during interaction with people. Privacy boundaries are set based on trust; open when there is trust and closed when there is no trust [Petronio, 2002]. There are two main types of boundaries: personal boundary and collective boundary. "personal boundary" protects the personal information which has not been shared; where "collective boundary" protects personal information has been shared. (Hahn, 2018).

In the context of Instagram, it is believed a user with a private profile (PTP) has both personal and collective boundaries. For a user with PTP, most of their personal information is closed until they approve the follower's request and decide to open the boundary based on who the followers are. This also means that a private profile owner

(PTPO) has a closed network of followers that forms the second privacy boundary- Collective Boundary. In contrary, public profile owners (PCPO) have open boundaries because they have decided to share all of their Instagram information with the public.

Research by Fianu, Ofori, Boateng & Ampong (2019) suggested that on Instagram, the user places some trust in the confidant while disclosing personal information in the hope that there will not be boundary turbulence. Deduced from this, a PTPO has more protection to prevent boundary turbulence than a PCPO,. However, and an area of interest for this study, is the level of trust between the PTPO who has better privacy boundary and the PCPO who place trust to a much wider audience?

- Cultivation Theory

Persistent exposure cultivates one's world view (Tsay-Vogel et al., 2018). They further explained that "the persistent exposures to (self-disclosure) behaviours may in turn cultivate one's world view." This research uses this theory to test if exposure to different profile privacy status can affect a user's trust. For example if a user is browsing other profiles, every profile they see is either PCP or PTP. Will that experience change their trust, in particularly general trust? Tsay-Vogel et al. (2018) also explained that "Attitude towards privacy is related to self-disclosure. Platforms may be cultivating certain behaviour on platforms through the functionalities, design of interfaces and even policy control over content published."

This theory is particularly interesting as it adds a bilateral element to this study. Behaviour such as changing profile privacy status may affect profile owners themselves as well as other users. Using the memes example mentioned earlier, its growing popularity and virality can be a potential form of media to assist the cultivation. Appendix A shows the evidence that profile privacy has become a topic in the meme community.

- Privacy and Privacy Concern

Privacy can be defined as taking control over information about ourselves. (Fried, 1968). Privacy-seeking behaviour refers to the things people do to protect their information (Zlatolas, Welzer, Heričko & Hölbl, 2015). Privacy concern on social media has unresolved complexity. Due to this, privacy concerns continue to grow as personal data is required for more and more online services. As mentioned earlier, one of the common features for users to control their privacy is using privacy settings. Changing profile privacy settings is a common step that an individual user uses to control their visibility. However, SNS users trade their privacy for benefits on SNS such as social rewards, popularity, and enjoyment as they disclose personal information.

Although the concept of privacy has evolved from the right to be left alone to the right to control personal information, there has been an increase in publicly displaying one's personal information and network on SNS. (Chen and Chen, 2015). This has further demonstrated that privacy and self-disclosure have a somewhat paradoxical relationship (McKenna et al., 2007). Digital literacy has been found to have an impact on privacy-related online behaviours. Park (2011) concluded to three dimensions (a) familiarity with technical aspects of the Internet, (b) awareness of common institutional practices, and (c) understanding of current privacy policy.

Privacy involves controlling and regulating access to personal information before revealing to a group of audiences. It requires trust that the audience group will follow certain expectations. Some previous research has modelled privacy concern as an independent variable and self-disclosure as an outcome. Such research showed that high levels of privacy concerns are associated with lower self-disclosure outcomes. (Saffarizadeh, Boodraj, & Alashoor, 2017). Although this is all very useful information that shows the influencing factors of why users may choose PCP or PTP, however, profile status has not been linked to the profile owner's general trust or how it may cultivate other user's trust. This study will hope to add to the existing literature on privacy and trust by consolidating what we know on Privacy, Privacy concern, Self-disclosure and Trust.

- Trust and Self-disclosure

Trust can be defined as ‘ a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intention or behaviour of another’ (Rousseau, Sitkin, Burt and Camerer, 1998). However the definition of trust is still loose and very much dependant on the context. The role of trust in the online world is extremely important, especially the study of the moderating role of trust. (Bargh & McKenna, 2004). Researchers who have studied the moderating role of trust suggested that in a context where there is a lack of information online, users’ motivation to trust or not to trust is an important moderator of how they respond. (Wieselquist, Rustult, Foster & Agnew, 1999).

Trust is a critical issue in both online and offline disclosures of personal information. A lot of things we do online both requires trust and forms trust. Whether it is giving your personal details when signing up for something; or sharing your photo or story with people online who have never met; or creating a social profile to represent who or promote who you are which may include your personal information such as name, job, photos, location or even about your family. For social media, Trust is crucial in terms of helping users to collect relevant and reliable information. It is very important that we continue studying trust and how it evolves along with the development of SNS.

Self-disclosure is a process of interaction by which a person discloses information about himself or herself to another person. Self-disclosure is a predominant part of social networking because SNS users share a lot of personal information on SNS, (Fianu et al., 2019). Hsiao (2007) found that self-efficacy and personal outcome expectations exert a significant impact on the intention to share information online. This explains that users’ behaviour will differ based on their self-efficacy and their expectations from creating a social profile. It is also important to note that social profile is a part of the persona which a user created for the online world. According to Belk (2014), this persona is called the Digital Self which is an extended version of our core self. If this is

the case, then our online profile not only reflects who we are, it also forms the sense of self and it will also impact users' behaviour both online and offline.

Studies have also linked self-disclosure with trust. Foubert and Sholley (1996) compared trust with self-disclosure in their study, which found Women with low trust had significantly more self-disclosure than men with low trust. Also, women with high trust had significantly more self-disclosure than men with high trust. Some research focused on refining and defining the trust like Fianu et al. (2019) and they argued that "trust in SNS members and trust in the SNS service provider were found to have a significant effect on SNS self-disclosure. Privacy awareness, privacy concerns, privacy invasion experience, and privacy-seeking behaviour were found to have a significant effect on trust in the SNS service provider." Although existing research is useful, however unlike them, this research selects a particular responsive behaviour of users to their privacy concern and link it with trust.

- Instagram

For this research, Instagram is the most appropriate and ideal platform. Instagram is known to be used for self-presentation, especially "more polished self-presentation via the creation of stylized and carefully shaped visual portraits", (Boczkowski, Matassi & Mitchelstein, 2018)

On the Instagram platform, there are two very distinctly defined profiles; public profile (PCP) and private profile (PTP), see Appendix B for examples. They have a significant difference in visibility and other platforms such as LinkedIn and Twitter are less suitable for this reason.

When a user comes across new content outside their network, if the content was posted by a user with PCP (see Figure B1), it is visible to everyone; if the content is posted by user with PTP, the content is restricted to their followers network only. Others will need to request to follow the PTP owner in order to access the content of

interest, however, everyone is able to see the basic profile information which is a small photo and user name to identify who they might be (Figure B2).

Instagram also has a large customer base of one billion users using the platform every month and 500 million users using Instagram stories every day. (Instagram,2019)

This Study

This study brings together the three key concepts discussed above: privacy concern, trust and self-disclosure. In the context of this study, users' profile privacy choice of having a PCP (higher self-disclosure) or PTP (lower self-disclosure) are considered as behavioural reactions to privacy concerns. The aim is to continue to further understand the links between these concepts and as to how they might influence each other. In order to look at these concept more closely, this study is divided into two parts.

Part 1 – It looks at the differences between profile privacy status and a user's trust score. Using quantitative research and data collected from an online survey to explore the potential links privacy status and trust scores. In this part, the user's profile privacy status (public or private) are independent variables, and the dependant variable is the user's trust score.

Part 2 – It focuses on the effect that profile privacy intervention may have on trust. It involves exposing participants to different profiles (public or private) and then measuring their trust scores post intervention. Group 1 will be exposed to a series of PCPs and Group 2 will be exposed to a series of PTPs. Exposures to different profiles (PCP or PTP) are independent variables and the change of trust score is the dependant variable.

- Research Title

Private or public profile: exploring the links between a user's privacy status and trust on Instagram

- Research Questions and Hypothesis

There are 3 research questions and 3 hypotheses identified for this research.

RQ1: *Is there a significant difference between the trust scores of PCPO and PTPO?*

H1: *There will be a significant difference between the trust scores of PCPO and PTPO.*

RQ2: *Will privacy status intervention affect a participant's trust?*

H2a: *There will be a significant difference between change in trust scores and different intervention groups.*

H2b: *Exposure to PCP (Group 1) will increase trust and exposure to PTP (Group 2) will decrease trust.*

RQ3: *Is there a significant difference between a participant's profile privacy status (Public or private) and changes in their trust scores after the privacy status intervention?*

H3: *There will be a significant difference between profile privacy status and changes in their trust scores after the privacy status intervention.*

A user's decision of having a PCP or PTP involves how much personal information the user is willing to disclose to everyone. This disclosure carries certain risks and trust is likely to play a key role. The results of this study will hopefully add new dimensions on whether profile privacy (a privacy concern related behaviour) can indicate a users' level of trust and even potentially shape the relationship between privacy concern, self-disclosure and trust.

Methodology

Design

To test the hypotheses listed above, this study is a quantitative, quasi-experimental study with a correlational repeated measure. Online experiments were used as a part of the study. The reason for choosing online experiments is to keep this study as close to the natural online environment where the behaviour occurs. In terms of the survey, two survey links were created. Survey 1 and Survey 2 both have exactly the same procedure and same questions except the online experiments were different. (See Appendix C for copy of survey questions, procedures and briefing content.)

