

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Tena Prvulović

**Vloga informiranega razkrivanja podatkov pri zaupanju v spletna
družbena omrežja**

**The role of informed data disclosure in trust towards social
networking sites**

Diplomsko delo

Ljubljana, 2020

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Tena Prvulović

Mentorica: doc. dr. Urška Tuškej Lovšin

**Vloga informiranega razkrivanja podatkov pri zaupanju v spletna
družbena omrežja**

**The role of informed data disclosure in trust towards social
networking sites**

Diplomsko delo

Ljubljana, 2020

Acknowledgement

I wish to thank all the people whose assistance was provided during my studies.

Foremost, I wish to express my deepest gratitude to my mentor. Professor Urška Tuškej Lovšin has expertly guided me through this process and supported me when times got tough.

Without your persistent guidance, this thesis would not have been realised.

I wish to acknowledge the support I had from my family and friends. Most of all my sister, Maša. Thank you for all the patience and advice.

The role of informed data disclosure in trust towards social networking sites

The number of social networking site users is rapidly growing. Users are encouraged to disclose their data on these sites. By disclosing their data, users expose themselves to a number of risks. Studies show that users are concerned that their data will be used in unforeseen ways and would like to be informed about how their data is used. Yet, even though users express high levels of privacy concerns they are at the same time being relatively uneducated in disclosing their data. Therefore, it is important to urge users to become more aware of the privacy protocols of social networking sites. Studies have shown that in turn, social networking sites can expect more trust from their users if they provide high quality information and educate them. Therefore, it's important to understand what role informed data disclosure has in trusting social networking sites. With an aim to research this topic, theoretical part of the thesis focuses on a literature review of the relevant contributions to the topics of data disclosure on social networking sites, privacy awareness and trust in social networking sites. The empirical part of the thesis contains qualitative research in the form of six semi-structured interviews. The research showed that even when users are aware of the possible risks, they consciously expose themselves to possible risks when disclosing their data on social networking sites and mostly do not change their behaviour. Trust in social networking sites has been shown to decrease as the privacy awareness of users increases.

Keywords: privacy, brand trust, social networking sites

Vloga informiranega razkritja podatkov na zaupanje v družbena omrežja

Število uporabnikov spletnih družbenih omrežij hitro narašča. Te platforme uporabnike spodbujajo, da na njih razkrivajo svoje podatke, čeprav se uporabniki na ta način izpostavljajo številnim tveganjem. Študije so pokazale, da so uporabniki zaskrbljeni glede razkrivanja svojih podatkov in bi o njihovi uporabi želeli biti bolj informirani. Kljub izražanju zaskrbljenosti glede uporabe osebnih podatkov pa posamezniki ne kažejo želje po ozaveščanju glede razkrivanja teh podatkov na spletnih družbenih omrežjih. Zato si je potrebno prizadevati najti načine, na katere bi se uporabniki začeli zavedati pomena ozaveščanja glede razkrivanja podatkov. Študije so namreč pokazale, da bi na ta način spletna družbena omrežja lahko bila deležna večjega zaupanja s strani uporabnikov. Zato je pomembno razumeti, kakšno vlogo ima informirano razkrivanje podatkov pri zaupanju v družbena omrežja. Teoretični del diplomske naloge se, s ciljem preučiti to vprašanje, osredotoča na pregled literature o tematikah razkrivanja podatkov na družbenih omrežjih, ozaveščenosti o zasebnosti in zaupanju v spletna družbena omrežja. Empirični del diplomske naloge vsebuje kvalitativno raziskavo, izvedeno v obliki šestih polstrukturiranih intervjujev. Raziskava je pokazala, da tudi kadar se uporabniki zavedajo možnih tveganj, ki so jim izpostavljeni pri razkrivanju podatkov na spletnih družbenih omrežjih, večinoma ne spremenijo svojega vedenja. Pokazalo se je, da se, s tem ko se ozaveščenost uporabnikov o zasebnosti povečuje, zaupanje v spletna družbena omrežja zmanjšuje.

Ključne besede: zasebnost, zaupanje v blagovno znamko, spletna družbena omrežja

Table of contents

1 INTRODUCTION.....	6
2 DATA DISCLOSURE ON SOCIAL NETWORKING SITES	9
2.1 SELF-DISCLOSURE ON SOCIAL NETWORKING SITES	9
2.2 PERCEIVED RISKS OF DATA DISCLOSURE ON SOCIAL NETWORKING SITES.....	10
2.3 PRIVACY CONCERNS	11
2.4 THE ROLE OF PRIVACY CONCERNS IN DATA DISCLOSURE.....	12
3 AWARE DATA DISCLOSURE	15
4 TRUST IN SOCIAL NETWORKING SITES.....	17
4.1 DEFINING TRUST IN SOCIAL NETWORKING SITES	17
4.2 THE ROLE OF TRUST IN SNS.....	18
4.3 ANTECEDENTS OF TRUST IN SOCIAL NETWORKING SITES	19
5 THEORETICAL FRAMEWORK SUM-UP AND THE DEFINITION OF THE RESEARCH PROBLEM.....	21
6 EMPIRICAL RESEARCH	24
6.1 METHODOLOGY.....	24
6.3 ANALYSIS OF INTERVIEWS.....	25
6.4 DISCUSSION	29
6.4 LIMITATIONS AND FURTHER RESEARCH.....	31
6.5 PRACTICAL IMPLICATIONS.....	32
7 CONCLUSION	33
8 SUMMARY IN THE SLOVENE LANGUAGE.....	34
9 REFERENCES.....	36
10 APPENDIXES	42
10.1 APPENDIX A	42
10.2 APPENDIX B	50
10.3 APPENDIX C	58
10.4 APPENDIX D	65
10.5 APPENDIX E.....	72
10.6 APPENDIX F.....	81

1 INTRODUCTION

Nowadays, in the so-called digital age, people are spending a substantial amount of time on social networking sites, with an average of 144 minutes daily as measured in 2019 (Statista, 2019). The past decade has been marked by an exponential surge in the usage of social networking sites (Perrin, 2015). The number of social networking site users has grown by 288 million users in the previous year alone (Kemp, 2019). This growth is also accompanied by an increase in privacy and security concerns as people are prompted to share their information and engage with others in a quick and easy way. This trend of data disclosure on social networking sites leads to privacy concerns which is one of the very relevant problems in regard to data disclosure on social networking sites. Questions are being raised about how and under which conditions the data of users is collected, as well as what type of data users are willing to disclose on social networking sites (Taddei and Contena, 2013).

Research shows that users willingly divulge personal, at times even intimate, information on social networking sites which implies that a certain degree of trust exists towards those social networking sites (Dwyer, Hiltz and Passerini, 2007). As users disclose personal data online on social networking sites, they expose themselves to a number of risks. By examining the difference between perceived privacy risks and perceived privacy concerns of social networking site users and their self-disclosure on those social networking sites, one can determine how informed the data disclosure of users is. Studies show that users are concerned that their data will be used in unforeseen ways and would like to be informed about how their data is used, so that in turn they can make informed choices (van den Berg and van den Hof, 2012). Yet, Lilley, Grodzinsky and Gumbus (2012) argue that social networking site users are expressing high levels of privacy concerns while at the same time being relatively uneducated and passive. A study (Joergensen, 2014) has shown that users are not aware of the implications of disclosing their data on social networking sites and its' relation to third parties. Joergensen (2014) states that laws, state-imposed regulations or the accountability of the social networking sites themselves isn't enough for securing the privacy protection of users. As people are gradually using social networking sites more on a daily basis, it is important to assure safety of its users and making them aware of the potential risk they can be exposed to when disclosing their personal information on social networking sites. It is important to urge users to become

more aware of the privacy protocols of social networking sites and demand more protection, as they are exposing themselves to risks by being uninformed and unaware of the possible privacy risks. In turn, social networking sites can expect more trust from their users if they provide high quality information and educate their users (Miranda and Saunders, 2003). With a higher degree of trust comes more loyalty towards the social networking site (Hoffman, Novak, Perlata, 1999). Moreover, trusting a social networking site leads to lower privacy concerns and subsequently more data disclosure (Taddei and Contena, 2013).

This thesis will concentrate on researching the role of aware and informed data disclosure and its connection to trust of users towards a social networking site. Researching how the concepts of privacy awareness and subsequently having informed data disclosure relates to brand trust can help us understand how to improve privacy policies of social networking sites, legislation and regulations regarding data gathering, analysing and usage. Therefore, this thesis will focus on answering the following research question: what role does informed data disclosure have in trust towards a social networking site?

To answer the research question and to give more understanding to the relationships between the concepts of informed data disclosure on social networking sites and trust towards those sites, a study which includes various social networking sites is needed. In this thesis, three social networking sites will be used to understand the influence informed data disclosure on social networking sites has on brand trust towards those sites: Facebook, Instagram and LinkedIn.

Facebook is a social networking site which is open for membership to anyone claiming to be over the age of 13. At first it was intended only for students, but it expanded to become a global social networking site in 2013 and now has more than 2.3 billion monthly users (Statista, 2018(a)). Earlier studies (Acquisti and Gross, 2006; Gross and Acquisti, 2005) have shown that privacy concerns did not impact the amount of data disclosed on Facebook. Since then, the social networking site has changed immensely. A later longitudinal study (Stutzman et al., 2012), which was conducted over the course of six years, has shown that users are concerned less about privacy and disclosed more of their information.

Instagram is a photo and video sharing social networking site which was founded in 2010. As of 2018, it has 1 billion active users which makes it the second most popular social networking

site (Statista, 2018(b)). Given that Instagram is a fairly new social networking site, not much research has been conducted on data disclosure. To the best of my knowledge, only two studies have been conducted so far. The first study (Al-Kandari, Melkote and Sharif, 2016) researched the predictors of self-disclosure on Instagram on a case study of young adults in Kuwait. The second study (Shane-Simpson, Gaggi, and Gillespie-Lynch, 2018) compared Facebook, Instagram, and Twitter in regard to preferences, privacy concerns and attention seeking, trust in different social networking sites and the affordances on each site. The results indicate that users disclose more on Instagram than Facebook, while they trust Facebook's brand more and have fewer privacy concerns for it than for Instagram. Even though Facebook owns Instagram, the privacy concerns between them vary.

LinkedIn is a professional social networking site which focuses on business and employment services. While there are only a few studies regarding privacy concerns and risks on LinkedIn (Chang, Liu, and Shen, 2017), to the best of my knowledge, no studies have been conducted about data disclosure on the site. Given that Facebook is the most used social networking site, it has also been the subject of most applicable research.

The literature review shows that there is a need to research the role that informed data disclosure on Facebook, Instagram and LinkedIn has in generating brand trust towards these sites. To answer the gap, this thesis will firstly examine the existing literature on informed data disclosure on social networking sites, aware data disclosure and trust in social networking sites. Secondly, an empirical qualitative research on how these concepts are related will be executed.

2 DATA DISCLOSURE ON SOCIAL NETWORKING SITES

2.1 SELF-DISCLOSURE ON SOCIAL NETWORKING SITES

The concept of self-disclosure comes from various fields of psychology and sociology. It is broadly defined as "any information about the self that is intentionally or unintentionally communicated to another person through verbal or nonverbal messages" (McCroskey and Richmond, 1977, p. 40). To narrow the scope, in a social networking site setting self-disclosure is defined as "the act of disclosing individuals' factual information voluntarily and intentionally, consisting of regional orientations, thoughts, as well as photographs via web-based social networks" (Pang, 2018, p. 2234). Social networking sites are designed to elicit self-disclosure as it is necessary to provide personal data to even register (Boyd and Ellison, 2008).

From the perspective of information technology social networking sites are defined as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" (Boyd and Ellison, 2008). This particular definition is of relevance for this thesis, as it supports the assumption that sharing data is a requirement for membership on social networking sites. The cornerstone of all social networking sites is the profiles that users need to create to join them. To create a profile, users are asked to disclose certain personal data. The data is visible to either their contacts on the social network or to the general public, depending on their privacy settings, whereas the type of data shared is determined by the possibilities a social networking site offers.

Furthermore, as the name itself suggests, the purpose of social networking sites is to network and interact with other people. Users are prompted to connect with other users and publicly display connections and some communications, even though most social networking sites also have private messaging options. Thereby users, in various ways, disclose personal information. Social networking sites function on the premise that by disclosing information on them, users can expect reciprocity. The reasons for social networking site usage are varied, but several have a great impact on a users' decisions to continue social networking site usage. Debatin, Lovejoy, Horn, and Hughes (2009) have found that there are three main reasons for social networking sites usage and disclosure of personal data: "(1) the need for diversion and entertainment, (2) the need for (para-social) relationships, and (3) the need for identity

construction". The authors state that if a social networking site fulfils these needs, a user will continue to disclose personal information, regardless of the possible privacy risks.

2.2 PERCIEVED RISKS OF DATA DISCLOSURE ON SOCIAL NETWORKING SITES

Given that social networking site users disclose substantial amounts of personal information on their social networking site profiles, they expose themselves to a number of risks. De Moor et al. (2008) made a comprehensive list of possible risks for Internet usage, however it can be easily translated to risks related to social networking site usage. The authors divided them into three categories: content, contact and commercial risks (De Moor et al., 2008):

- The content category of risks refers to inappropriate content which users of social networking sites may be exposed to.
- Contact risks are related to the fact that users of social networking sites can be contacted through the information they provide on their profiles or through the social networking sites themselves.
- The last category refers to the commercial risks. These refer to the misuse of information by third parties through applications or for advertisement purposes.

The data that users provide on their social networking sites can be tracked and shared with third parties (Debatin et al., 2009).

Bechmann's (2014) study has reiterated what many studies have concluded so far – users are not aware of the possible risks related to social networking site usage, especially relating to the commercial risks of a social networking site. Users are more worried that the shared information will reach their social circle, than that it will be used for other purposes by third parties (Bechmann, 2014, Joergenses, 2014). The findings of these studies point that users are blissfully unaware of the possible repercussions. For instance, by consenting to share data with applications on Facebook, users unknowingly grant access to their profile, list of friends, email address and in some cases even to their inbox messages, newsfeed interactions and 'secret' groups. Mayer-Schönberger and Cukier (2013) further argue that when users were giving their consent for data collection, they were not aware of how it will be used. We have moved into a big-data age and the data is now used more for secondary purposes, rather than its primary uses.

This brings us to the question: how can users knowingly consent to data collection and usage when, at the time of their consent, this type of data usage did not even exist? Without the users of social networking sites being informed about every aspect of why their data is collected and how it will be further used, there can be no informed consent.

2.3 PRIVACY CONCERNS

Through social networking sites people disclose their personal information on their social network profiles thereby divulging the information to an essentially unlimited audience (Heravi, Mani, Choo, and Mubarak, 2017, p. 1922). Therefore, a concern for privacy is a crucial problem related to data disclosure on social networking sites.

Various definitions of privacy have been offered in literature with no consensus over one. Privacy can be divided into three categories: (1) territorial privacy, (2) privacy of a person and (3) information privacy (Kokolakis, 2017, p. 123). As territorial privacy is related to the area in physical proximity of a person and privacy of a person refers to protecting a person from an intrusion (Kokolakis, 2017, p. 123). While territorial privacy and privacy of a person both refer to the privacy in a physical sense, information privacy is concerned with the usage of personal data. For the purposes of understanding the informed data disclosure on social networking sites, it is sensible to put focus on information privacy. Information privacy is a segment of the more general concept of privacy and it consists of personal communication privacy and data privacy (Bélanger and Crossler, 2011, p. 1018). To understand privacy concerns in an online setting, information privacy is most commonly used as it is related to the personal data users disclose about themselves and their right to have control over the mentioned data. Clarke (1988, p. 500) defined it as "the interest an individual has in controlling or at least significantly influencing, the handling of data about themselves". When users use the Internet and join social networking sites, they are giving a part of their privacy away by disclosing their information online which raises concerns about how their data is handled.

Privacy concerns regarding data disclosure are growing more and more due to the extent of the digitalisation (McParland and Connolly, 2007). The concern for data disclosure stems from users' perception of possible risks of data disclosure on social networking sites. Concern for

information privacy can be divided into three categories including (1) collection of data, (2) control and (3) awareness (Malhotra, Kim and Agarwal, 2004, p. 338):

- The collection of data refers to the concerns about data collection by social networking sites as well as the benefits users have from disclosing their personal information.
- The control is the right of users to have control over their information on social networking sites, such as the possibility to change their privacy settings or consent to their data being shared with third parties.
- Awareness is seen as a passive counterpart of control. It refers to the how well users are informed about and aware of how social networking sites handle the data disclosed.

2.4 THE ROLE OF PRIVACY CONCERNS IN DATA DISCLOSURE

Privacy concerns stem from the possible risks that can occur when users disclose data on social networking sites (Mubarak and Choo, 2016). There have been numerous studies which have analysed the relationship between privacy concerns and privacy behaviour. Literature shows that there are inconsistent results in regard to how privacy concern influences the disclosure of data on social networking sites.

The earlier studies conducted on information privacy concerns on social networking sites indicated that users were not particularly troubled by possible privacy risks (Acquisti and Gross, 2005; Gross and Acquisti, 2006). Users' reactions to these concerns differ and even though people express concern, there have been discrepancies between these concerns and the actual amount of personal information disclosed online (Acquisti and Gross, 2005; Gross and Acquisti, 2006). This phenomenon is called the privacy paradox – despite users reporting high levels of concerns for their privacy, they still disclose substantial amounts of their information online (Kokolakis, 2017, p. 122). This phenomenon presumes that people tend to make irrational decisions. Even though users express concerns, they also often do not take measures to protect their privacy, for instance, by deleting cookies or changing their privacy settings on social networking sites. Studies conducted by Acquisti and Gross (2005; 2006) about privacy attitudes and subsequent behaviour on social networking sites produced similar results which supported the existence of the privacy paradox. However, there have been studies which aimed to explain how the privacy paradox occurred as people are not irrational beings. For instance, Acquisti and Gross (2005) have linked it to lack of information, bounded rationality and

psychological deviations. Recently Barth and de Jong (2017) conducted a systematic literature review examining the privacy paradox and stated that it can be explained by two factors, either biased risk assessment when appraising risks and benefits or little to no risk assessment. Biased risk assessment refers to the biases which influence the decision-making process such as bounded rationality, "time constraints, time inconsistency, immediate gratification and optimistic bias" (Barth and de Jong, 2017, p. 1045). Little to no risk assessment refers to users not being aware of the risks and therefore basing their decision-making process on the benefits alone (Barth and de Jong, 2017, p. 1048).

On the other hand, the more recent studies have demonstrated that there has been a surge in privacy concerns as users understand the possible privacy-related risks more (Debatin et al., 2009; Heravi, Mubarak and Choo, 2016; Heravi et al., 2017). Unlike the privacy paradox phenomenon, the privacy calculus theory (Laufer and Wolfe, 1977) posits that users decide whether they will share their personal information by assessing the perceived risks and anticipated benefits of information disclosure. The privacy calculus theory is viewed as a theory which helps to explain the rational processes of users when faced with risks and benefits of using social networking sites. It stems from economy and the notion that users rationalise and calculate when making decisions, meaning that users will be willing to disclose data if they have concluded that the positive outcomes will be greater than the negative ones. As users cannot predict the outcomes with complete certainty, they rely on their previous experiences, experiences from others and risk perception (Debatin et al., 2009).

Apart from contrast between the privacy paradox and privacy calculus, there is also an inconsistency in the perceived and actual disclosure of information. Most studies conducted so far have concentrated on the attitude towards or the intention to disclose information on social networking sites without measuring the actual data disclosed (Debatin et al., 2009; Heravi, Mubarak and Choo, 2016; Heravi et al., 2017). Perceived data disclosure is the amount of data users think they share on social networking sites, whereas actual data disclosure is the amount of data users do de facto disclose (Acquisti and Gross, 2006). Thus far only two studies have examined if a difference between the perceived amount of data disclosed and the actual data disclosed on social networking sites exists. The first study conducted by Acquisti and Gross (2006) examined the data of 209 people on Facebook and compared them to what the participants answered on a survey about data disclosure on the site. Most participants (77 %)

were sharing the same amount of information that they stated in the questionnaire. However, a small percentage (8 %) shared more and some disclosed less than they previously claimed in the questionnaire (11 %). The second study (Madejski, Johnson and Bellovin, 2012) had 65 participants and it compared the intentions to disclose to the privacy settings users have on their Facebook profiles. Most users had at least one sharing violation either sharing what they did not want to (94 %) or some data was hidden, even though they wanted it to be shown (85 %). The authors of both studies concluded that the significant dichotomy between the reported and actual data is due to the users' not knowing how the privacy settings of Facebook function and how Facebook treats their data which further indicates that of disclosing data to social networking sites is problematic due to the users not informedly disclosing their data to social networking sites.

3 AWARE DATA DISCLOSURE

From the moment we wake up we are faced with many decisions – from trivial choices such as what to wear to those with wider implications. There are three main decision-making approaches: cognitive, habitual and affective (Solomon, 2010). Cognitive decision-making is deliberate and rational. Habitual decision making is automatic and unconscious, whereas affective is emotional and immediate. To simplify, we can divide them into rational (cognitive) and irrational (habitual and affective) (Solomon, 2010). Rational decision-making is based on more precise processing of information. This approach proposes that humans are rational beings which try to gather as much information about a given problem as possible, compare all the alternatives and finally, come to a decision (Barry, 1987, p. 268). It consists of five steps: (1) problem recognition, (2) information search, (3) evaluation of alternatives, (4) choice and (5) post-hoc evaluation (Kotler and Keller, 2003). On the other hand, the irrational decision-making are choices people make without having to try much or by simply reacting affectively (Solomon, 2010).

To rationally resolve a problem, one has to first recognise that it is there and be aware of the problem (Kotler and Keller, 2003). If sharing personal data on social networking sites is not perceived as a problem, users may resort to consenting to privacy policies and terms of service even though they are not fully aware of what these entail. For instance, a study has shown that when joining a social networking site 73 % of users do not read privacy policies and terms of service by which they agreed to provide their first-born child as payment for using the social networking site (Obar and Oeldorf-Hirsch, 2018). This points to the issue of privacy awareness. As Malhotra et al. (2004) have suggested, one of the components of information privacy is awareness, in other words the degree to which users of social networking sites are aware of and informed about how their data is handled.

Privacy awareness is "the attention, perception and cognition of: (1) whether others receive or have received personal information about him/her, his/her presence and activities, (2) which personal information others receive or have received in detail, (3) how these pieces of information are or may be processed and used, and (4) what amount of information about the presence and activities of others might reach and/or interrupt the individual" (Pöttsch, 2008, p.

228). It is a prerequisite for users of social networking sites to make informed decisions on data disclosure. One could argue that by becoming a member of a social networking sites you are aware of that fact and you understand the privacy risks regarding your data, however, it is not entirely clear how consent actually works in a given situation. Studies have shown (Acquisti and Gross, 2005; Acquisti and Gross, 2006; Nyoni and Velempini, 2018) that users are mostly unaware of the possible risks regarding data disclosure on social networking sites. Moreover, the studies (Acquisti and Gross, 2006; Madejski, Johnson and Bellovin, 2012) conducted on the dichotomy between the perceived and actual data disclosed on social networking sites have shown that users do not understand how their data is handled.

Research on the consequences of privacy awareness is scarce. However, studies have proven (e.g. Nehf, 2005; Park, Campbell, & Kwak, 2012) that users are more prone to privacy protection behaviours both on a technical and social level, if they are well informed and aware of the possible privacy risks. Tow, Dell, and Venable (2010) state that users changed their behaviour when they were informed about the possibility of identity theft. When users perceive that there are possible privacy risks, they react not only cognitively, but also emotionally (Choi, Jiang, and Yap, 2012). A study was conducted on whether "improved user understanding of the potential inferences that can be made from information shared on SNSs influences privacy awareness and attitudes toward further disclosure" (Padyab, Päivärinta, Ståhlbröst, and Bergvall-Kåreborn, 2019). The results showed that privacy awareness is context-dependent and that users of social networking sites require more cognitive awareness. As the participants were shown the possible interferences, most of their attitudes towards privacy changed from affective to cognitive. The results of the study conducted by Padyab and colleagues (2019) demonstrated that social networking site users cannot be expected to make rational decisions, if they are not aware of the problems at hand. The research mentioned above indicates that there is a need for simplifying privacy policies and educating users of social networking sites about possible risks and way in which privacy settings function.