In survey 1, participants were exposed to six mocked-up public profiles. In survey 2, participants were exposed to six mocked-up private profiles. The participants who received survey 1 forms Group 1 and participants received survey 2 forms Group 2. (See Appendix D for design diagram)

All participants completed a survey with demographic questions and Instagram related questions including their profile privacy status and General Trust Scale by Yamagishi & Yamagishi (1994) on a 5-point scale. (See Appendix E for more information on the trust scale)

IV 1 = User's profile privacy status (PCP or PTP)

DV 1 = trust

K = 2

Section 2 (online experiment)

Each participant was subsequently asked to complete an online experiment. Two surveys were randomly distributed so the participants with one link to survey 1 were exposed to 6 mocked-up PCPs (See Appendix F); the other participants who received another link to survey 2 were exposed to 6 mocked-up PTPs (See Appendix F). After the exposure, they were asked to repeat the trust questionnaire again. This

experiment tested whether or not there is a change in a user's trust score before and after the intervention. For this part, the user's own profile status (PCP or PTP) and their exposure to mocked-up PCPs and PTPs are independent variables, the changes in their trust level is dependant variable.

IV 2 = user's profile privacy (PCP or PTP)

IV 2 = exposure to PCP or exposure to PTP

DV 2 = changes in trust

K=4

Pilot study

A pilot study was conducted, useful feedback was provided and changes were implemented.

- Language and grammatical errors were corrected.
- Settings errors such as whether to allow multiple answers.
- Clearer explanation for the experiment section was required and amended.
- Participants expressed the experiment section was a little confusing as they did not know what they should be looking at. Some changes were made to clarify the instruction.
- Some positive feedback was also provided in that the layout of the survey was very clear and easy to follow.

Participants

A snowball sampling method was used to recruit participants. Social media posts, private messages, group emails, word of mouth and face to face promotions were all used as methods. Links were shared randomly in the recruitment process and participants were advised to only fill out one survey.

SNS used in recruitment included LinkedIn, Facebook and Twitter. Instagram was not used as the link is not clickable in the post. Additionally, due to the type of audiences, it was considered to be less effective to carry out this research.

There were a total of 58 respondents, 26 in Group 1 and 32 in group 2. One of the respondents in group two failed to complete the General Trust Scale but did complete the Privacy Status Intervention hence the difference in numbers in the respective sections of the research.

Apparatus

Survey Monkey was the chosen survey platform for conducting, distributing, collecting and analysing the survey results. SPSS was used for quantitative statistical analysis.

All participants needed a computer (either PC or laptop) or a smart phone to complete the survey.

Material

The Trust Scale used in this study is a 6-item questionnaire that uses general statements to measure participants' beliefs about honesty and trustworthiness of others, in general. (Yamagishi & Yamagishi, 1994). (See Appendix E)

The score for each item is averaged together to form a continuous measure of generalized trust.

Ethics

Ethics in research provides rules that specify appropriate and inappropriate behaviour in the conduct of research and application of findings. Although no major complications of this research were found, a few steps were taken to ensure that this research followed all the ethical requirements.

All participants in this research were over 18 years of age. Because Instagram's age limit is 13, an age related question was included in the survey to ensure the participants had met the age requirement.

To ensure the right courtesy was given to different parties involved, some permissions were obtained and information was provided including:

- Ethical A form was submitted and approved by the Department of Technology and Psychology Ethics Committee and any personal identifier such as email was clearly stated as optional. (See Appendix G for a copy of the form submitted)
- A consent form was obtained from all participants. (See Appendix C)
- Participants were made aware of their right to withdraw at any time. (See Appendix C)
- An explanation page to the participants about the research and what was asked of them. (See Appendix C)
- Researcher and supervisor's contact details were provided for further contact.
- Procedure. (See Appendix C)

Results

Descriptive Data

(See Appendix H for additional data and tables)

- Demographic

Of the 58 participants who completed the experiment, female participants accounted for 60.3%, with male participants accounting for 37.9% and the remaining 1.7% of participants preferred not to answer.

The most prominent age group of the participants was aged 35-44 which accounted for 27%, and followed by 14% of aged 45-54.

In terms of their usage behaviour, over 99% of the participants are active users who uses at least monthly and less than 1% do not use Instagram at all.

- Profile Status and Groups

A total of 57 valid responses were collected on profile status, including 19 PCPs (33.3%) and 38 PTPs (66.7%).

There were 26 participants in Group 1 (PCP intervention) and 31 participants in Group 2 (PTP intervention). With regard to the profile owner's status in each group, 10 PCPs and 16 PTPs in Group 1 and 9 PCPs and 22 PTPs in Group 2.

- Instagram Usage

The purpose of using Instagram was included in the survey to help understand the motivation behind the users and to explore potential relationships with trust scores. The descriptive status showed that 50% of participants use it for social interaction and an interesting 17.2% for peeking.

- Validity and Reliability

For this research, the general trust scale was assessed and Cronbach's alpha were used to test the reliability of the constructs. The Cronbach's Alpha was .787, and because it was greater than .7, it is regarded as acceptable for its internal consistency.

Descriptive data was collected and compared to the bell curve. Figures I1, I2 and I3 are shown below, all 3 trust scores were close to being normally distributed with positive skewness.

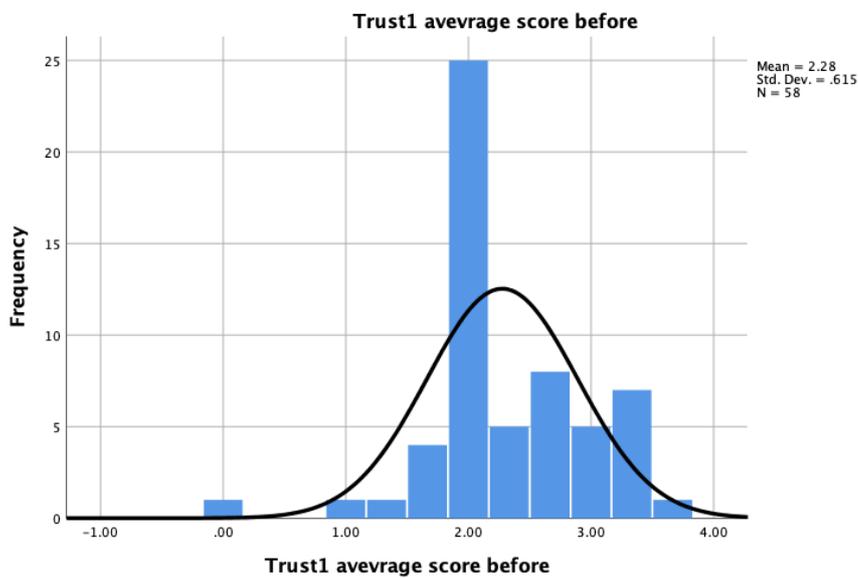


Figure I1: Histogram for Trust before Intervention (T1)

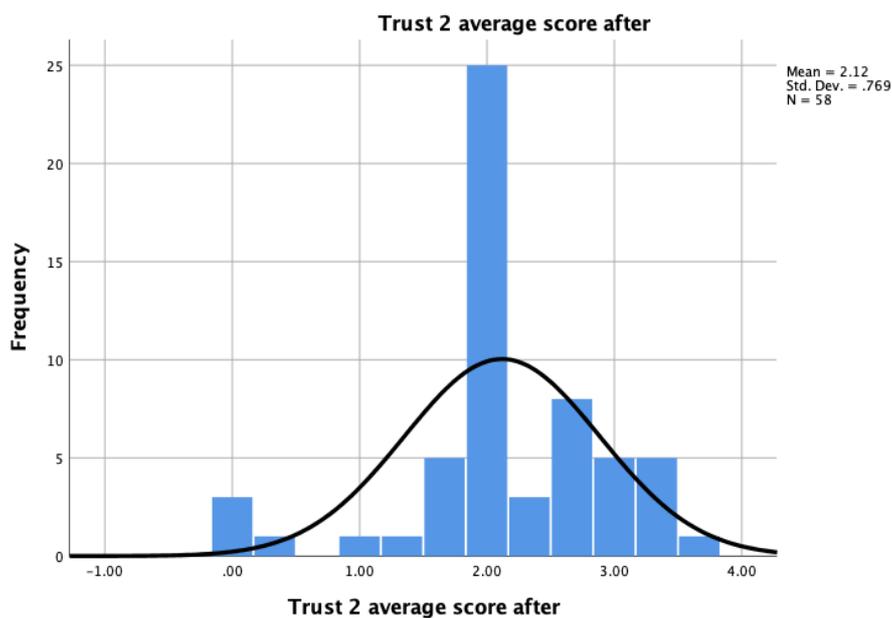


Figure I2: Histogram for Trust after Intervention (T2)

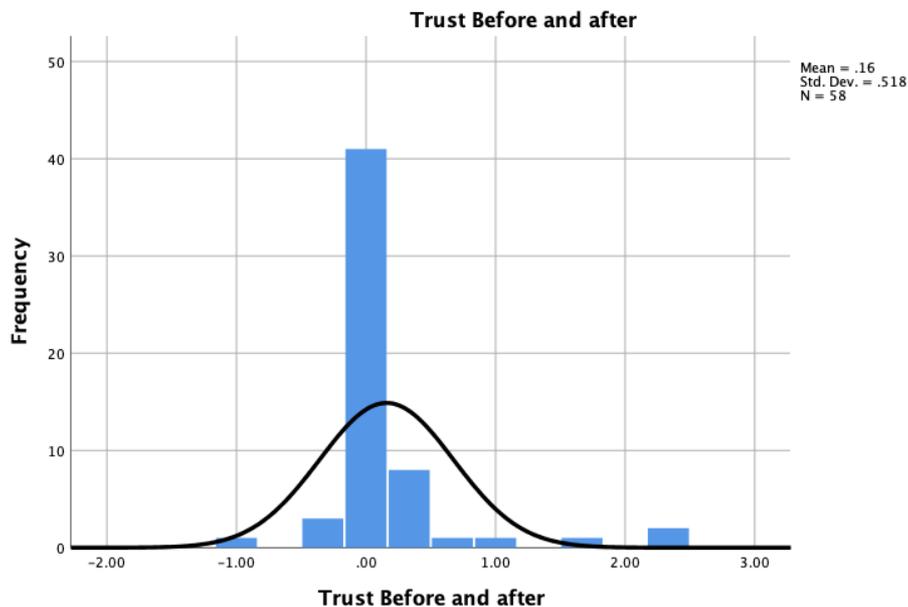


Figure I3: Histogram for change in Trust Score (T3= T2-T1)

SPSS reports

Data analysis was conducted using the Independent Sample t-test and a two-way ANOVA on SPSS. An Independent t-test was used for testing the significant difference between participants' profile status and their trust scores before intervention. The two-way ANOVA was the appropriate analysis for the two independent groups who were exposed to two types of profiles (PCP and PTP) and to compare how their trust score may have changed after exposure.

RQ1: *Is there a significant difference between the trust scores of public profile holders and private profile holders*

H1: *There will be a significant difference between the trust scores of public profile holder and private profile holder.*

A total of 57 valid responses were collected from 58 sampled participants who completed a general trust scale. An independent samples t-test revealed that Public Profile Owners (PCPO) (M=2.000, SD=.63586 and N=19) had a lower general trust score than Private Profile Owners (PTPO) (M=2.386, SD=.55223, N=38). By conventional criteria, this difference is considered to be statistically significant ($t = -2.36$, $P = .022$). (See Appendix J for additional data and tables)

The Null hypothesis was rejected, therefore hypothesis 1 was confirmed. There was a significant difference between the trust scores between PCPO and PCTO.

Table J1

Trust 1 scores by group statistics (Public and private profile groups)

Group Statistics					
	Privacystatus	N	Mean	Std. Deviation	Std. Error Mean
Trust1 avevrage score before	Always Public	19	2.0000	.63586	.14588
	Always private	38	2.3860	.55223	.08958

Table J2

Trust 1 Independent Samples Test

Independent Samples Test								
		Levene's Test for Equality of Variances		t-test for Equality of Means				
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Trust1 avevrage score before	Equal variances assumed	.861	.358	-2.365	55	.022	-.38596	.16323
	Equal variances not assumed			-2.255	31.928	.031	-.38596	.17119

RQ2: *Will privacy status intervention affect a participant's trust?*

H2a: *There will be a significance difference between change in trust scores and different intervention groups.*

H2b: *Exposure to PCP (Group 1) will increase trust and exposure to PTP (Group 2) will decrease trust.*

A total of 58 sampled participants completed the privacy status intervention which required the participants to view 6 mocked-up PCPs or 6 mocked-up PTPs. A two-way ANOVA test was chosen for hypotheses 2 and 3. The results showed no significant difference to the change in trust score between invention Group 1 and Group 2. $F(1,53) = 0.404$, $p = .528$, partial $\eta^2 = .008$. (See Appendix K for additional data and tables)

With a P value of 0.528 which is greater than .05, it was failed to reject the null hypothesis 2a. Therefore it confirms that privacy status intervention did not have any significant effect on change of trust.

Descriptive statistics data also showed that both Group 1 ($M=.1987$) and Group 2 ($M=.1290$) saw an increase in trust score, therefore it was failed to reject the null hypothesis 2b as well. Exposure to PCP and PTP both had a positive impact on the trust score.

Table K2
T3 Descriptive Statistics Dependent Variable

Descriptive Statistics				
Dependent Variable: Trust Before and after				
Group	Privacystatus	Mean	Std. Deviation	N
Public	Always Public	.0000	.17568	10
	Always private	.3229	.69247	16
	Total	.1987	.56964	26
Private	Always Public	-.0741	.36430	9
	Always private	.2121	.51224	22
	Total	.1290	.48631	31
Total	Always Public	-.0351	.27543	19
	Always private	.2588	.58855	38
	Total	.1608	.52229	57

RQ3: *Is there a significant difference between a participant's profile privacy status (PCP or PTP) and changes in their trust scores after the privacy status intervention?*

H3: *There will be a significant different between profile privacy status (PCP or PTP) and changes in their trust scores after the privacy status intervention.*

A total of 57 valid responses were collected from 58 sampled participants who completed general trust scale before and after the privacy status intervention. A two-way ANOVA test revealed that there was a significant privacy status effect on trust scores. $F(1,53) = 0.404$, $p = .041$, partial $\eta^2 = .076$. With a P value of .041 which is less than .05, the null hypothesis 2 was rejected and hypothesis 2 was confirmed. (See Appendix K for additional data and tables)

There was a significant difference between profile privacy status (PCP or PTP) and trust scores after the privacy status intervention.

It was also found that in Group 1 (exposed to PCP), PCPOs did not change their trust score (T3 mean=.0000) post intervention, however, PTPOs saw an increase in trust (T3 mean=.3229); in Group 2 (exposed to PTP), PCPOs saw a decrease in trust scores (T3 mean=-.0741); and PTPOs had a higher trust score (T3 mean=.2121) after intervention. In summary, intervention (regardless of which profiles PCP or PTP were used) it had a positive effective on trust on PTPOs, in other words, PTPOs had T3 after intervention in both groups.

Table K4
Tests of Between-Subjects Effects Dependent Variable: T3

Tests of Between-Subjects Effects						
Dependent Variable: Trust Before and after						
Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	1.234 ^a	3	.411	1.552	.212	.081
Intercept	.666	1	.666	2.514	.119	.045
Group	.107	1	.107	.404	.528	.008
Privacystatus	1.163	1	1.163	4.389	.041	.076
Group * Privacystatus	.004	1	.004	.016	.900	.000
Error	14.042	53	.265			
Total	16.750	57				
Corrected Total	15.276	56				

a. R Squared = .081 (Adjusted R Squared = .029)

- Other Findings (See Appendix L for additional data and tables)

There is a significant positive relationship between privacy status and trust 1 scores, $r(55)=.304$, $p=.022$. This can be interpreted that private profile holders had higher trust before intervention.

There is a significant positive relationship between privacy status and trust 3 scores, $r(55)=.268$, $p=.044$. This can be interpreted that private profile holders had higher trust after intervention.

There is a significant positive relationship between Instagram usage and trust 3 scores, $r(56)=.298$, $p=.023$. This can be interpreted that people who use Instagram more frequently had higher trust after intervention.

Discussion

Overview of Findings

The main objective of the research was to study Instagram profile privacy along with the user's trust score; and using a profile privacy intervention by exposing them to other profiles to test whether it will change their trust. Quantitative analysis and online experiments were used and overall goals were achieved with some significant differences found.

The results suggested four key findings:

1. Users with PTP had higher trust scores than users with PCP. A new link was established to CMP theory which offered an explanation for this finding. Higher trust is contributed to by more privacy boundaries that private profiles had.
2. Users' trust scores were altered post intervention. However, there were no significant differences found between the types of profiles used in intervention and changes in trust scores (Trust 3).
3. Intervention had a positive effective on users with PTP, whose trust score were increased in both Group 1 and Group 2. This could also be interpreted as private profile owners had higher trust scores regardless before and after intervention.
4. A significant positive relationship was found between Instagram usage and changes in trust (Trust 3). People who use Instagram more frequently had higher trust scores post intervention.

Implications

Theoretical Implications

These findings are valuable additions to the understanding of Instagram profile privacy and trust. Although previous research suggested that privacy concerns were found to have a significant effect on trust in the SNS service provider.” (Fianu et al., 2019), this study was the first to link a user’s responsive behaviour to privacy concern, privacy status, or to a user’s general trust. The results linked higher privacy concern behaviour, user with private profile (PTP) to higher trust. This could be explained as discussed earlier by CPM theories and its privacy boundaries.

This research has further expanded the use of CPM theory in the context of Instagram and profile privacy studies. CPM theory taught us that privacy boundary protects personal information during online interaction. This study confirmed that users with PTP, which is classified as having both more personal and collective boundaries, have higher general trust scores than users with PCP. The findings also contributed to the understanding of privacy and trust. Like previous literature had suggested, the relationships between privacy and self-disclosure are somewhat paradoxical. This research helped to shed light on how a user’s behaviour in response to privacy is linked to their trust and allowed us to put a quantifiable number on a user’s trust based on their profile status.

Although the Intervention itself did not confirm our theory that exposure to certain types of profile status will change trust, it did however confirm that having a private profile due to higher privacy concerns linked to an positive effect on trust. In both groups, the trust score of users with PTP increased regardless of what profile they were exposed to. It showed contradicting findings to previous research on the higher the privacy concern, the less trust users have on SNS (Fogel & Nehmad, 2009).

The results from the intervention did not support the cultivation theory as this study found no significant effect from the exposure. There could however be other explanations such as the duration of exposure was insufficient for changes to occur, with the execution of the experiment such as the lack of control over whether the users had browsed the profiles properly or even if the users were sceptical or confused about the experiment, each of which may also have an impact on the results.

Practical Implications

These findings also add practical values to how users and business can approach privacy related issues and concerns. For users, the findings help them to understand that not only can the privacy setting help them to protect their personal information, but with that protection it also has a positive impact on their trust. This study helps to clarify any misconception of trust associated with what types of profile status users have.