4 TRUST IN SOCIAL NETWORKING SITES

4.1 DEFINING TRUST IN SOCIAL NETWORKING SITES

Every interaction carries a degree of risk with it as the involved parties cannot be sure about the other party's behaviour. An important factor in every interaction is trust which is defined as "a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviours of another" (Rousseau, Sitkin, Burt and Camerer, 1998, p. 395). It is pertinent for maintaining and building relationships, not solely between people, but also between business entities and consumers. Having a strong brand is a pivotal factor which influences how customers behave and what they associate with the company, as well as being an important differentiation mechanism. By being familiar with a certain brand, consumers can anticipate the quality and the overall experience they will receive (Morgan and Hunt, 1994). Furthermore, when customers receive value from a brand, it helps build a relationship between the brand and the customer, which subsequently leads to greater brand trust and loyalty (Kay, 2006). As such, brand trust is defined as "the willingness of the average consumer to rely on the ability of the brand to perform its stated function" (Chaudhuri and Holbrook, 2001, p. 82). Ring (1996) divided brand trust into rational and emotional trust. Emotional trust stems from personal experience with the brand and emotional involvement, whereas rational trust is based on rational decisions made by consumers when evaluating possible risks of interacting with a brand and the objective information gathered (Ring, 1996). Trust in a brand guides the consumers' intentions and the outcomes of their behaviour. For instance, brand trust influences satisfaction with the brand and long-term relationship maintenance (Morgan and Hunt, 1994), reduces uncertainty about the brand and vulnerability, as well as the intention to interact with the brand again (Chaudhuri and Holbrook, 2001).

Literature reviews show that consumers' trust in a brand arises with the help of various factors which differ from industries, however, for marketing, crucial dimensions impacting the level of trust are the integrity and reliability of the business (Morgan and Hunt, 1994). Given that privacy is the one of the most relevant concerns for users online (McParland and Connolly, 2007), trust towards a social networking site plays an important role in how they use the social networking site (Martin, 2018). As interpersonal trust is generally defined as "an expectancy held by an individual or a group that the word or promise of another individual or group can be relied upon" (Rotter, 1971), in the context of social networking sites we can define trust as the expectancy of users to rely upon the social

networking site to treat the user's data fairly. Sustaining trust online is based on not breaching the privacy of consumers by misusing or sharing their information.

4.2 THE ROLE OF TRUST IN SNS

Literature reviews have shown that trust in a social networking site is an essential predictor of behaviour on the site, as well as if the site will be used at all. Previous studies have confirmed that trust in a social networking site plays an important role in continuance of usage and it reduces consumers' perception of risk (Metzger, 2004; Hoffman et al., 1999). Moreover, it increases the probability that users will disclose personal information and recommend the social networking site to other people, as does it increase loyalty to the site (Hoffman, Novak, Perlata, 1999). Taddei and Contena (2013) argue that when users of social networking sites have trust in the site, they automatically have lower privacy concerns which also impacts the amount of data disclosure. It is important to note that most of the previous studies put their focus on studying the role of trust in disclosing data on social networking sites. However, it is of vital importance to understand the role of trust as a consequence of decision-making processes and aware data disclosure.

Trust is a critical prerequisite for online commerce, as one cannot determine the counterpart's intents as easily as in face-to-face communication. Research (Culnan and Armstrong, 1999; Hoffman, Novak, Perlata, 1999) suggests that users do not provide data online mostly because they do not have enough trust, as it is a crucial factor in assessing the possible risks and benefits. If users were to have enough trust in a brand, such assessments would not be necessary.

Kim, Ferrin and Rao (2008) have suggested users have to be adequately informed to trust and subsequently also disclose personal information on social networking services. Similarly, Bleier and Eisenbeiss (2015) have also emphasised the importance of trust in online retail and ad personalization, as well as the significance of overt data collection for building brand trust indicating that it is crucial that users are informed about how and what their data is used for to gain their trust. Privacy awareness is one of the components of information privacy which refers to how well the users of social networking sites are informed about how their data is being

handled (Malhotra, Kim and Agarwal, 2004, p. 338). To reiterate, it is crucial that users are aware of what their data is used for, if not for ethical, then for the purpose of retaining business.

A user-oriented information privacy model from social networking sites can only lead to a more profitable relationship for both counterparts (Han and Maclaurin, 2002). By giving users control over their information and the knowledge of how that information is collected and used will lead to less privacy concerns and more trust from the users, which will consequently make them disclose more data and continue to use the social networking site (Grace and SurrIDGE, 2017). In an environment that is increasingly competitive, businesses have to strive to retain customers by gaining their trust. With the recent developments regarding the new laws in the European Union which were prompted by several big data breaches in the last decade, it is becoming clearer that laws are not the only practices that need to change (Gleibs, 2014). Therefore, social networking sites have to change their approach to information privacy of their users' and make their policies and intentions more transparent.

4.3 ANTECEDENTS OF TRUST IN SOCIAL NETWORKING SITES

Grabner-Krauter and Bitter (2015) state that the development of trust in social networking sites is a dynamic concept which can be divided into three stages. The first stage is when users become members of a social networking site, the second is when the trust starts to stabilise, as they continually use the site and the last stage when users start losing trust in the social networking site. In the first stage, users use cognitive or observation-based cues. Cognitive cues relate to how users perceive the brand by calculating risks versus the benefits (Grabner-Krauter and Bitter, 2015). Users also appraise the social networking site size, ease of use and usefulness of the site and topics on the site (Kim, Ferrin and Rao, 2008). Other cognitive cues are perceived privacy and security, perceived risks and privacy concerns (McKnight, Cummings and Chervany, 1998; Kim, Ferrin and Rao, 2008). After a period of using the site, users have more knowledge and experience about the social networking sites, as well as more interactions with other users of the site upon which they have built trust. Literature shows that in the second stage the factors influencing trust towards social networking sites can be affect- and experience-based (Lewicki and Bunker, 1995; Kim, Ferrin and Rao, 2008). One other group of factors that influence higher trust are personality-oriented trust antecedents which refer to the personality characteristics and habits of users (Grabner-Krauter and Bitter, 2015). For example, certain

personality characteristics can make users identify with the social networking sites and identification with a social networking site has been shown to result in higher trust of users towards it (Grabner-Krauter and Bitter, 2015).

For the purpose of understanding to what extent informed data disclosure influences brand trust in social networking sites, the cognition-based antecedents of trust should be emphasised. To reiterate, privacy awareness is users knowing and understanding what their data is used for. Therefore, cognitive cues, such as perceived risks, security and concerns, are an indicator of privacy awareness. Gleibs (2014) has discussed the ethical side of informing users about how their data is used. For instance, Facebook collected and mined users' data under the pretence of research, only for it to be breached. Even though users have consented to their data being used for 'research purposes', many of them were completely unaware of that fact which lead them to feel betrayed and to significantly lose trust in Facebook as a brand. For users to trust a brand it is pertinent that they have high quality information which helps them make rational decisions as to whether and how they will interact with a brand (Miranda and Saunders, 2003). Also, making the privacy settings of social networking sites more user-centric will ultimately lead to more trustworthiness for the site (Han and Maclaurin, 2002). It is the ethical duty of every social networking site to be transparent about how they will treat their user's data and inform them clearly about it.

5 THEORETICAL FRAMEWORK SUM-UP AND THE DEFINITION OF THE RESEARCH PROBLEM

The theoretical review has shown that data disclosure on social networking sites is one of the key problems on these sites, as users are mostly unaware of the possible risks. With social networking sites integrating into the everyday lives of many people, it is important to ensure that users are educated. This is significant, not only for the users, but for the social networking sites as well. Some previous studies indicate that as users become more informed and gain more control over their data, their privacy concerns reduce and trust in the social networking sites increases (Grace and Surridge, 2017; Miranda and Saunders, 2003). These concepts have been researched in numerous studies, but to the best of my knowledge, there has been no study that used Facebook, Instagram and LinkedIn with the purpose of examining the role that informed data disclosure has in the degree of trust towards a social networking site. Therefore, the objective of this research was to answer the following main research question: **what role does informed data disclosure have in trust towards a social networking site.**

Disclosing data when using social networking sites is an imperative (Boyd and Ellison, 2008). By divulging personal data, users expose themselves to a number of risks (DeMoor et al., 2008). Research has shown that users are mostly oblivious to the risks of social networking site usage (Acquisti and Gross, 2005; Acquisti and Gross, 2006; Bechmann, 2014; Joergenses, 2014; Mayer-Schönberger and Cukier, 2013; Nyoni and Velepini, 2018). However, they still express a great deal of privacy concerns (McParland and Connolly, 2007). This gap in knowledge and awareness of the possible risks leads to users behaving paradoxically, i.e. expressing privacy concerns while at the same time not taking measures to protect their privacy (Barth and de Jong, 2017). Research has shown that if users are more aware of the possible risks, they also engage in privacy protective behaviour (Nehf, 2005; Park, Campbell, & Kwak, 2012; Tow, Dell, and Venable, 2010). However, a critical literature review has shown that there was a lack of insights on whether aware data disclosure is even important for social networking site users and to what extent is it relevant for the usage of different social networking sites. To address this gap, this study will put its focus on researching whether and to what extent do users find it important to be aware of possible risks when disclosing their data on various social networking sites, namely Facebook, Instagram and LinkedIn. Given that the literature review has shown that people mostly do not know enough to make an informed decision (Acquisti and Gross, 2005; Acquisti and Gross, 2006; Bechmann, 2014; Joergenses, 2014; Mayer-

Schönberger and Cukier, 2013; Nyoni and Velempini, 2018), we want to address the following research question:

RQ1: How much importance do users of a social networking sites give to being aware of the possible risks when disclosing data on that social networking site?

Another objective is to explore the role of trust in users' future behaviour towards various social networking sites, such as their intention to continue using the social networking site. Previous research (Debatin, Lovejoy and Hughes, 2009) has shown that the satisfaction users get from social networking sites usually overrides the perceived risks and concerns. Debatin, Lovejoy and Hughes (2009) have argued that users of social networking sites will continue using them if they fulfil their needs, even though they could be exposing themselves to a number of risks. Deriving from the findings we additionally address the following question:

RQ2: Will users of social networking sites continue to use the social networking site, regardless of the privacy risks and concerns?

In the case that users are aware of the privacy risks regarding the sharing of their data on social networking sites, the key objective of our research is to analyse the degree of trust they have in the social networking site. Research has determined that trusting a social networking site is crucial for their continuance of usage of the site and reducing risks perceptions (Hoffman et al., 1999; Martin, 2018; Metzger, 2004). Most of the research so far has examined how trusting a social networking site impacts data disclosure perception (Hoffman et al., 1999; Metzger, 2004; Taddei and Contena, 2013). However, there is a gap in research which would explain whether being informed and aware of the possible privacy risks related to data disclosure influences the degree of trust towards a social networking site. This research would try to close the gap by examining the role of privacy aware data disclosure in trust towards social networking sites. Thus, we propose the following research question:

Q3: Will users of social networking sites express higher trust toward this social networking site when they are informed about the possible privacy risks when disclosing their data on that site (and therefore aware about them)?

In my thesis, I will concentrate on exploring how well consumers are informed about data disclosure on Facebook, Instagram and LinkedIn, how privacy concerns influence their behaviour on social networking sites, and what role aware disclosure of their data plays in their trust towards these social networking sites. Furthermore, a comparison between the attitudes towards three social networking sites, Facebook, Instagram and LinkedIn, will be examined. Facebook, Instagram and LinkedIn were chosen as they are the sites with the most users, apart from Twitter. Users of social networking sites can hardly be expected to be completely aware of all the privacy implications of social networking site usage because of lack of knowledge and the fast advancement of technology. Even though transparency about data collection and usage is the ethical duty of every social networking site, it is important to determine if it is a factor in their business retention. By understanding the role that privacy aware data disclosure has in trust towards social networking sites, benefits for both the users and the companies can be derived, i.e. with the help of this research, privacy policies, terms of usage and legislation can be improved.

6 EMPIRICAL RESEARCH

6.1 METHODOLOGY

Qualitative methodology was used to research the relevance of privacy aware data disclosure for the users of various SNS and the role of aware data disclosure in trust towards social networking sites. A semi-structured interview was used as a research technique. Interview contained four sets or themes of questions that focused on researching the following: the context of social networking site usage, the importance of privacy awareness, the relevance of trust towards social networking sites and respondents' attitudes towards their intention of usage continuance of Facebook, Instagram and LinkedIn. Semi-structured interviews were chosen as a research method as this technique allowed the interviewer to explore the problem in-depth. Moreover, given that most of the previous research on the topic focused mainly on quantitative approaches, more in-depth research is necessary.

The questions were open-ended with the aim of making the interviews more informal and conversational. This allows for more individualised answers and the possibility of sub-questions. Furthermore, several projection techniques were used, as these make it easier for people to express their beliefs and motivations. In some cases, respondents are not able or not willing to give an answer to a direct question, and projection techniques aid the respondents in projecting their attitudes on a different subject thereby possibly revealing more about their actual beliefs and attitudes (Solomon, 2010).

The interviews were conducted between the 28th of August and 19th of September 2019 on different locations. Six interviews were conducted in total: four in person and two over the telephone. The interviews lasted between 15 and 30 minutes on average. The interviews were recorded with a phone and later transcribed. Several criteria were taken into account: age, gender, nationality, social media usage and the awareness of the respondents. All of the interviewees are in their twenties and there is an equal amount of gender representation; three males and three females. To ensure cultural similarity, all of the respondents are citizens of one of the European Union countries. All the respondents have profiles on Facebook, Instagram and LinkedIn. Furthermore, all interviewees use some, if not all, of the social networking sites for business purposes and are therefore more knowledgeable about privacy and data disclosure than

most. None of the respondents had problems with revealing their true names which indicates truthfulness that could impact research findings. However, their names were anonymised.

Table 6.1 Demographic summary of interviewees

Name	Age	Gender	Nationality
Leo	27	M	Belgian
Lisa	26	F	German
Dominic	27	M	German
Mila	27	F	Croatian
Ana	29	F	Croatian
Yusuf	26	M	Belgian

6.3 ANALYSIS OF INTERVIEWS

Most of the respondents use Facebook to connect with other users or informing themselves about various topics. For Instagram the answers varied more compared to Facebook. Whilst some use it solely for professional purposes, others use it to share their experiences or see what other people are doing. For LinkedIn all of the interviewees responded they use it for business purposes such as finding a job or connecting with existing or potential employers and colleagues. The frequency of use varies among respondents and social networking sites. Most respondents use Facebook and Instagram daily, whereas LinkedIn is used more sporadically.

To get an insight into information people usually disclose on each of the social networking sites, a projection technique was used. The respondents were asked what they think other people usually disclose on each of the social networking sites. This helped the respondents to project the behaviour on other people which resulted in different answers than when they were asked to share what they themselves used the social networking sites, as people tend to see themselves and their actions differently than that of most other people. Interview analysis showed that most of the interviewees thought that people usually disclose basic information on Facebook, such as posting statuses, photos, where people are and what they are doing. Some state that they

think a lot of personal data is disclosed by people on Facebook and even expressed concern about what types of information people are willing to share.

“But there are some things that, you know, people share photos of their very, very young children, um.... And they don’t really understand there are many precarious groups on Facebook that could abuse that data.” (Ana, personal interview, September 2019)¹

Instagram is perceived differently by the respondents, as the type of data posted is mostly disclosed in a different, more visual form. However, some of the interviewees still believe that other people disclose too much personal data on the social networking site. For LinkedIn the respondents specified that it was a different type of data that people usually disclose which is mostly related to business and work purposes, not so as much personal data which is the reason why most did not see it as problematic. To compare the ideas the interviewees have about themselves and other people, the respondents were asked how much they themselves disclose on each of the social networking sites. Most claim they do not share anything on Facebook, however, just by having a profile and using the social networking site they do, though unconsciously, disclose personal data. The respondents did not seem to understand the difference between sharing a post or disclosing data. This indicates that respondents were not aware that they disclose data simply by using a social networking site and that they therefore disclose more than they actually believe. Instagram is used occasionally to share pictures and videos of the places they visit or to promote their business. LinkedIn is viewed as an entirely different platform than Facebook and Instagram, as respondents usually do not post on the social networking site, they rather only disclose work-related data, i.e. data that they would like to be public. While this type of data is still personal, respondents do not view it as such.

To get more of an understanding about how respondents feel about privacy policies of social networking sites in general, another projection technique was used. Word association is a method used to get insight into the immediate reaction a person has about the subject at hand (Abir, 2010). The respondents had to quickly respond with the first thing that comes to mind when privacy policies of social networking sites are mentioned. All of the connotations were negative, and everyone mentioned that no one reads them. Therefore, another projection

¹ The transcript of the interview can be found in Appendix E

technique was used to determine the respondents' feelings and attitudes towards privacy policies. The respondents were asked to describe a person which would read a privacy policy. The answers were negative and similar, describing the person as anxious or paranoid. Given that no one has read the privacy policies and described the person that would in a negative way, a follow up question regarding their concern with the privacy of their data on social networking sites was asked. Some were not worried, but even saw it a positive way, as it allows for the advertisements shown on the social networking sites to be more tailored to them. However, some of the respondents have shown that they were not aware of the potential risks of data disclosure on social networking sites:

“What can happen? It would concern me if my banking data would be leaked or something because then I can lose something, but what can I lose if my data goes out? I don't have a problem with people knowing what kind of sites I like, what my age is or... Like, what can happen?” (Dominic, personal interview, September 2019)²

Some others did express privacy concerns, but they have a feeling of not being able to influence or control it. Even though, the respondents never actively searched for alternatives for any of these sites since 'everyone' is using them and it defeats the purpose to use others which only contributes to the feelings on resignation. To assess how informed the interviewees are about data protection, they were asked if there were any other ways that they inform themselves about data disclosure on social networking sites and most did not, with some expressing feelings of resignation yet again. The respondents mostly don't feel that their data is protected by Facebook or Instagram, as they stated they were aware of the recent data breach scandals revolving around it. However, most said the scandals did not change their behaviour on the social networking sites. LinkedIn is again viewed differently because of the different type of data disclosed and the different way of interacting with the social networking sites. The respondents do not see LinkedIn as a personal social networking site, but as a more professional one and therefore disclose only the data that they would in a very formal setting. Consequently, they do not believe that the possible privacy risks of using LinkedIn are as severe as with Facebook or Instagram.

The next set of questions was a projection technique in which the interviewer pretended to be a new user of each of these sites and asked for advice from the respondents. By using the role-

² The transcript of the interview can be found in Appendix C

playing projection technique, the elicited answers helped to uncover real and deep-seated feelings and opinions, rather than asking directly. For Facebook there was a general feeling of distrust from all of the respondents with some saying that everything is in the privacy policies and terms of agreement which you agree to and some even claiming that Facebook would even lie about certain policies and share your data with third parties without your consent. For Instagram everyone answered the same stating it's the same company and there are no differences in their policies. For LinkedIn most of the respondents said that they actually don't know, but assume that, since it is a social networking site like Facebook and Instagram, that it ultimately operates in the same way. The respondents show a high degree of distrust towards the social networking sites because they are aware that their data is being mined and used. When asked whether trusting a social networking site impacts how much data they disclose, the answers varied. Some said that they definitely post less because they are more aware of the possible risks and implications of data disclosure on social networking sites. At one point in the interview the respondents expressed that they did not trust Facebook and Instagram because of the data breaches, while still stating later on that it did not change their behaviour or overly concern them. This points to a cognitive dissonance with the respondents, as they express contradictory opinions and feelings.

“No, I don't trust any of them because they make money of our data. That's like their main income to advertise and maybe even sell the data, I don't know. Probably happened.” (Yusuf, personal interview, September 2019)³

When asked whether they have ever thought of stopping using social networking sites themselves and what would motivate them to stop, three of the respondents could not think of a reason they would stop using social networking sites. Three have already thought of stopping, but they cannot because it is strongly linked to their work or business. The respondents also expressed the feelings of having no control and being pressured into using the social networking sites simply because everyone else does.

“I find that using something that I feel like I have no control over in a way is, you know, annoying and I don't like the feeling that I'm pressured into doing something, which we all are.” (Ana, personal interview, September 2019)⁴

³ The transcript of the interview can be found in Appendix F

⁴ The transcript of the interview can be found in Appendix E

6.4 DISCUSSION

As the theoretical review, the research has shown that users are mostly unaware of the possible risks of data disclosure on social networking sites. The goal of this research was to answer what role informed data disclosure has in trust towards a social networking site. As Boyd and Ellison (2008) have stated and the answers of the respondents in our research confirm, social networking sites operate in a way which makes it necessary to disclose data to register and use them. Debatin, Lovejoy and Hughes (2009) state users continue using social networking sites and disregard the possible privacy risks if the site fulfils their needs, such as the need for relationship, entertainment or identity construction. All the interviewees mentioned at least one of these needs being fulfilled by Facebook, Instagram and LinkedIn. Moreover, they showed the intention to continue usage, regardless of the privacy risks.

As Obar and Oeldorf-Hirsch (2018) have proven in their study, the majority of people do not read privacy policies. All the respondents in this study have also admitted to never having read one. Some have even expressed that the privacy policy is there to protect the company, rather than the user. Users of social networking sites are consenting to privacy policies without reading them and without being aware how they disclose data and what it is used for. Not understanding and reading privacy policies translates into them not being aware of the possible risks. However, most the respondents that were aware of the possible risks, despite not having read the privacy policies, still did not change their behaviour. The privacy paradox has been mentioned in several studies (Barth and DeJong, 2017; Kokolakis, 2017) and proven yet again since even though the respondents stated that they were concerned about their data on social networking sites, they continued using and disclosing data on the sites. This dissonance can be explained by the needs the social networking sites fulfil and that not using social networking sites nowadays, especially considering the age of the participants, is extremely difficult. The contrasting theory of privacy calculus states that users of social networking sites calculate the risks and the benefits of usage to decide how much data they will disclose (Laufer and Wolfe, 1977). Elements of this theory have also proven to be correct by this research. Based on the knowledge that the respondents had they have decided that the possible benefits, such as socialising or promoting their business, outweigh the possible risks. However, it has to be noted that the participants were mostly not taking direct action to inform themselves and are bounded rationally. Several respondents mentioned that they have started to disclose less on the social networking sites as they grew older. Jia et al. (2015) have proven that teenagers tend to function under bounded rationality

and lower risk assessment and therefore it is harder for them to make rational decisions related to privacy. With this we can conclude that users of social networking sites often do not give importance to being aware of the possible risks of disclosing data on that social networking site.

In the case that users are aware of the privacy risks regarding the sharing of their data on social networking sites, the key objective of our research is to analyse the degree of trust they have in the social networking site. Research has determined that trusting a social networking site is crucial for their continuance of usage of the site and reducing risks perceptions (Hoffman et al., 1999; Martin, 2018; Metzger, 2004).

One of the aims of this research was to examine the role that privacy aware data disclosure has in trust towards social networking sites. The findings show that the more users are aware of the possible risks of using social networking sites, the less they trust and share on the sites. The trust that users have in social networking sites decreases, as they become more informed and aware. Several studies (Hoffman et al., 1999; Martin, 2018; Metzger, 2004) have confirmed that trusting a social networking site is a prerequisite to continue to use the site. However, most of the research has concentrated on explaining how trust influences data disclosure. The literature review has pointed in the direction that users will trust a social networking site more if they were more informed about the possible risks of using it. However, the results of this study have contradict this proposition. As Miranda and Saunders (2003) have stated, social networking sites are trusted more if they are transparent to their users about the collection and usage of their data. Therefore, we could conclude that users of social networking sites would trust the sites more if they were educated by the sites themselves.

Most of the respondents exhibit a great deal of distrust towards Facebook and Instagram and less so towards LinkedIn. This may be because the nature of data disclosed on LinkedIn is not perceived to be as personal as the one disclosed on Facebook and Instagram, or that the participants do not view LinkedIn as a typical social networking site. Given that LinkedIn is a social networking site used for business purposes, the data that people disclose on the site is the type of data they would like their potential employer to see, so they perceive it as not as risky. However, a lot of the respondents simply do not know that the data disclosed is as personal as

with Facebook and Instagram and use LinkedIn as much as Facebook and Instagram. Therefore, it could be argued that the respondents are bounded rationally as they cannot assess the risks due to incomplete information (Barth and de Jong, 2017).

As it has been mentioned, this research aimed to close the gap which would explain what role being informed and aware about data disclosure risks plays in trusting a social networking site. We can conclude that trust plays an important role in how much users are willing to share, however, that does not necessarily reflect in their behaviour. The more informed users are about the possible risks of social networking site usage and what their data is used for, the more they distrusted the social networking site.

This research also aimed to answer how trust towards a social networking site shapes future usage intention. As Debatin, Lovejoy and Hughes (2009) have concluded, users continue to use a social networking site regardless of the risks. Furthermore, the level of trust of the respondents in this study had no impact on whether they use the site. Some of the respondents did mention that they thought of stopping using social networking sites due to lack of trust but have ultimately not done it. Most of the interviewees stated that they will continue to use the social networking sites for as long as others use them. This has also been confirmed by the conformity and peer group pressure theory which posits that people feel indirect pressure to adapt to the majority, even though they maybe would have acted differently individually (Crutchfield, 1995). Therefore, we can conclude that users of social networking sites will continue to use the sites, regardless of the privacy risks and concerns.

6.4 LIMITATIONS AND FURTHER RESEARCH

As all research, this one has its limitations. Firstly, a methodological limitation was a lack of prior research on the specific topic of privacy awareness, i.e. informed data disclosure. Furthermore, the number of conducted interviews is relatively small and consists only of millennials and Europeans. Therefore, the findings cannot be generalised. However, one could argue having a sample that consists of millennials might have been beneficial for this study as they are all experienced in using social networking sites. Moreover, this research is based on the self-reported behaviour of the respondents, making the findings not entirely reliable as self-

reported data is subject to all kinds of biases, such as selective memory, attribution or exaggeration. However, the respondents have shown that they are honest by choosing to use their real names. Another important point to mention is that none of the respondents were native English speakers which could have limited their answers.