From a commercial perspective, it was mentioned earlier that a trend has been identified where some businesses or individuals are switching from public to private Instagram accounts to gain more followers. This study has helped in interpreting this new phenomenon with a scientific explanation. By introducing more privacy boundaries, it can help to achieve commercial goals which requires trust such as attracting followers. Consumers are often more concerned about disclosing information to commercial organisation (Metzger, 2004). Therefore, this new insight is important for building better consumer relationship and loyalty.

Limitations

A number of potential limitations needed to be considered. Although a significant difference was found between profile privacy status and trust score, it is not clear as to what other influencing factors could have contributed to the trust score. Therefore, the findings can only confirm that there is a link between profile privacy and a user's trust score but it cannot confirm causation because other possible variables were not considered or were excluded in this study.

The fact that profile privacy intervention failed to have any effect on the trust score could also be explained by how the experiment was carried out where the profile used in Intervention Feedback from participants included some of level of confusion about the experiment and the profiled looked fake. Also a total number of 6 mocked-up profiles may not be enough to cause any effect.

In this study, profile privacy was considered as a response to privacy concern. However, there was no privacy concern related question in the survey and therefore the participants' levels of privacy concern is unclear.

Earlier, after an example of users on Instagram changing their accounts to gain followers, there should have been a question to identify the number of followers in order to explore the possible relationship.

Sample size turned out to be smaller than expected after omitting some participant's data where they did not have an actual Instagram account.

General trust scale has its own strength and weakness, although this research is particularly focusing on general trust that can be applied online and offline. However, these questions can be incredibly vague and ambiguous. For example, the questions were referring to most people, but what does it mean by most people. Also the context of the trust is also important. When a user trusts that other users will not do anything bad with the information available in their profile, it does not mean they will trust them enough with other information.

Evaluation

The present critical evaluation and learnings are:

Research questions and hypotheses were changed several times through the research which resulted in many revisions of literary reviews and changes in methodology. Due to the lack of the researcher's experience in SPSS statistics analysis, some questions and answers in the survey could have been constructed better. For example, the question of "What privacy status do you use on Instagram?" had 5 possible answers which were too many for the appropriate statistics test (two-way ANOVA). In the end, only 'Always Public' and 'Always Private' answers were kept and other were manually omitted.

Future research

Although evidence suggests that a significant relationship exists between privacy status and trust, further research is required to identify how much effect privacy status has on trust and what influencing factors to trust there might be. Also, this study failed to include questions to identify what types of privacy concerns users may have and the level of their concerns. This could also be a valuable insight to add to our understanding of profile privacy and trust.

Another element of profile privacy which was not included in this study is when a user switches from public to private or vice versa. This could also indicate different levels of trust, especially if data could be captured on the changes before and after the switch.

Conclusion

Choosing a public or private profile can be considered as a responsive behaviour to privacy concern which is closely linked to trust. While popular social media platforms like Instagram are here to stay for the foreseeable future, users' behaviour of choosing public or private profiles is more than a simple decision or step to protect their information. Having a private profile represents more privacy boundaries (both the personal boundary and collective boundary). These boundaries could be one reason that users with PTP have higher trust than users with PCP as they can control when they open these boundaries and to whom. On the other hand, when users with private profiles are exposed to other profiles, their trust increases regardless of what type of profile privacy they were exposed too. This is also significant as it shows that creating the privacy boundary can have long lasting positive effects on our trust which could also prevent possible turbulence. Although this research did not support the cultivation theory that persistent exposure to self-disclosure behaviours may in turn cultivate one's world view, future research can alter the research method to test other hypotheses.

References

- Alvarez, E. (2020, March 24). Instagram is cracking down on meme pages that go private as a growth hack. Retrieved from <https://www.inputmag.com/culture/instagram-private-meme-pages-accounts-followers-growth-hack-adam-mosseri>
- Bargh, J. A., & McKenna, K. Y. (2004). The Internet and social life. *Annu. Rev. Psychol.*, 55, 573-590.
- Belk, R.W. (2014). Extended self in a digital world. *Journal of Consumer Research*, 40(3), 477-500. doi: 10.1086/671052
- Boczkowski, P. J., Matassi, M., & Mitchelstein, E. (2018). How young users deal with multiple platforms: The role of meaning-making in social media repertoires. *Journal of Computer-Mediated Communication*, 23(5), 245-259.
- Cambridge Dictionary. Retrieved 2nd November, 2019. Retrieved from <https://dictionary.cambridge.org/dictionary/english/privacy-settings>
- Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behaviour, and Social Networking*, 18(1), 13-19.
- Clement, J. (2020, April 1). Number of global social network users 2010-2023. *Statista*. Retrieved from: <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>
- Europa. (2019a). Over €230 million available for security research projects. *Europa Website*. Retrieved on 2nd November, 2019. Retrieved from

https://ec.europa.eu/info/news/over-eu230-million-available-security-research-projects-2019-mar-19_en

European Commission. (2010). Attitudes on Data Protection and Electronic Identity in the European Union. *Europa website Special Eurobarometer 359*. retrieved on 2nd November, 2019. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf

European Commission. (2015). Data protection. *Europa website Special Eurobarometer 431*. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

Fianu, E., Ofori, K. S., Boateng, R., & Ampong, G. O. A. (2019). The interplay between privacy, trust and self-disclosure on social networking sites. *International Working Conference on Transfer and Diffusion of IT* (pp. 382-401). Springer.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behaviour*, 25(1), 153-160.

Foubert, J. D., & Sholley, B. K. (1996). Effects of gender, gender role, and individualized trust on self-disclosure. *Journal of Social Behaviour and Personality*, 11(5), 277–288.

Hahn, A., PhD. (2018). Communication privacy management theory. *Salem Press Encyclopedia*. Retrieved from <https://ezproxy.iadt.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ers&AN=129814571&authtype=sso&custid=ns153255&site=eds-live>

- Instagram Statistics (2019). Retrieved from <https://instagram-press.com/our-story/>
- Lee, D. (2019, October 15). Instagram's latest security feature lets you better manage third-party app permissions. *The Verge*. Retrieved from <https://www.theverge.com/2019/10/15/20916216/instagram-privacy-third-party-app-permissions-security-feature>
- Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of computer-mediated communication*, 9(4), JCMC942.
- McKenna, K. (2007). Through the Internet looking glass. *Oxford handbook of Internet psychology*, 205-221.
- McKenna, K., Joinson, A. N., Reips, U. D., & Postmes, T. (2007). *Oxford handbook of internet psychology*. New York: Oxford University Press.
- Park, Y. J. (2011). Digital literacy and privacy behaviour online. *Communication Research*, 40(2), 215–236. doi:10.1177/0093650211418338
- Petronio, S. (2002) *Boundaries of privacy: dialects of disclosure*. Albany: State University of New York Press
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: a cross-discipline view of trust. *Academy of Management Review*, 23(3), 393–404.
- Saffarizadeh, K., Boodraj, M., & Alashoor, T. M. (2017). Conversational assistants: investigating privacy concerns, trust, and self-disclosure. *ICIS 2017 Proceedings*. 19. Retrieved from <https://pdfs.semanticscholar.org/982a/7639da911924f5595606ec44198d1720dc86.pdf>

- Shifman, L. (2013). Memes in a Digital World: Reconciling with a Conceptual Troublemaker. *Journal of Computer-Mediated Communication*, 18(3), 362–377. doi:10.1111/jcc4.12013
- Tamir, D. I., & Mitchell, J. P. (2012). Disclosing information about the self is intrinsically rewarding. *Proceedings of the National Academy of Sciences of the United States of America*, 109(21), 8038–8043. doi:10.1073/pnas.1202129109.
- Tang, J., & Liu, H. (2015). Trust in Social Media. *Synthesis Lectures on Information Security, Privacy, & Trust*. Morgan & Claypool Publishers. doi: 10.2200/S00657ED1V01Y201507SPT013
- Thompson, S. (2019, November 22). Social media the ‘big game changer’ for trust in experts. *Irish Times*. Retrieved from <https://www.irishtimes.com/news/science/social-media-the-big-game-changer-for-trust-in-experts-1.4059313>
- Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviours among Facebook users. *New Media & Society*, 20(1), 141-161.
- Wieselquist, J., Rusbult, C.E., Foster, C.A., Agnew, C.R., 1999. Commitment, pro-relationship behavior, and trust in close relationships. *J. Personal. Soc. Psychol.* 77:942–66
- Yamagishi, T. & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion*, 18, 129-166

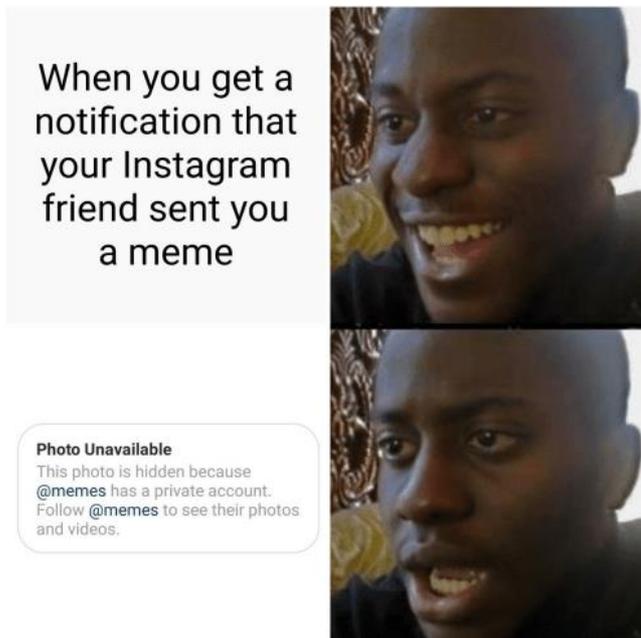
Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behaviour, 45*, 158-167. Doi: 10.1016/j.chb.2014.12.012

Appendix A

Examples of Memes of attitude towards private profiles



Figure A1



It was probably something I already saw on Reddit anyway.