There are plentiful opportunities for further research. Future research could expand the scope to more participants to test if the conclusions of this study still hold when more of the general public is included. Future studies would benefit from examining the actual behaviour of participants rather than just relying on self-reporting. The topic of privacy aware data disclosure on social networking sites is a broad and vastly unexplored field that could be examined in future research with both qualitative and quantitative methods. As social networking sites are evolving and changing constantly, so should the research studying it.

6.5 PRACTICAL IMPLICATIONS

This thesis offers a theoretical insight into the role that privacy awareness and informed data disclosure have in trust towards social networking sites. The findings of this thesis have shown that users express lower degrees of trust towards a social networking sites when they are more informed about the possible privacy risks. Ultimately, this means that companies can maintain relationships with consumers only if the consumers trust how their data is being handled. The first step to building trust in regard to data disclosure is informing customers about their data and giving them the option to opt-out. This goes beyond the companies alone, as adjustments in legislation are needed as well. The findings of this thesis point out that a more consumer-centric model is needed for information privacy because it will lead to healthy relationships in the online world. Benefits for both consumers and users can be derived. Consumers will have control over their data, whereas the companies will enjoy more trust.

7 CONCLUSION

This research utilises qualitative methodology to explore the role of informed data disclosure in trust towards three social networking sites: Facebook, Instagram and LinkedIn. Social networking sites are used by almost half of the people in the world and they are mostly used daily (Statista, 2017; Statista, 2019). Unimaginable amounts of users' personal data is collected and used by these sites. Most people are not even aware of the extent to which their data is mined, but even those that are do not feel like they are in a position to change anything (Joergensen, 2014).

Privacy policies, which are intended to protect the privacy of the end-users, seem to protect mostly companies. Users of social networking sites cannot be aware of all the possible risks if they do not read the privacy policies. However, they are written in a language most people do not understand and are too long for most people to be bothered. Not reading privacy policies leaves users to more exposure to risks because they are not informed. Some do turn to other sources for information, but this only leads to more distrust towards the social networking sites. Miranda and Saunders (2003) have stated that social networking sites will be trusted more by their users, if they are honest, educative and transparent to their users about how and what their data is collected for.

The critical research review has shown trust is an important antecedent of behaviour on social networking sites. However, to the best of my knowledge, no study so far has researched how being informed about and aware of the possible risks of data disclosure shapes the trust users have towards a social networking site. This research has shown that even when users are aware of the possible risks that they expose themselves to when disclosing data on social networking sites, they mostly do not change their disclosure behaviour. However, the trust in social networking sites decreases as the privacy awareness of users increases.

8 SUMMARY IN THE SLOVENE LANGUAGE

Pregled literature poudarja pomen preučevanja vloge, ki jo ima informirano razkrivanje podatkov na Facebooku, Instagramu in LinkedInu pri zaupanju v spletna družbena omrežja. Namen te raziskave je bil sprva preučiti obstoječo literaturo, ki zadeva razkrivanje podatkov na spletnih družbenih omrežjih, zavestno in podučeno razkrivanje podatkov in nazadnje tudi zaupanje v spletna družbena omrežja. V drugem delu je bila izvedena kvalitativna raziskava, v kateri sem se osredotočila na preučevanje vloge zavestnega in informiranega razkrivanja podatkov in vloge takšnega razkrivanja pri zaupanju uporabnikov spletnim družbenim omrežjem. Preučitev, kako koncepti zavedanja o zasebnosti in posledično razkrivanja osebnih podatkov vplivajo na zaupanje spletnim družbenim omrežjem kot znamkam, nam namreč lahko pomaga razumeti, kako izboljšati strategijo varovanja zasebnosti spletnih mest na družbenih omrežjih, ter tudi zakonodajo in predpise glede zbiranja, analiziranja in uporabe podatkov. Osrednji namen te teze je bil odgovoriti na vprašanje, kakšno vlogo ima informirano razkrivanje podatkov pri zaupanju v spletna družbena omrežja.

Za boljši vpogled v vlogo, ki jo ima razkrivanje osebnih podatkov na spletnih družbenih omrežjih pri zaupanju v njih, sem na podlagi pregleda literature ugotovila, da bi bila potrebna študija, ki zajema različna spletna družbena omrežja. V raziskavi sem – s ciljem bolje razumeti, kakšno vlogo ima zavedno razkrivanje podatkov na družbenih omrežjih pri zaupanju blagovnim znamkam družbenih omrežij – podatke pridobila primerjalno za tri spletna družbena omrežja, in sicer Facebook, Instagram in LinkedIn.

S ciljem odgovoriti na temeljno raziskovalno vprašanje sem s pomočjo literature postavila tri dodatna raziskovalna vprašanja, na katera sem skozi raziskavo poskusila odgovoriti:

- RV 1: Koliko pozornosti uporabniki spletnih družbenih omrežij posvečajo informiranju o tveganjih pri razkrivanju zasebnih podatkov?
- RV 2: Bodo uporabniki spletnih družbenih omrežij slednja uporabljali še naprej, ne glede na tveganja in pomisleke glede zasebnosti?
- RV 3: Bo zaupanje uporabnikov spletnim družbenim omrežjem večje ob večji informiranosti glede potencialnih tveganj pri razkrivanju zasebnih podatkov?

Za preučitev vloge razkrivanja zasebnih podatkov uporabnikov različnih spletnih družbenih omrežjih in vloge zavestnega in informiranega razkrivanja podatkov pri zaupanju v spletna družbena omrežja, sem izvedla kvalitativno raziskavo, in sicer 6 polstrukturiranih intervjujev, ki so vsebovali štiri sklope vprašanj. Ti so se osredotočili na kontekst uporabe spletnih družbenih omrežij, na pomen ozaveščenosti o zasebnosti, na pomen zaupanja v spletna družbena omrežja in na odnos intervjuvancev do namena njihove nadaljnje uporabe Facebooka, Instagrama in Linkedina. Polstrukturirani intervjuji so bili izbrani kot raziskovalna metoda, saj je ta tehnika meni kot raziskovalcu omogočila poglobljeno raziskati zastavljeno raziskovalno vprašanje.

Rezultati raziskave so nam pomagali odgovoriti na prvo zastavljeno raziskovalno vprašanje, saj so pokazali, da se uporabniki spletnih družbenih omrežij pogosto ne zavedajo morebitnih tveganj pri razkrivanju svojih podatkov na določenem družbenem omrežju. Drugi cilj raziskave je bil preučiti vlogo tveganja, ki ga prinese razkrivanje zasebnih podatkov, pri zaupanju spletnim družbenim omrežjem. Rezultati raziskave so pokazali, da se z večjim zavedanjem o morebitnih tveganjih pri uporabi spletnih družbenih omrežjih manjša zaupanje do teh spletnih mest in tudi njihova uporaba. Študija je skušala odgovoriti tudi na vprašanje, kako zaupanje v spletna družbena omrežja oblikuje prihodnost njihove uporabe. Študija je pokazala, da bodo uporabniki še naprej (nekritično) uporabljali spletna družbena omrežja, in sicer neodvisno od morebitnih tveganj in pomislekov glede varstva njihove zasebnosti. Ta podatek nam je ponudil odgovor na drugo zastavljeno raziskovalno vprašanje.

Tako kot pregled literature je tudi moja raziskava opozorila na pomen zaupanja kot pomembnega napovednika vedenja na spletnih družbenih omrežjih. Na podlagi pregleda literature lahko rečem, da do sedaj še nisem zasledila študije, ki bi se osredotočila na raziskavo vloge informiranega in zavednega razkrivanja podatkov pri oblikovanju zaupanja uporabnikov spletnim družbenim omrežjem, zato sem ta vidik v raziskavi dodatno naslovila. Raziskava je pokazala, da uporabniki, kljub zavedanju morebitnih posledic izpostavljanja zasebnih podatkov, svojega vzorca vedenja na spletnih družbenih omrežjih večinoma ne spreminjajo. Temu dejstvu navkljub pa se zaupanje v slednja zmanjšuje, ozaveščenost uporabnikov o zasebnosti podatkov pa se postopno povečuje. S tem smo odgovorili na tretje raziskovalno vprašanje, saj so rezultati raziskave pokazali, da uporabniki spletnih družbenih omrežij tem spletnim mestom zaupajo manj ob večji informiranosti glede potencialnih tveganj pri razkrivanju zasebnih podatkov. Na podlagi vsega tega lahko sklepamo, da se uporabniki – kljub vsemu vedenju, ki ga imajo – ne želijo ali pa ne zmorejo odpovedati uporabi spletnih družbenih omrežij, saj zavzemajo velik delež njihovega prostega časa.

9 REFERENCES

1. Abir, E. (2010). *U.S. Patent No. 7,711,547*. Washington, DC: U.S. Patent and Trademark Office.
2. Acquisti, A. and Gross. R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge.
3. Al-Kandari, A., Melkote, S. R., & Sharif, A. (2016). Needs and Motives of Instagram Users that Predict Self-disclosure Use: A Case Study of Young Adults in Kuwait. *Journal of Creative Communications*, 11(2), 85–101.
4. Altman, I., and Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. New York: Holt, Rinehart & Winston.
5. Barth, S., & De Jong, M. D. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics*, 34(7), 1038-1058.
6. Barry, T. E. (1987). The development of the hierarchy of effects: An historical perspective. *Current issues and Research in Advertising*, 10(1-2), 251-295.
7. Bechmann, A. (2014). Non-informed consent cultures: Privacy policies and app contracts on Facebook *Journal of Media Business Studies*, 11(1), 21–32.
8. Bélanger, F., and Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4), 1017–1041.
9. Bleier, A., and Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3), 390-409.
10. Boyd, D. M and Ellison, N.B. (2008). Social Network Sites: definition, history and scholarship. *Journal of Computer-Mediated Communication*, (13), 210–230.
11. Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior*, 69, 207-217.
12. Chaudhuri, A., & Holbrook, M. B. (2001). The chain of effects from brand trust and brand affect to brand performance: the role of brand loyalty. *Journal of marketing*, 65(2), 81-93.
13. Choi, B. C. F., Jiang, Z., & Yap, E. (2012). Information sharing in online dyadic exchange: A relational dialectic perspective.

14. Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498-512.
15. Crutchfield, R. S. (1955). Conformity and character. *American Psychologist*, 10(5), 191.
16. Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10(1), 104-115.
17. Debatin, B., Lovejoy, J. P., Horn, A. K., and Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, 15(1), 83-108.
18. De Moor, S., Dock, M., Gallez, S., Lenaerts, S., Scholler, C., & Vleugels, C. (2008). Teens and ICT: Risks and Opportunities. Retrieved from http://www.belspo.be/belspo/fedra/TA/synTA08_nl.pdf
19. Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.
20. Gleibs, I. H. (2014). Turning virtual public spaces into laboratories: Thoughts on conducting online field studies using social network sites. *Analyses of Social Issues and Public Policy*, 14(1), 352-370.
21. Gross, R., and Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71–80). ACM.
22. Grabner-Kräuter, and Bitter. (2015). Trust in online social networks: A multifaceted perspective. *Forum for Social Economics*, 44(1), 48-68.
23. Grace, P., and Surridge, M. (2017, August). Towards a model of user-centered privacy preservation. In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (p. 91). ACM.
24. Han, P. and Maclaurin, A. (2002). Do consumers really care about online privacy? *Marketing Management*, 11(1):35.
25. Heravi, A., Mani, D., Choo, K. R. and Mubarak, S. (2017). Making decisions about self-disclosure in online social networks. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 1922–1931.

26. Heravi, A., Mubarak, S., and Choo, K. K. R. (2016). Online Social Networking Has a Greater Effect on Others than on Me: A Third-Person Effect Perspective. *arXiv preprint arXiv:1605.04723*.
27. Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80-85.
28. Jia, H., Wisniewski, P. J., Xu, H., Rosson, M. B., & Carroll, J. M. (2015, February). Risk-taking as a learning process for shaping teen's online information privacy behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 583-599). ACM.
29. Kay, M. J. (2006). Strong brands and corporate brands. *European Journal of Marketing*, 40(7/8), 742-760.
30. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, 44(2), 544-564.
31. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134.
32. Kotler, P., & Keller, K. (2003). *Marketing Management*, (international version).
33. Krasnova, H., Kolesnikova, E., and Günther, O. (2009). It won't happen to me!. *Self-disclosure in online social networks*. In *AMCIS 2009 Proceedings*.
34. Joergensen, R. F. (2014). The unbearable lightness of user consent. *Internet Policy Review*, 3(4).
35. Lewicki, R. J., & Bunker, B. B. (1995). Developing and maintaining trust in work relationships. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations*. *Frontiers of theory and reserach* (pp. 114 – 139). London: Sage Publications.
36. Lilley, S., Grodzinsky, F. S., & Gumbus, A. (2012). Revealing the commercialized and compliant Facebook user. *Journal of information, communication and ethics in society*, 10(2), 82-92.
37. Laufer, R. S., and Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, 33(3), 22–42.
38. Madejski, M., Johnson, M., & Bellovin, S. M. (2012, March). A study of privacy settings errors in an online social network. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 340-345). IEEE.

39. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), 336-355.
40. Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, 82, 103-116.
41. Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.
42. McCroskey, J. C. and Richmond, V. P. (1977). Communication Apprehension as a Predictor of Self-disclosure. *Communication Quarterly*, 25(4), 40–43.
43. McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *The Academy of Management Review*, 23(3), 473 – 490.
44. McParland, C., & Connolly, R. (2007). Online Privacy Concerns: Threat or Opportunity. In *Proceedings of the 2007 European and Mediterranean Conference on Information Systems (EMCIS2007)*.
45. Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, 9(4), JCMC942.
46. Milne, G. R., & Boza, M. E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of interactive Marketing*, 13(1), 5-24.
47. Miranda, S. M., & Saunders, C. S. (2003). The social construction of meaning: An alternative perspective on information sharing. *Information systems research*, 14(1), 87-106.
48. Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of marketing*, 58(3), 20-38.
49. Nehf, J. P. (2005). Shopping for privacy online: Consumer decision-making strategies and the emerging market for information privacy. *U. Ill. JL Tech. & Pol'y*, 1.
50. Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1-20.
51. Padyab, A., Päivärinta, T., Ståhlbröst, A., & Bergvall-Kåreborn, B. (2019). Awareness of Indirect Information Disclosure on Social Network Sites. *Social Media+ Society*, 5(2), 2056305118824199.

52. Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, 28(3), 1019-1027.
53. 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.
54. Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American psychologist*, 26(5), 443.
55. Shane-Simpson, C., Manago, A., Gaggi, N., & Gillespie-Lynch, K. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in Human Behavior*, 86, 276-288.
56. Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196.
57. Pang, H. (2018). Microblogging, friendship maintenance, and life satisfaction among university students: The mediatory role of online self-disclosure. *Telematics and Informatics*, 35(8), 2232-2241.
58. Perrin, A. (October, 2015). Social Media Usage: 2005-2015. *Pew Research Center*. Retrieved from: <https://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/>.
59. Pöttsch, S. (2008, September). Privacy awareness: A means to solve the privacy paradox?. In *IFIP Summer School on the Future of Identity in the Information Society* (pp. 226-236). Springer, Berlin, Heidelberg.
60. Solomon, M. R. (2010). *Consumer behaviour: A European perspective*. Pearson education.
61. Statista. (2019). *Daily time spent on social networking by internet users worldwide from 2012 to 2019 (in minutes)*. Retrieved from: <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/>.
62. Statista. (2018(a)). *Facebook – statistics and facts*. Retrieved from: <https://www.statista.com/topics/751/facebook/>.
63. Statista (2018(b)). *Number of monthly active Instagram users from January 2013 to June 2018 (in millions)*. Retrieved from: <https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/>.

64. Statista. (2019). *Number of social network users worldwide from 2010 to 2021 (in billions)*. Retrieved from: <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>.
65. Stutzman, F., Capra, R., and Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27(1), 590-598.
66. Stutzman, F. D., Gross, R., and Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of privacy and confidentiality*, 4(2), 2.
67. Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure?. *Computers in Human Behavior*, 29(3), 821-826.
68. Van den Berg, B., & van der Hof, S. (2012). What happens to my data? A novel approach to informing users of data processing practices. *First Monday*, 17(7).

10 APPENDIXES

10.1 APPENDIX A

Interviewee name: Leo

Age: 27

Sex: male

Nationality: Belgian

Location: Lovina, Indonesia

Duration: 26'' 30'

Date: 28.08.2019.

T: Hi, thank you for participating in this interview and I guarantee that all of your data will be anonymously used. So, do you use Facebook?

L: Yes

T: And Instagram?

L: Yes

T: And LinkedIn?

L: Yes

T: So why would you say that you use Facebook?

L: Facebook is more to... I use Facebook most, prob, most, blah...

T: (laughs)

L: Most of the time for, uh, with the Messenger app to connect with friends, uh, I watch a lot of videos. Like funny videos and everything. I'm not like a person that will post anything on Facebook, but I'm like more to see what other people will do or what's happening in the world. Instead of reading the newspaper, I'll like look at the newspaper, uh, the posts of the newspapers on Facebook. I would read that. See what my friends are doing or what's happening around the world. That's mainly my main reason that I'm on Facebook.

T: Ok. Why do you use Instagram?

L: Because I use Instagram to... When I take photos of, uh, objects and everything to put it on Instagram to probably get likes, to see if people like my kind of ideas and photographs or, or. Like, I like to be creative and my creative output is on Instagram 'cause I hardly post photos of myself.

T: And why do you use LinkedIn?

L: Uh, it's, uh, it's a different way to find jobs and to get connected with people that can find you a job. Because I don't believe in putting all your eggs in one basket. Like you have to go to the... What's the English word for it? The... It's not internship, but Intrim kantooren...

T: Aha

L: If you know what I mean?

T: Uh, yes, kind of. The people that help you find jobs.

L: Yeah, the people that help me find jobs. I always, like, instead of going to one office I go to ten offices. And, like, LinkedIn is also one of the options that I can do to find jobs. But it's easy. It's online. I can do it on my cell phone. I don't have to go to the offices themselves, so that's way more easy for me, as well. That's (inaudible).

T: Heh, ok. Do you know what types of data usually people usually disclose on Facebook?

L: I think most of the time personal data like photos of themselves going on holiday, uh, what are they doing, um, what are they gonna do or they need some help bugging stuff. Facebook is so multi purposely used nowadays. In the beginning it was like posting about yourself. Now you can buy and sell everything, like, chat to other people. So, it's, um, they increased or, um, they maximised actually their public. So, I think that's what they use it most for.

T: So, you think that people disclose a lot of personal data on Facebook?

L: Yeah. For sure.

T: Okay. What about Instagram? What types of data do people disclose on Instagram?

L: Also, quite a lot of personal data. Depending on what kind of person you're actually looking at. Because you have influencers. They will photograph themselves in certain places to promote that kind of, uh... Whatever they are actually taking photos of or promoting. You have the personal, like the more artistic people, like I count myself more in the artistic people. For photographing old buildings, nature, animals, whatever makes you creative in that kind of point. And then you have the other third kind of people. They take photos of themselves just to, I don't know, when they're on a holiday, uh, just for themselves. That's what I'd... The three main differences on Instagram.

T: Ok. And what types of data do you think people usually disclose on LinkedIn?

L: Aah, probably work related. Like their resumes, connections to... Like I found a new job or I'm working there and then people can see that you're working there or maybe like poach you from the one company to promote you to the other company. I think it's more work related.

T: So, when you think of privacy policies of social networking sites what is the first thing that comes to your mind?

L: Huuh... It's a really big debate in, like, privacy policies. Like people are, like, yeah, my privacy is violated. Everything, all my information is out there, but I think personally, if you don't have to hide anything, if you're not, if you're not hiding anything that's, like, not supposed to be out there, you shouldn't be afraid of anything. The social app, why they actually, in my opinion, why they need so much different kind of data of you is to just link up everything. Because if I look up something on Google, it'll automatically appear on my Facebook as well. People might think like, yeah, they look into my history that I'm looking around in Google, for Google searches and everything and I get ads and everything on Facebook. I think it's easy for me 'cause I'm looking for it and it's already popping up on my Facebook and I get the commercials and everything. So, I think it's convenient. Ok, is my privacy violated? I don't personally have anything to hide. They can look up, look into me. I'm not that interesting, in my opinion. I think for most people it's the same, but I think as well, like, yeah... (shrugs)

T: Does that concern you ever?

L: There should be boundaries, but, like, if it's to, to... Like I said, if it's easier to connect people they're looking for and like to connect all the apps together. Like if they use your personal data

to connect like Instagram, Facebook, LinkedIn, Google searches, everything. Like if it's all connected just for the purpose of that, no problem with it. But if it's like to investigate like, for example, umm... I look up how to make a bomb. Just for fun. It's not that the FBI should know. It's, like, I'm not a terrorist, I'm just maybe curious. I like to know stuff.

T: Ok.

L: There are boundaries. Ok, it's good for people to know, for example, what are they doing. Are they doing something wrong to investigate them, but there should be other ways. Not invading personal privacy. That's what I think. That's where you have to draw the line.

T: Ok. Do you know someone who has read privacy policies of social networking sites?

L: Uuh, how do you mean by read?

T: As in, when you want to become a member of a SNS... To become one, you actually have to read and agree to a privacy policy.

L: I think most people don't read it because it's too long. And they aren't bothered to read it. If they would simplify it, umm... The problem is it's really hard to simplify the privacy policy because there are so many rules around it and no one is actually bothered to read it. In my opinion. I think I've never read one properly. I would just like, if I have to, look through it. Most of the time it's like, yeah, you're allowed to this and this and this. Most, most times you're giving them more access than you actually know and that's, I think that's a bad thing because they know nobody is bothered to read it. But without reading it, you're actually saying you're allowed to do this and this and this. And probably half of the people don't even know what they're signing up for. And, uh, like I said, I don't have anything to hide, but somebody else or some... Mostly the older generations have more problems with it because they're, like, more private about their personal stuff. The nowadays youth and everything, they post everything about themselves. I'm going on holiday, I went on a holiday, I went on drinks with that person, they're really open about everything. So, they have less of a problem with it. If the social network checks on them, but I think it's more a problem for the older generations. But they should simplify it, the privacy policy because no one is bothered to read like 5 pages of text.

T: Well, more, though. (Laughs)

L: Well it could be more, but I'm just summing it up. Like, nobody cares to read it.

T: And what do you think would motivate someone to read privacy policies?

L: Make a video. It's easier to watch a video of someone explaining it to you than rather reading it 'cause reading is way more harder for some people. They're not bothered to put their own time into it and I think that, if you put up a video. Like, an obligated video that you can not cancel, you have to watch the whole movie that tells you, like, what you're supposed to, supposed to do or what you're signing up for. I think that's the best way to bring it to the people 'cause I can't be bothered by reading it.

T: Umm, ok. So did you ever look into alternatives for these sites? For instance, for Facebook: Diaspora, Ello, EyeEm, Vero. For Instagram: Flickr, Google Photos, Imgur, Pinterest. For LinkedIn: Opportunity, Meetup, Sumry, Jobcase?

L: No, because half of them you summed up, I have no idea what they are. Like I know Flickr, I know LinkedIn, Facebook, Instagram. Uhh, you have a few other ones, but I'm not bothered. Like, I'm, I would say I'm a 50/50 person on social media. Like, I'm on there, but I don't post a lot about myself because I'm a private person myself. Like I don't, I have nothing to hide, so

people can look into me, but I'm not gonna put photos of myself. Like, I have photos of myself on there, but I'm not gonna say, like, today I ate this, I'm here, nor photos of myself. I will show photos of those places, but not of me. Because, uh, the more... It's more of actually a work reason that I do it. Because, um, nowadays how many times does a person look themselves up on Google. What do they find if they type in my name?

T: Mhm

L: And I think that's important. Because if I type my name into Google, you immediately see Facebook, Instagram, whatever. If you go to Instagram, you can see photos. And it could be a disadvantage for your job. For example, I like to party, I like to drink, maybe I smoke a joint or maybe I do some drugs of whatever. If I'm not bothered, like, if I have photos of that and I post them (inaudible). If I go to a job interview and they like, I like look you up. And they see straight away photos of me blowing some weed, ale, smoking some weed or drinking or partying whole day, having tattoos, that might... Then I have a bad review because they're actually gonna have pretences about me. Like, they're gonna... Like first impressions are really important, especially when you find a job. So I'd rather see them, like... The first impression is me, when I'm there. Not when they look me up. Because that's my disadvantage. Because they're gonna create a vision or an opinion about me without me being there to correct them. And that's why I don't think it's always good to post, like that's why I'm private about myself. But that's my personal opinion about it.

T: That's what we're here for (laughs). Ok, so are there any other ways you inform yourself about data disclosure or data protection on SNS? Such as reading blog posts or articles, discussing it with friends or reading laws and regulations...

L: Mostly with friends. Like I said, I'm not bothered with reading stuff. I don't mind. I, I think my Facebook is probably the least protected, whatever, everybody can see whatever I'm doing, but I never post something. Like, I used to post, like, when Facebook was in the beginning and popular and everything, I would post myself, but now I think it's been almost half a year, a year that I've posted a photo of myself. I'm not... I only have it to watch movies how people are doing stuff, what are they doing... I think Facebook for me is mostly for video. Funny videos, educative videos... For most that's why I'm there. Or to buy and sell stuff. It's just another gateway to buy, sell, watch videos, instead of YouTube or... And you can connect and share with everybody and tag people in funny videos. That's mainly what I'm doing on Facebook. I think actually, like, nowadays... I don't know when Facebook was generated or, like, made... Probably...

T: About 10?

L: Yeah, 10 years ago...

T: I mean, that it was, like, public.

L: Public and everything. But I think Facebook is dying out in the youth. Nobody, like, it's going, like... Now I think actually the older generation is more on Facebook than the younger generation because the younger generation is already switching to something new. 'Cause we always want new things and that's what, I think in five years most of the youth people is probably not gonna be on Facebook anymore to, like, post photos about themselves because they use Instagram for it. If you're gonna see through the messenger or the buy and sell, like I told you, that's gonna be still there, I think. Or maybe some other name or some other company, but in general posting about yourself... Facebook is not up to date with that anymore, in my opinion.

T: Well it's the same company now, though.

L: Yeah, yeah(inaudible). Mark Zuckerberg has a fuckload of money. Sorry for my English, but... (laughs)

T: (laughs)

L: They have a lot of money for it, so...

T: Ok. So, do you feel that the privacy of your data is protected by each of these sites? So please respond by Facebook, Instagram, LinkedIn.

L: I once saw the video of Mark Zuckerberg being in court asked questions. Like, about the data laws and everything. And he was asked, like, yeah you can see whatever is in that description. But the thing is, like, they analyse everything you do for the purpose of commercials, they can promote you videos that you're looking up, like, your search history and everything that's gonna be promoted... But all that data is computer analysed. It's an encrypted message. They cannot print it out, what I'm typing, so it's an encrypted... So, it's safe, somewhere. There is our... I think they are, they are within certain laws. They cannot, like, for example, I'm writing with you. I have a whole conversation with you. It could be friendly, sexual, work, whatever... It's not that somebody's like I want that guy's conversation now on paper. I think that's really hard for them to just get it out. Maybe if you're Mark Zuckerberg, maybe. But I still think it's encrypted. So, I think there are strict laws about it. It's pretty safe, but it's just your data, data is used for connecting everything with each other and I think personally that's a good thing. It makes life a lot easier.

T: So, you think that your data is somewhat protected by each of these...?

L: Like you, like you said it yourself, somewhat. I think it could be more, it could be less. I have no idea because I have not really agreed to, read every terms of agreement, but I've definitely think they are somewhat protected.

T: On each of these?

L: Yeah.

T: Ok. So now for the next several, several questions we're going to pretend that I am a new user that wants to join each of these SNS, so I'm going to ask you for some advice.

L: Alright.

T: Ok, so let's start with Facebook. So, can I trust that Facebook will not use my data for any other purposes?

L: Then Facebook?

T: Yes, other than I intended it for, to be...

L: Just on Facebook... I think no. I think Facebook uses it for a lot more than just Facebook.

T: So, you think that I can't trust Facebook that it won't share my data with third parties?

L: I think they do. I wouldn't... If you don't, if you don't want your data to be, um, that your data gets in the hands of a third party, I wouldn't trust Facebook.

T: And do you think I consent to that somewhere in the...?

L: Yeah, for sure.

T: Ok.

L: A 100 % sure.

T: Do you think that they will be honest when, in my dealings with me, in their dealings with me?

L: If you read the terms of agreement properly and you really understand everything that they're saying, I think there's some note that they will tell you they're doing it.

T: And do you think that they're transparent and that they clearly communicate about how my data is connected and what it's used for?

L: Yeah, you used the word clearly... That's a really... How can I say it? It is there but it's not clearly. It's in the text, but it's somewhere in alinea, page 15, alinea 3, small words... It's, it's... I don't want to use the word hidden. It's in there, but it's hard to find and you really have to properly read and analyse everything that's in the terms of agreement and then it will be in there, but it's for... Like I said, nobody reads it.

T: Ok.

L: It's gonna be in there, but... Like I said, page 15, alinea 3, whatever. It's gonna be in there.

T: Then for Instagram. Can I trust that they will not use my data for other purposes?

L: I would've said maybe yes. But now you said to me that Facebook bought Instagram, so I'm pretty sure right now.

T: So, would you answer the same to all the questions that I've asked so far? So that I can't trust that they will share my data with third parties without my consent, that they're honest and transparent...?

L: See that's what I mean. If I put my name into Google, first thing, in the first two or three searches is Instagram. So, they're already sharing it on some other platform. So no, like exactly the same answers.

T: And for LinkedIn?

L: Probably yeah. Probably, probably the same. Not really sure, LinkedIn. I'm not so familiar, I know LinkedIn, but I'm not so familiar with LinkedIn as I am with Facebook and Instagram. But I would say all the same.

T: And do you think that I should trust SNS in general?

L: But that depends on the word trust. With what do you want to trust social media with?

T: With my data.

L: And how important do you think your data is to be private or not private? That's the problem.

T: Ok. And what would you say, uh, if you had to choose one of the three and say which one do you trust the most?

L: Hmm, equally none.

T: Equally none, ok (laughs). Ok, so are you aware of any recent data breach scandals revolving around these SNS?

L: Huh, there's probably gonna be a few 'cause, like I said, talked about lawsuit against Mark Zuckerberg. So, there's definitely gonna be some breaches and leaks and whatever and in Belgium as well, where I'm from (inaudible).

T: (laughs)

L: Umm, there's been a breach. I don't know which party it was, it was about a political party. Probably NVA. Umm, they, when you looked at, they would give you, um... I don't wanna use the word propaganda, but when you have certain search histories, they will, like how can I say? Certain kind of videos are sent to you or information sent to you, that is gonna pop up on your Facebook or everything and then it's like I'm gonna vote for them. 'Cause I, like, get a lot of commercials, if I look up, like, I'm...

T: Ah, in that sense, yeah, ok. Well that's, uh...

L: I think there was something about it in Belgium because they, they use a lot of, uh... It was, I don't wanna say a scandal, but something about that. That they use your data to, um, promote their certain kind of political parties. But is it bad? I'm actually not, I don't... In my... It's bad probably, but I don't care.

T: Did that, did any of those scandals change your behaviour?

L: No, not at all.

T: No, ok. So, do you know someone who has stopped using SNS? Either one of these or all together.

L: Like, you have people who are bothered that their data is used, you have people who don't think that's a problem. And do I know people personally? I, I know... Puh, it's hard to say. I know people who are bothered by it, but they still use it, but they've really protective of what they ever post. But will they stop? Probably not. Cause they still use it for something, not to post photos about themselves, but they know, like... They will read the terms of agreement. Like, I'm talking about the mom of a friend of mine. She reads, I, I'm not gonna say she reads the terms of agreement, but she's like 'I'm not gonna put up when I'm on holiday, I'm not gonna say when I'm going this or this because that's information that gets used', but she still posting photos when she was on a holiday and when she's travelling or having friends or family over. So, she's still posting on there even though she knows her data is used and she's complaining about it, but she still does it. So, I don't know. It's a vicious circle. It goes around. Everybody uses it and nobody cares. They will probably use it, like, you have the big scandal in, in America with Snowden and everything. That they use your data and they spy on you and whatever. Is it bad? A 100 % sure. Do I care? Personally, no. Spy on me, I have nothing to hide.

T: (laughs) So what do you think would motivate someone to stop use, using SNS?

L: Uh, that's a hard thing. It's so integrated in society at this point, but (inaudible)... For me personally, it would be through an educative video. Like, really, a transparent video about everything you're agreeing to without even acknowledging what you're agreeing to. If that would be in a whole video explained. And you have to see it and you would see it and you know what you're actually, uh, giving use. What they're actually using your data for... That might stop a person. But it all depends on the person, how they're, do they read them, do they watch a video, do they care, do they don't care, it all depends on the person, you cannot say... For me personally, it's hard to see it globally, on a very large scale. But it's really possible to go, for like, every different kind of person. You can make a video, you can make the pages and everything with the agreements, you can make an audio book, that somebody says it, like... you

have to have multiple options instead of just the books. Because, like, the pages... Read the terms of agreement, I don't like reading so I'm not gonna read them. You can say like listen or watch to it. I might do it. I'm not gonna say I'm gonna do it. I might do it. I think the biggest problem is, like, because for a new person goes to Instagram, Facebook, LinkedIn, they wanna use it now. They make the app, ale, they download the app. They go onto the app. They sign up. And they wanna use it now. And sign up. You (inaudible), you add everything, read through the terms of agreement. Yes. And I'm using it. They don't, they don't wanna put the time and effort into reading it. That's what I think. And even the video or the audio book, the people just wanna use the app now. Like, download it and use it now. Not download it, read everything, make sure all your data is secure and then use it. 'Cause that takes a lot of time and then people are probably not interested in using the app anymore. That's why it's not obligated to read it. You can just click it, check the box, I read it. And, uh, and yeah.

T: So, what would you actually conclude, what would motivate you to stop using SNS? Only the video? Or some kind of scandal? Or, I don't know, that something personally happens to you or to your friends or?

L: Probably, that's I think one of the hardest questions so far 'cause I don't think I would stop, 'cause I'm not bothered by it all. Like I said, I think of myself like maybe the government thinks I have state secrets or anything, I don't know. In my opinion, it's what are they gonna find about me.

T: Yeah, it's...

L: But I think, as well, I'm not gonna say like Facebook necessarily, but I think pretty much any phone these days... Even with a laptop they can turn on your webcam and everything. Like even now you're using your iPhone to record this message. Who knows where that recording is saved up? Who knows? Like you could find out, reading the terms of agreement, but, like, I'm not bothered. Who knows what happens?

T: Yeah, ok.

L: That's how far it goes. You can go really deep into it. Like it has to be protected and everything and everything. And it has to be protected. Is it gonna be if a scandal, information about myself, like, for example, a stupid video of me being drunk, walking around naked in the street. And it's like published over there. Probably would laugh with it. Like I said, I have nothing to hide. I'm not ashamed of myself, like cool. I would be like 'how the fuck did they get the photo?', but probably in some terms of agreement, I agreed that they could use the photo for whatever they wanted. And now there's a photo of me in the city, naked.

T: (laughs) Ok.

L: I don't care. So that's why it's really hard. I think it's really interesting questions and things, but I think it's really hard for me. Like, I'm not into social media that much, but would I stop it? Probably not. Even with a scandal or anything. It'd have to be a huge, huge scandal and even then... I'm not creative enough to think of that kind of a big scandal to make me stop.

T: Ok, well that's it. Thank you so much for participating!

10.2 APPENDIX B

Interviewee name: Lisa

Age: 26

Sex: female

Nationality: German

Location: Canggu, Indonesia

Duration: 18'' 40'

Date: 07.09.2019.

T: Hi! Thank you so much for participating in this interview. I just want to assure you that all of your data will be anonymous and used only for the purposes of this thesis.

L: Ok.

T: Ok, so... Do you use Facebook?

L: Yes, I do.

T: Instagram?

L: Yes.

T: And LinkedIn?

L: Yes.

T: So why would you say that you use Facebook?

L: Umm... I use Facebook only for Facebook groups and for my family in the Balkans. So I can, like, get in touch with them.

T: And why do you use Instagram?

L: Umm, more for friends and sharing my experiences and for fun.

T: And LinkedIn?

L: Umm, not too much, but for job purposes.

T: How often would you say that you use Facebook?

L: Umm, maybe once every two weeks.

T: Oh really?

L: Yeah, like, I don't browse really often. I just sometimes just go in there. Or when somebody is writing me from my family, I go to Facebook.

T: Ok. And Instagram?

L: Every day (laughs).

T: Ok. And LinkedIn?

L: Umm, maybe once a month. Yeah...

T: Ok, so... Do you know what types of data other people usually disclose on Facebook?

L: What do you mean with disclose?

T: So, share.

L: Aha. If I know what they share?

T: Mhm.

L: Other people?

T: What would you say people usually share on Facebook?

L: Aha. On Facebook... I don't know. Um, events they're doing, like, I'm at a coffee right now or at a restaurant, what they're doing...

T: Ok. And what do you think that usu-, people usually disclose on Instagram?