Figure A2

When you're trying to stalk someone on Instagram but their accounts private

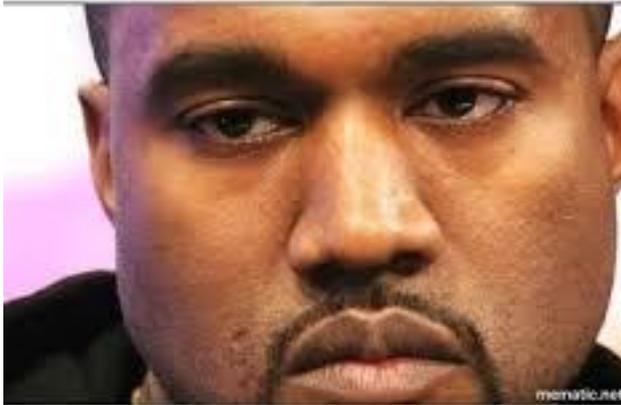


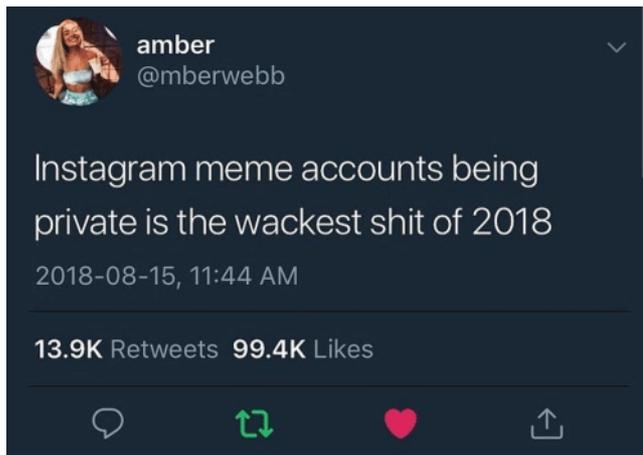
Figure A3

When you go to look at someone's Instagram but their account private



Such a disappointment. And when the person keeps switching between private or not 🙄 like bruuuh is not like you like privacy, let it public! 😞
👁️ needstostalk prostalker

Figure A4



Shits annoying as fuck. I'm staying public

Figure A5

When you tap on someone's Instagram account but they're private so you have to judge them off of their tiny profile pic



Figure A6



Figure A6



Figure A7

Appendix B

Examples of public profile and private profile on Instagram



Figure B1: sample public Instagram profile

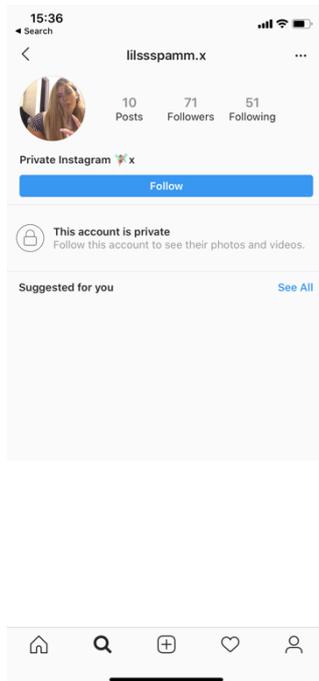


Figure B2: sample private Instagram profile

Appendix C

Online Survey and Experiment

There were two Survey Monkey Links used and randomly distributed.
(They are no longer working because surveys are closed)

- Survey 1 (PCP intervention):
<https://www.surveymonkey.com/r/VQSQ2N5>
- Survey 2 (PTP intervention):
<https://www.surveymonkey.com/r/HWLDWTR>

Welcome

You are asked to complete this online survey for a research project as a part of my MSc in Cyberpsychology study. The research is designed to explore the relationship between profile privacy (public or private) and trust.

Brief

Thanks for your interest in taking this survey.

Why this research?

As more people spend more time on social media, I want to understand how social media usage is impacting on our behaviour and attitude. This research is designed to provide a better understanding of an Instagram user's profile privacy choice and its impact on viewers' general trust.

Data

This survey will collect some basic demographic questions about you, your general usage of Instagram, profile privacy status and opinion on general trust. There are 28 questions in total and estimated time to complete is 6 minutes.

Your name will NOT be collected so your data is anonymised however it's preferable that you can provide us with your email address in case we need to contact you for follow up but it is not compulsory.

The data will be stored on Survey Monkey and my personal laptop which is password and biometric data protected. I am the only user with access.

I respect your trust and privacy and therefore your data will not be sold or passed on to any other third parties.

Rights

You may decide to stop completing the survey at any time. You have the right to request that any data you provided to that point be withdrawn. You have the right to omit or refuse to answer or respond to any demographic questions that are asked of

you (as appropriate).

Benefits & Risks

During your participation, you may become more aware and conscious about your own profile privacy and even take action to change. This research is to collect the data and your opinion prior to taking this survey.

There are no other known risks to taking part in this survey.

Consent

By clicking on 'Yes' below, you are agreeing that you have read and understood the information above; you are aware of potential risks, your questions have been answered satisfactorily and you are taking part in this research voluntarily. I will process your data in line with the research plan.

If you have any questions, please contact:

myself: N00173983@student.iadt.ie

my supervisor: Robert.Griffin@iadt.ie

Q1 Do you agree to participate in this survey?

Yes

No

Questionnaire

Q2 Do you use Instagram?

Yes I still use

Never used

Used but not anymore

Q3 How many Instagram account(s) do you have?

1

2

3+

Q4 What is your Age?

Under 18

18-24

25-34

35-44

45-54

55-64

65+

Q5 What is the gender you are most identified with?

- Female
- Male
- Other
- Prefer not to answer

Q6 What privacy status do you use on Instagram?

- I always or mainly use a public profile
- I always or mainly use a private profile
- I change my profile status regularly
- I don't have an Instagram account
- Other (please specify)

Q7 (Optional) Please include your email address in case the researcher needs to do a follow up, otherwise leave it blank and proceed to the next question.

Q8 How much do you use Instagram?

- Daily
- Weekly
- Monthly
- None at all

Q9 What do you mainly use Instagram for? (Choose 1 **Social Interaction (e.g. friend's updates and** answer based on your primary Instagram account if you have more than 1 account)

- Social Interaction (e.g. friend's updates and communicate)
- Archiving (e.g. record events, thoughts, photos or videos etc)
- Self-expression (e.g. provide updates, share information or get noticed)
- Escapism (e.g. escape from reality, forget troubles or avoid loneliness)
- Peeking (e.g. browse photos, celebrities or other people's lives)
- Other (please specify)

Trust Questionnaire

Q10 Most people are basically honest.

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

Q11 Most people are trustworthy

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

Q12 Most people are basically good and kind

Strongly agree
Agree
Neutral
Disagree
Strongly disagree

Q13 Most people are trustful of others

Strongly agree
Agree
Neutral
Disagree
Strongly disagree

Q14 I am trustful

Strongly agree
Agree
Neutral
Disagree
Strongly disagree

Q15 Most people will respond in kind when they are trusted by others.

Strongly agree
Agree
Neutral
Disagree
Strongly disagree

Experiment (Profile intervention)

There are a total of 6 profiles.

You only need to browse them as you would normally browse random profiles on Instagram, no specific instruction on what you should look out for.

These profiles are not clickable

Survey 1 - Public Profile Intervention.

Mocked-up public profiles (three female)

Survey 2 - Private Profile Intervention.

Mocked-up private profiles (three male)

Trust Questionnaire (repeat)

Q16 Most people are basically honest

Q17 Most people are trustworthy

Q18 Most people are basically good and kind

Q19 Most people are trustful of others

Q20 I am trustful

Q21 Most people will respond in kind when they are trusted by others.

Debrief

Thank you for participating in this research.

This research will help us to understand more about the relationship between trust and Instagram users' profile privacy; especially if and how profiles with different privacy settings can affect our trust.

If you have any questions about this research or would like to follow up with the researcher.

Please Contact: N00173983@student.iadt.ie

Appendix D

Research Design Diagram

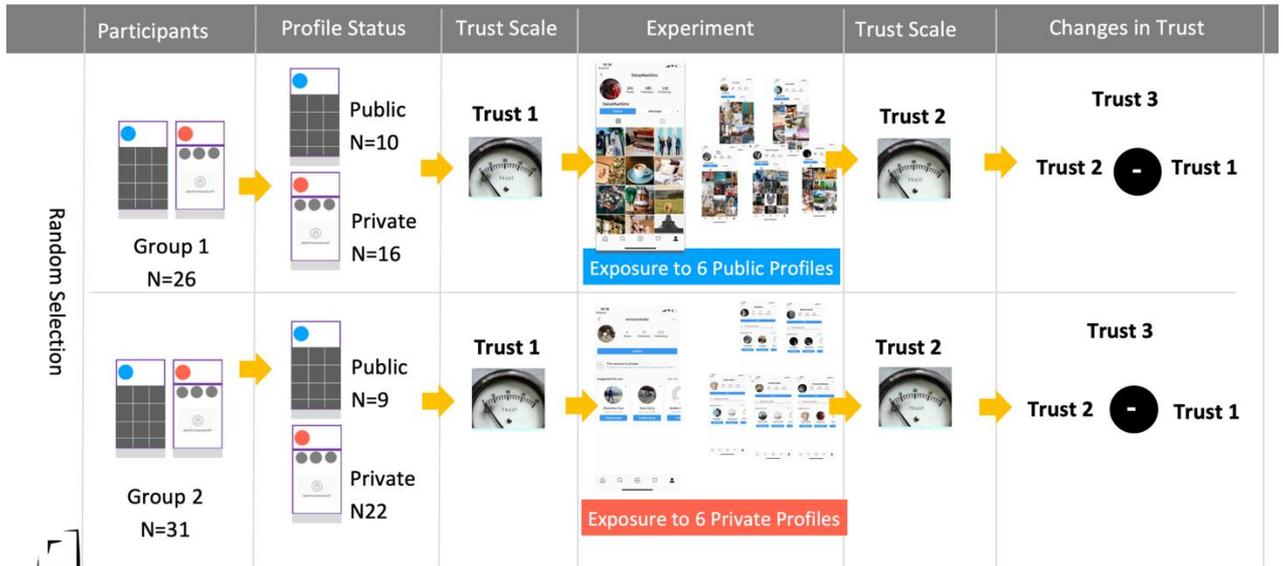


Figure C1: Diagram to explain the research design.

Appendix E

General Trust Scale

Reference:

Yamagishi, T. & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion, 18*, 129-166.

Description of Measure:

A 6-item questionnaire that uses general statements to measure participants' beliefs about honesty and trustworthiness of others, in general. Some of these items come from Yamagishi's (1986) Trust Scale.

Scale:

Using the following scale, please indicate how much you agree or disagree with the following statements:

1	2	3	4	5
<i>Strongly Disagree</i>	<i>Disagree</i>	<i>Neutral</i>	<i>Agree</i>	<i>Strongly Agree</i>

- 1.) Most people are basically honest.
- 2.) Most people are trustworthy.
- 3.) Most people are basically good and kind.
- 4.) Most people are trustful of others.
- 5.) I am trustful.
- 6.) Most people will respond in kind when they are trusted by others.

Scoring:

The score for each item is averaged together to form a continuous measure of generalized trust.

Appendix F

Mocked-up Public and Private Profiles for Profile Intervention

Survey 1 - Public Profile Intervention. Mocked-up public profiles (three female)

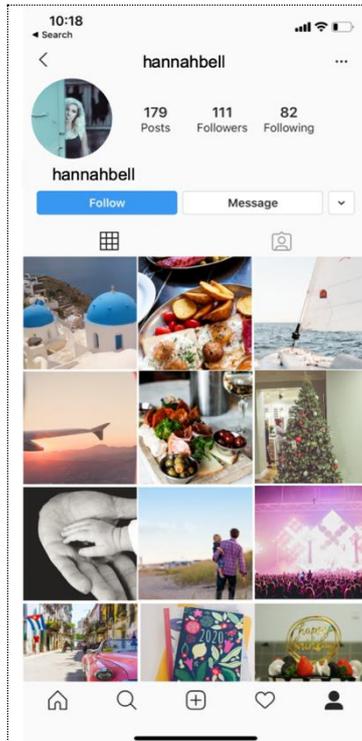


Figure F1.1: Mocked-up Public Profile

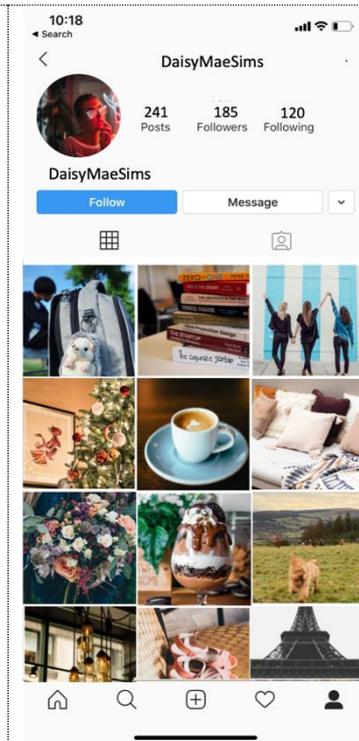


Figure F1.2: Mocked-up Public Profile

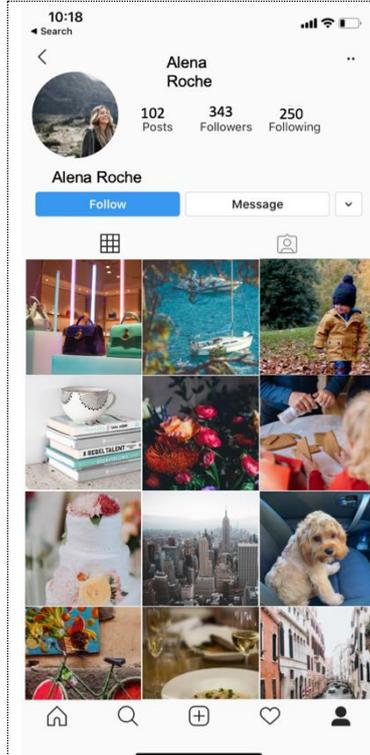


Figure F1.3: Mocked-up Public Profile

Survey 2 - Private Profile Intervention. Mocked-up private profiles (three female)

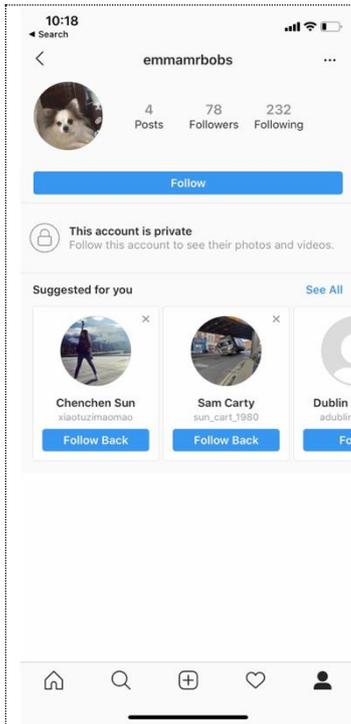


Figure F2.1: Mocked-up Private Profile

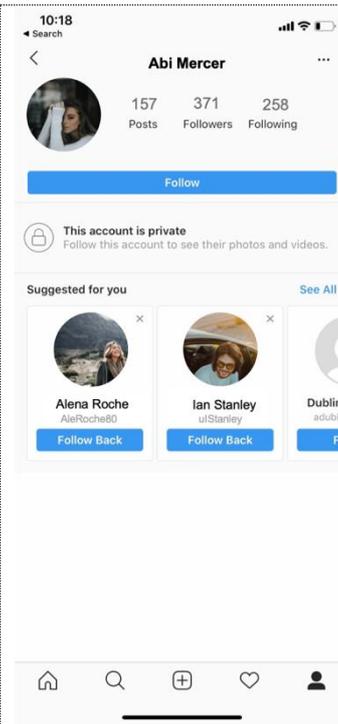


Figure F2.3: Mocked-up Private Profile

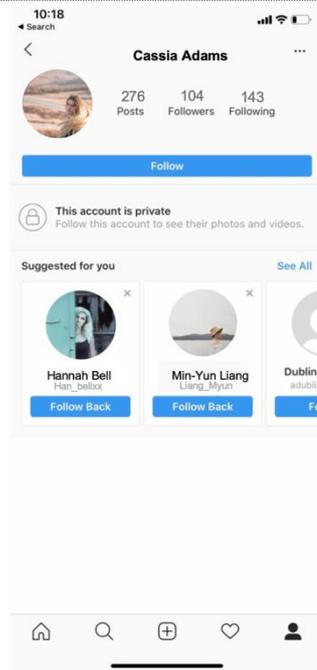


Figure F2.2: Mocked-up Private Profile

Survey 2 - Private Profile Intervention. Mocked-up private profiles (three male)

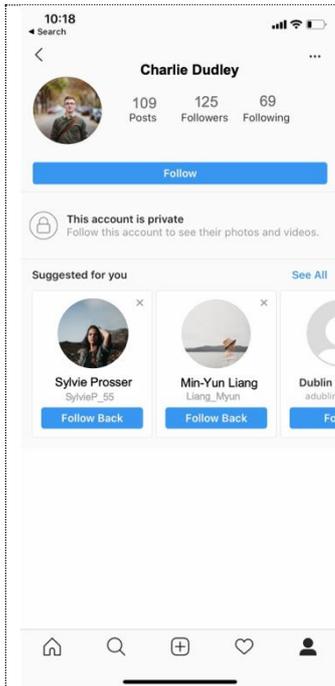


Figure F2.4: Mocked-up Private Profile

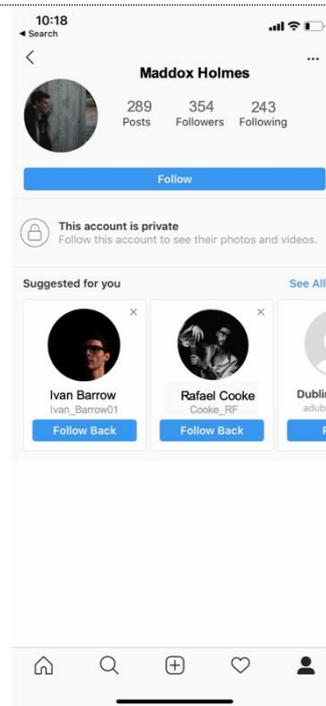


Figure F2.5: Mocked-up Private Profile

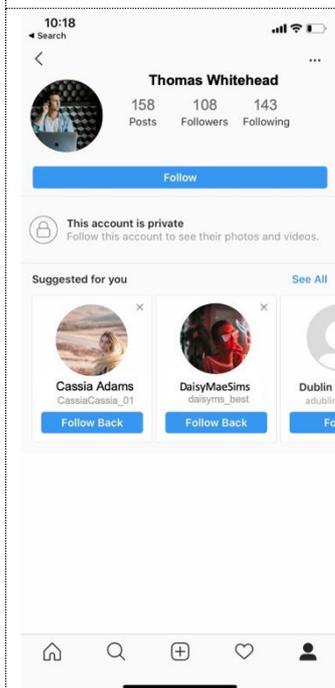


Figure F2.6: Mocked-up Private Profile

Appendix G

Ethical Form

DEPARTMENT OF TECHNOLOGY AND PSYCHOLOGY ETHICAL APPROVAL FORM A

Title of project

Private or Public Profile: Exploring the Linkage between Profile Privacy & Trust on Instagram

Name of researcher Jing Reilly N00173983

Email contact N00173983@students.iadt.ie

Name of supervisor Rob Griffittin

		Yes	No	N/A
1	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	V		
2	Will you tell participants that their participation is voluntary?	V		
3	Will you obtain written consent for participation (through a signed or 'ticked' consent form)?	V		
4	If the research is observational, will you ask participants for their consent to being observed?			V
5	Will you tell participants that they may withdraw from the research at any time and for any reason?	V		
6	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	V		
7	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	V		
8	Will you debrief participants at the end of their participation (i.e., give them a brief explanation of the study)?	V		
9	If your study involves people between 16 and 18 years, will you ensure that <u>passive</u> consent is obtained from parents/guardians, with active consent obtained from both the child and their school/organisation?			V
10	If your study involves people under 16 years, will you ensure that <u>active</u> consent is obtained from parents/guardians <u>and</u> that a parent/guardian or their nominee (such as a teacher) will be present throughout the data collection period?			V
11*	Does your study involve an external agency (e.g. for recruitment)?		V	
12	Is there any realistic risk of any participants experiencing either physical or psychological distress or discomfort?		V	
13	Does your project involve work with animals?		V	

14	Do you plan to give individual feedback to participants regarding their scores on any task or scale?		V	
15	Does your study examine any sensitive topics (such as, but not limited to, religion, sexuality, alcohol, crime, drugs, mental health, physical health)		V	
16	Is your study designed to change the mental state of participants in any negative way (such as inducing aggression, frustration, etc.)		V	
17	Will your project involve deliberately misleading participants in any way?		V	
18	Do participants fall into any of the following special groups?	People with learning or communication difficulties	V	
		Patients (either inpatient or outpatient)	V	
		People in custody	V	

If you have ticked **No** to any of questions 1 to 11, or **Yes** to any of questions 12 to 18 you should refer to the PSI Code of Professional Ethics and BPS Guidelines and consult with your supervisor without delay. You will need to fill in Ethical Approval Form B and submit it to the Department of Technology and Psychology Ethics Committee (DTPEC) in place of this form.

There is an obligation on the researcher to bring to the attention of the DTPEC any issues with ethical implications not clearly covered by the above checklist.

I consider that this project has **no** significant ethical implications to be brought before the DTPEC. I have read and understood the specific guidelines for completion of Ethics Application Forms. I am familiar with the PSI Code of Professional Ethics and BPS Guidelines (and have discussed them with my supervisor).

Signed _____ Print Name _____ Date _____
Applicant

I have discussed this project with my student, and I agree that it has no significant ethical implications to be brought before the DTPEC.

Signed _____ Print Name _____ Date _____
Supervisor

* If you are dealing with an external agency, you must submit a letter from that agency with the form A. The letter must provide contact details, and must show that they have agreed for you to carry out your research in their organization.

Appendix H
SPSS Descriptive Data

Table H1

Frequencies by Group

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Public	26	44.8	44.8	44.8
	Private	32	55.2	55.2	100.0
	Total	58	100.0	100.0	

Table H2

Frequencies by Privacy Status

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always Public	19	32.8	33.3	33.3
	Always private	38	65.5	66.7	100.0
	Total	57	98.3	100.0	
Missing		1	1.7		
Total		58	100.0		

Table H3

Frequencies by Instagram Usage

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Daily	31	53.4	53.4	53.4
	Weekly	14	24.1	24.1	77.6
	Monthly	8	13.8	13.8	91.4
	None at all	5	8.6	8.6	100.0
	Total	58	100.0	100.0	

Table H4

Frequencies by Purpose

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Social Interaction	29	50.0	50.0	50.0
	Archiving	6	10.3	10.3	60.3
	Self-expression	4	6.9	6.9	67.2
	Escapism	3	5.2	5.2	72.4
	Peeking	10	17.2	17.2	89.7
	Other	6	10.3	10.3	100.0
	Total	58	100.0	100.0	

Table H5

Frequencies by Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	4	6.9	6.9	6.9
	25-34	11	19.0	19.0	25.9
	35-44	27	46.6	46.6	72.4
	45-54	14	24.1	24.1	96.6
	55-64	2	3.4	3.4	100.0
	Total	58	100.0	100.0	

Table H6

Frequencies by Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	35	60.3	60.3	60.3
	Male	22	37.9	37.9	98.3
	Prefer not to answer	1	1.7	1.7	100.0
	Total	58	100.0	100.0	

Table H7
Descriptive Statistics for Trust Scores T1, T2 and T3

	N	Minimum	Maximum	Mean	Std. Deviation
Trust before and after	58	-1.00	2.33	.1580	.51811
Trust 1 average score before	58	.00	3.50	2.2759	.61539
Trust 2 average score after	58	.00	3.50	2.1178	.76854
Valid N (listwise)	58				

Appendix I

Histogram

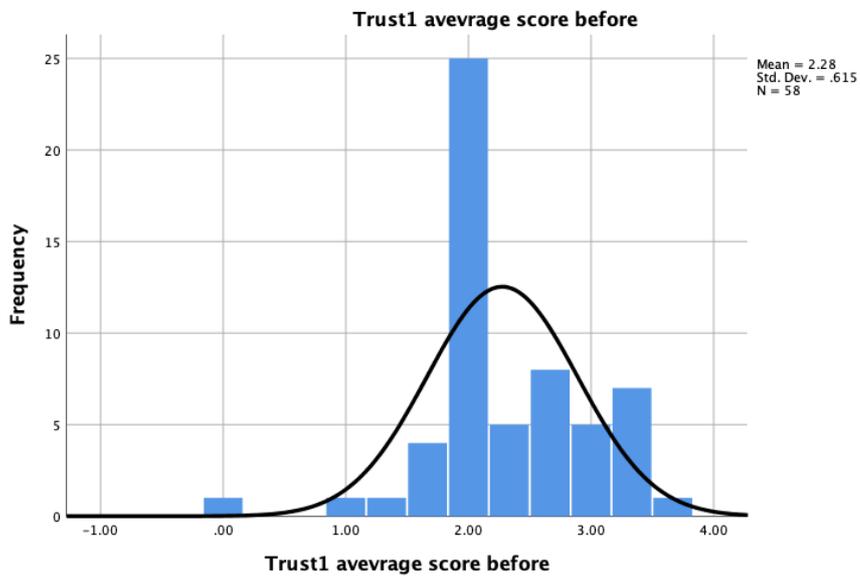


Figure I1: Histogram for Trust before Intervention (T1)

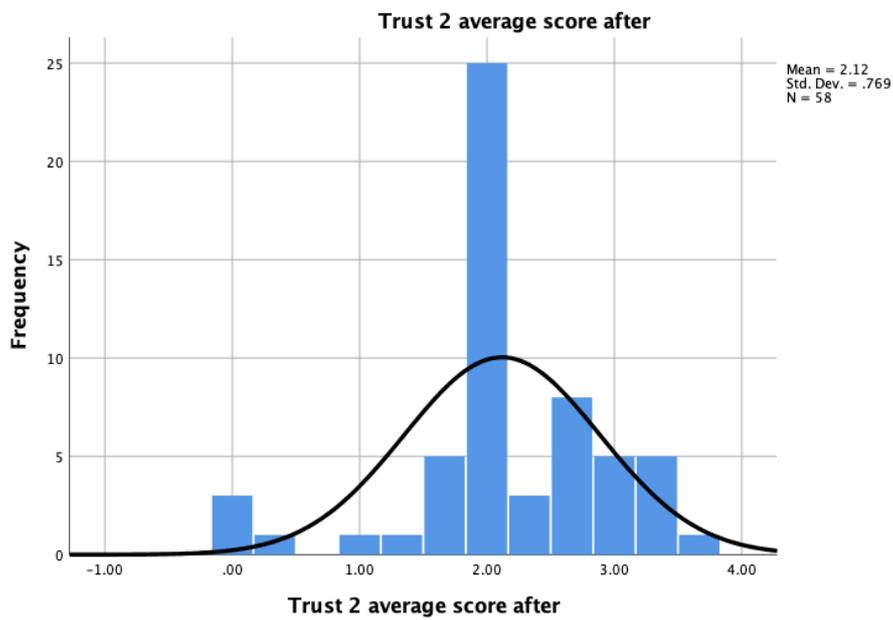


Figure I2: Histogram for Trust after Intervention (T2)

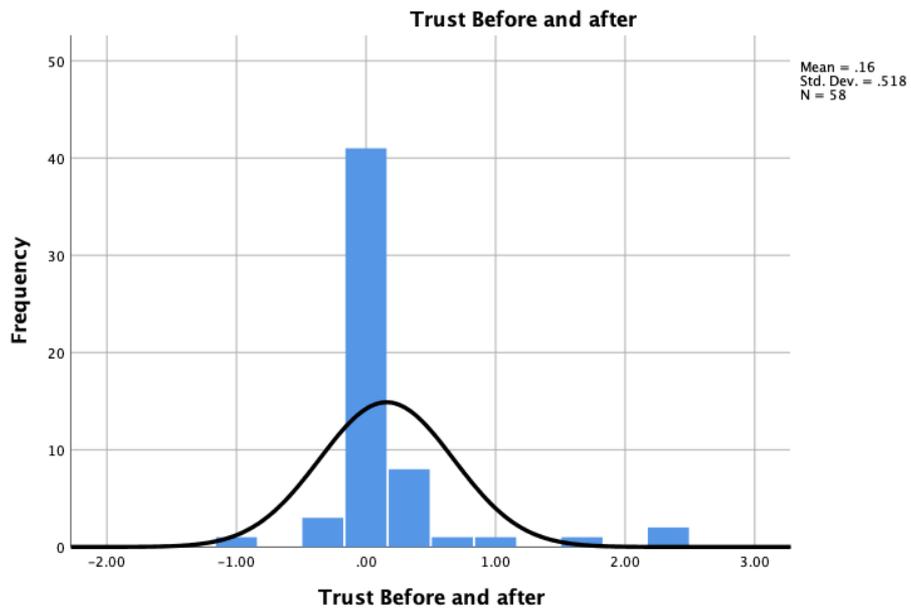


Figure I3: Histogram for change in Trust Score (T3= T2-T1)

Appendix J
SPSS Output T-Test

Table J1
Group Statistics

	Privacy Status	N	Mean	Std. Deviation	Std. Error Mean
Trust 1 Average Score before	Always Public	19	2.0000	.63586	.14588
	Always Private	38	2.3860	.55223	.08958

Table J2
Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Trust1 Average Score before	Equal variances assumed	.861	.358	-2.365	55	.022	-.38596	.16323	-.71308	-.05885
	Equal variances not assumed			-2.255	31.928	.031	-.38596	.17119	-.73469	-.03724

Appendix K
SPSS Output Two-way ANOVA

Table K1
Between-Subjects Factors

		Value Label	N
Group	1	Public	26
	2	Private	31
Privacy Status	1	Always Public	19
	2	Always private	38

Table K2
Descriptive Statistics Dependent Variable: T3

Group	Privacy Status	Mean	Std. Deviation	N
Public	Always Public	.0000	.17568	10
	Always private	.3229	.69247	16
	Total	.1987	.56964	26
Private	Always Public	-.0741	.36430	9
	Always Private	.2121	.51224	22
	Total	.1290	.48631	31
Total	Always Public	-.0351	.27543	19
	Always private	.2588	.58855	38
	Total	.1608	.52229	57

Table K3
Levene's Test of Equality of Error Variances^{a,b}

		Levene Statistic	df1	df2	Sig.
Trust Before and After	Based on Mean	1.669	3	53	.185
	Based on Median	.723	3	53	.543
	Based on Median and with adjusted df	.723	3	38.133	.544
	Based on trimmed mean	1.302	3	53	.284

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Dependent variable: Trust Before and after

b. Design: Intercept + Group + Privacy Status + Group * Privacy Status

Table K4

Tests of Between-Subjects Effects Dependent Variable: T3

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	1.234 ^a	3	.411	1.552	.212	.081
Intercept	.666	1	.666	2.514	.119	.045
Group	.107	1	.107	.404	.528	.008
Privacy Status	1.163	1	1.163	4.389	.041	.076
Group * Privacy Status	.004	1	.004	.016	.900	.000
Error	14.042	53	.265			
Total	16.750	57				
Corrected Total	15.276	56				

a. R Squared = .081 (Adjusted R Squared = .029)

Table K5

Group Dependent Variable: T3

Group	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Public	.161	.104	-.047	.370
Private	.069	.102	-.135	.273

Table K6

Privacy Status Dependent Variable: T3

Privacy Status	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Always Public	-.037	.118	-.274	.200
Always private	.268	.085	.098	.437

Table K7

Pairwise Comparisons Dependent Variable: T3

(I) Privacy Status	(J) Privacy Status	Mean Difference (I-J)	Std. Error	Sig. ^b	95% Confidence Interval for Difference ^b	
					Lower Bound	Upper Bound
Always Public	Always private	-.305*	.145	.041	-.596	-.013
Always Private	Always Public	.305*	.145	.041	.013	.596

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Appendix L
SPSS Output Correlations

Table L1
Correlations Descriptive Statistics

Mean	Std. Deviation	N
1.67	.476	57
2.2759	.61539	58

Table L2
Correlations Privacy Status and Trust 1

		Privacy Status	Trust 1 (Before)
Privacy Status	Pearson Correlation	1	.304*
	Sig. (2-tailed)		.022
	N	57	57
Trust 1 (Before)	Pearson Correlation	.304*	1
	Sig. (2-tailed)	.022	
	N	57	58

*. Correlation is significant at the 0.05 level (2-tailed).

Table L3
Descriptive Statistics Instagram Usage and Trust 3 (Change)

	Mean	Std. Deviation	N
Instagram Usage	1.78	.992	58
Trust 3 (Change)	.1580	.51811	58

Table L4
Correlations Instagram Usage and Trust 3

		Instagram Usage	Trust 3
Instagram Usage	Pearson Correlation	1	.298*
	Sig. (2-tailed)		.023
	N	58	58
Trust 3	Pearson Correlation	.298*	1
	Sig. (2-tailed)	.023	
	N	58	58

*. Correlation is significant at the 0.05 level (2-tailed).

Table L5
Descriptive Statistics Privacy Status and Trust 3

	Mean	Std. Deviation	N
Trust 3	.1580	.51811	58
Privacy Status	1.67	.476	57

Table L6
Correlations Privacy Status and Trust 3

		Trust 3	Privacy Status
Trust 3	Pearson Correlation	1	.268*
	Sig. (2-tailed)		.044
	N	58	57
Privacy Status	Pearson Correlation	.268*	1
	Sig. (2-tailed)	.044	
	N	57	57

*. Correlation is significant at the 0.05 level (2-tailed).

Table L7
Correlations All

		Group	Privacy Status	Instagram	Instagram Accounts	Age	Gender	Instagram Usage	Purpose	Trust Before and after	Trust 1 average score before	Trust 2 average score after
Group	Pearson Correlation	1	.100	-.118	.140	-.092	-.223	.041	-.060	-.071	-.066	-.005
	Sig. (2-tailed)		.461	.377	.293	.490	.093	.758	.653	.594	.623	.972
	N	58	57	58	58	58	58	58	58	58	58	58
Privacy Status	Pearson Correlation	.100	1	.017	.157	-.243	-.189	.000	-.105	.268*	.304*	.058
	Sig. (2-tailed)	.461		.901	.243	.068	.159	1.000	.437	.044	.022	.669
	N	57	57	57	57	57	57	57	57	57	57	57
Instagram	Pearson Correlation	-.118	.017	1	-.052	-.065	.036	.710**	.374**	.207	.157	-.014
	Sig. (2-tailed)	.377	.901		.698	.627	.786	.000	.004	.119	.240	.916
	N	58	57	58	58	58	58	58	58	58	58	58
Instagram Accounts	Pearson Correlation	.140	.157	-.052	1	.007	-.257	-.054	-.112	-.080	.045	.090
	Sig. (2-tailed)	.293	.243	.698		.961	.051	.687	.404	.552	.736	.502
	N	58	57	58	58	58	58	58	58	58	58	58
Age	Pearson Correlation	-.092	-.243	-.065	.007	1	-.082	-.004	-.043	.018	-.186	-.161
	Sig. (2-tailed)	.490	.068	.627	.961		.542	.975	.747	.894	.161	.227
	N	58	57	58	58	58	58	58	58	58	58	58

Gender	Pearson Correlation	-.23	-.189	.036	-.257	-.082	1	-.041	.014	-.206	.005	.143
	Sig. (2-tailed)	.093	.159	.786	.051	.542		.757	.917	.121	.971	.286
	N	58	57	58	58	58	58	58	58	58	58	58
Instagram Usage	Pearson Correlation	.041	.000	.710**	-.054	-.004	-.041	1	.211	.298*	.026	-.180
	Sig. (2-tailed)	.758	1.000	.000	.687	.975	.757		.113	.023	.844	.177
	N	58	57	58	58	58	58	58	58	58	58	58
Purpose	Pearson Correlation	-.060	-.105	.374**	-.112	-.043	.014	.211	1	-.077	.129	.155
	Sig. (2-tailed)	.653	.437	.004	.404	.747	.917	.113		.566	.335	.245
	N	58	57	58	58	58	58	58	58	58	58	58
Trust Before and After	Pearson Correlation	-.071	.268*	.207	-.080	.018	-.206	.298*	-.077	1	.089	-.603*
	Sig. (2-tailed)	.594	.044	.119	.552	.894	.121	.023	.566		.508	.000
	N	58	57	58	58	58	58	58	58	58	58	58
Trust1 average score before	Pearson Correlation	-.066	.304*	.157	.045	-.186	.005	.026	.129	.089	1	.741**
	Sig. (2-tailed)	.623	.022	.240	.736	.161	.971	.844	.335	.508		.000
	N	58	57	58	58	58	58	58	58	58	58	58
Trust 2 average score after	Pearson Correlation	-.005	.058	-.014	.090	-.161	.143	-.180	.155	-.603*	.741*	1
	Sig. (2-tailed)	.972	.669	.916	.502	.227	.286	.177	.245	.000	.000	
	N	58	57	58	58	58	58	58	58	58	58	58

*. Correlation is significant at the 0.05 level (2-tailed).

** . Correlation is significant at the 0.01 level (2-tailed).