L: Umm... Food (laughs). A lot of food, um, travel, um, yeah... Same as Facebook maybe, but more with pictures. Yeah.

T: And LinkedIn?

L: Umm... Information. A lot of content that is valuable in knowledge.

T: Ok. Would you say that people disclose personal data on all three networks?

L: Umm, yes.

T: And on which one would you say that it's the most?

L: The most? I think on Facebook.

T: Ok. And how much do you disclose on Facebook?

L: Umm, not much. Not too much, I would say.

T: Ok. And on Instagram?

L: Umm, also not too much. Not anymore.

T: And LinkedIn?

L: Umm, only my businesses stuff. Nothing personal, I would say.

T: Uhh, ok. When you think of privacy policies on SNS what is the first thing that comes to your mind?

L: Umm... Privacy policy?

T: Mhm.

L: Umm, leaking security (laughs).

T: Yeah?

L: Yeah. I, I don't think... My first word won't be safety. I just know they... It's just safe for the website. So, they actually told you that if you sign up you will do Facebook stuff or

Instagram stuff, you can't actually sue them or do anything to them. That's just for their safety, I would say.

T: Ok. Ok. Umm, so do you know someone who has read the privacy policy of any SNS?

L: (laughs) Nobody, no.

T: Ok, if you could think of a person that would do it...

L: Yeah.

T: What would you describe them like? What would they be like?

L: Somebody who is really, umm, how do you say that in English? Anxious.

T: Ok.

L: Really, really scary of, umm, yeah, sharing their data or... I really think, yeah. I don't know. Somebody who's just scary to share their data and don't want to give the site too much personal stuff and, yeah, anxious person.

T: Ah, so that... You sharing your personal data, that doesn't concern you?

L: Ahh, not anymore. When I found out I think I was a little bit down. Not so much scared. I was shocked, but I don't know... I think I got a little bit open minded with that.

T: Ok. When you found out what? Sorry, I didn't get that.

L: Umm, for example, when they said, umm, that they use your data for advertising purposes.

T: Mhm.

L: I... First, my first thought was negative. I thought 'they using my data and making money out of it?', but I thought, when I thought about it, it's just personalised advertising. So, I don't see every bullshit, I just see what I want to see. So, I think I see it more positive now.

T: So you don't... Basically, you would say that you're not concerned that something bad might happen with your data?

L: Uhh, it could happen, I know that, but I think I'm not too concerned with it.

T: Ok. Uh, so did you ever look into alternatives for these sites? Such as Diaspora, Ello, EyeEm or Vero for Facebook. Flickr, Google Photos, Imgur or Pinterest for Instagram. And, like, Opportunity, Meetup, Sumry, Jobcase for LinkedIn. Or any other, if you?

L: I never actively looked for alternatives, but I use Pinterest. But not for the same purposes as Instagram. I only go there to get inspirated or just to find content.

T: And for LinkedIn? 'Cause I remember I was having a conversation earlier...

L: Yeah.

T: That you did use an alternative? Or? Aha, no. That was Dennis.

L: Yeah (laughs). But, um, there is an alternative called Xin. I think that's a German thing, but I don't use it.

T: Ok, how come you never looked into alternatives?

L: Uh, because I always found my jobs in a different, like, different ways. Umm, how do I say it? I never really needed LinkedIn, so I just have, I just have it.

T: And for Facebook and Instagram, how come you didn't search for alternatives?

L: For Facebook because I don't use Facebook too much, so I don't really need an alternative 'cause I don't really need Facebook as well, but Instagram... I don't know. I don't think that there is something similar to Instagram. That's just...

T: Yeah.

L: It's a unique application, I would say.

T: Ok. Uh, are there any other ways that you inform yourself about data disclosure on SNS?

L: Only when I do websites for others. Then I look into privacy policies and make sure everything is on the safe side.

T: Ah, so for instance, you don't discuss it with friends or read laws or regulations, blogposts?

L: Umm... Not really.

T: No?

L: No.

T: Do you feel that the privacy of your data is protected by Facebook?

L: No (laughs).

T: Why? Could you please elaborate a bit more?

L: Umm... I mean we all watch the news and we see Mark Zuckerberg having issues and, you know, being, um, not in a good situation with Facebook. So, I, I am aware of that they do use data... Probably in a not good way for us and we don't know it. So...

T: Mhm. So, you would say that your data is not so secure?

L: No, no, no. But that's why I'm also not giving too much personal data into Facebook or Instagram because I know that they might use it.

T: So, you would say the same for Instagram? That you don't feel that the privacy for your data is protected by Instagram?

L: Yeah, since I know that Facebook bought Instagram.

T: Yeah.

L: I mean... That's what I think. It's just the same company.

T: And LinkedIn?

L: Umm... I don't know actually, I've never really concerned with LinkedIn privacy policy or my safety of data.

T: Do you think it's because you disclose a different type of data?

L: I think so, yeah. It's something I want to be, something I want to publish those things. I want people to read it. So, I think... And it's different data. It's not personal things like my relationship status or something like that. It's just my personal working experiences, so, yeah...

T: Ok. Umm, ok. So, for the next several questions we are going to pretend that I am a new user of each of the SNS and I am asking you for advice.

L: Ok (laughs).

T: So, let's start with Facebook.

L: Ok.

T: So, do you think that I can trust that Facebook will not use my data for other purposes? Then just for what I intended them for, like...

L: Umm, no, I can't. I can't advise you or make it sure for you that they will not use it in a safe way.

T: Why?

L: Because they want to make money. And in the end, at the end of the day, it's still a company that wants to make money and you're the profit maker.

T: So, you believe that my data will be used for other purposes?

L: Definitely, so be careful (laughs).

T: Ok. Do you think that I can trust that Facebook will not share my data with third parties, but without my consent?

L: Um, if I'm sure about it?

T: Yes.

L: No, I think they will do it without your consent.

T: Without my consent?

L: Yes.

T: You even think that, like...

L: I think I even know it 'cause the way. What, how we work, we know we can use others' pictures without even asking them. And it's legal.

T: Ok, but do you think that it's written somewhere, and you just don't know?

L: No, no, it's written.

T: So, you do think that I would give my consent, but...

L: Oh, like in that way, you do give your consent. Yeah, as soon as you upload things – that is your consent.

T: Yeah, yeah, yeah. Ok. So, do you think that they will be honest in their dealings with me?

L: What do you mean with dealings?

T: Yeah, in our relationship. I don't know how to say. For instance, that they are not deceiving me in some way.

L: Oh, hmm... Good question. Umm, I don't know. It's a yes and it's a no. I think they try to put everything in the privacy policy, but you don't really read it, so they kind of deceive you, but they actually did say it somewhere. It's like a, it's a grey zone, I would say.

T: Ok. Um, do you think that they are transparent and that they clearly communicate about how my data is collected and what it's used for?

L: No (laughs). I mean they started now, but not, not as... It should be even better than they do now, definitely.

T: Elaborate a bit (laughs). I need a lot of your opinion, on everything.

L: (laughs) 'Cause when Facebook started they obviously didn't say much about how they use the data, but now that they are public and people get behind their safety policy, uh, privacy policy, they try to do, to be transparent, but I think they still hide the things they can hide. For example, giving your consent by uploading a thing. Like, this is not clear to many people, I think. And this is not transparent.

T: Ok. Ok, then uh... So, the same questions for Instagram. So, can I trust that Instagram will not use my data for other purposes?

L: No (laughs).

T: No?

L: Same as for Facebook.

T: Everything same as for Facebook?

L: I would say so, yeah.

T: And LinkedIn?

L: No clue for LinkedIn, honestly. I don't know. But I think they... I don't know, I never actually got into LinkedIn all too much.

T: Ok. Do you think that I should trust SNS in general?

L: Depends on what.

T: Yeah, trust them with my data.

L: Trust is a strong word. I would say no. Always be careful. You can use it for your purpose, but don't let social media use you for their purpose. So, as long as you are careful with your data, like, giving your personal data, I think you can trust them, like, really... How do you say? In a distance you can trust them, but actually... No. (laughs)

T: (laughs) Ok. Now for each one. Should I trust Facebook in general?

L: No.

T: Instagram?

L: No.

T: And LinkedIn?

L: Let's say yes (laughs).

T: (laughs) Why would you say yes to LinkedIn?

L: Because they only have one purpose of connecting you for like business purposes, that you can find a job or find others for your business or for applying somewhere. So, I think they use

your data, but it's a win-win situation, you know? So, I would say, yeah, you could trust LinkedIn?

T: And you don't think that with Facebook or Instagram that you also have a win on your side, let's say?

L: You have, but they also hide a lot of loses you have, so I think it's more a win for them than for you.

T: Ok. Do you think that how much you trust a specific SNS impacts how much data you will share?

L: Yes, definitely.

T: So, that's why you, for instance, decided not to share as much data?

L: Yeah, I think that, yeah, I think that... I did it when I was young so I, obviously, I shared a lot of data then, but then I realised what they do. And then I kind of blocked everything, but I think that the data I gave in there is kind of forever on Facebook, so I can't get it out of there.

T: Ok. So, for instance, are you aware of any data breach scandals revolving around any of these SNS?

L: Yeah. Like I said, Facebook, Mark Zuckerberg is pretty much in the news right now. Umm, yeah, I think Instagram got in the media when it got out that they can use your pictures for advertising purposes.

T: Really?

L: You didn't know that?

T: No.

L: Yeah, they can. As like, your upload is the consent. They can use your picture for advertising purposes.

T: Oh wow.

L: Like obviously they're not allowed to advertise you as a person or a human being, but if you wear, I don't know, a bracelet from a brand, they are allowed to use your picture to advertise their bracelet, so yeah...

T: Yeah. So, would you say that any of these scandals changed your behaviour?

L: No. And they didn't change others behaviour as well. People are still uploading things, I'm still uploading, um... Yeah. I don't know why. I just, I think it's not concerning me too much.

T: How come?

L: Umm, maybe because that's how I upload my pictures. It's mostly not my face or not even me in the pictures, just you know, photography things and, yeah... I don't really care. I don't even know why they should use my pictures. I think maybe that's because of this, yeah.

T: Ok. So, do you know someone who has stopped using SNS?

L: Yes, I know a few people actually. But they stopped using it because it's so time consuming, actually not because of the data.

T: No? Ok.

L: They, um, they felt a little addicted to Instagram and Facebook, so they deleted their account. They can only be contacted by phone or WhatsApp and that's it.

T: And have you ever thought of stopping using SNS?

L: I did when I was studying for my exams (laughs), 'cause it was also a little distracting, but I managed to control myself. So I don't even use it too much.

T: Ok, so you would say that... What would have to happen for you to stop using SNS?

L: Oh, to stop using it? I think, oh, I don't know. When others stop using it? Like, I don't know, I know all of my friends are not on Facebook and all of my family is not on Instagram and no one that I know is using Instagram any more, then I think that I would stop to because there is no one that is seeing what I post, you know what I mean? But, um, yeah, I think not a big scandal. It would not stop me.

T: Well that's it from my questions. Do you have anything you would like to add?

L: No, but it's an interesting topic. I see where it's going. Definitely interesting.

T: Thank you so much for participating,

L: Yeah, you're welcome!

10.3 APPENDIX C

Interviewee name: Dominic

Age: 26

Sex: male

Nationality: German

Location: Canggu, Indonesia

Duration: 16” 10’

Date: 07.09.2019.

T: Ok. Thank you for participating in this interview and I want to guarantee you that all of your data will be anonymously used and used only for the purposes of this thesis.

D: Ok.

T: Ok. So, do you use Facebook?

D: Yes.

T: Instagram.

D: Yes.

T: LinkedIn?

D: Yes.

T: So, why would you say that you use Facebook?

D: Facebook... Uh, I currently use for groups, like (inaudible) and a part of different interest groups where I get some information. And yeah, that's basically it, actually.

T: Ok.

D: And yeah, I work with Facebook for Facebook marketing.

T: Ok. And why do you use Instagram?

D: Instagram I use to see like photos of friends and family and everything.

T: And LinkedIn?

D: LinkedIn for, yeah, for business connections, basically.

T: And how often do you use Facebook?

D: Daily you mean?

T: Oh well, then you answered my question.

D: Yeah.

T: So more than once a day?

D: Yeah, more than once a day.

T: And Instagram?

D: Also.

T: LinkedIn?

D: LinkedIn, um, maybe every three to four days.

T: Ok, so, do you know what types of data other people usually disclose on Facebook?

D: What do you mean disclose?

T: Share.

D: Ah, ok. Um, currently not so many photos, less than before, and videos. Is it the right question, like what types of data usually?

T: Yeah, yeah. Like, yeah, what do they share on their profiles?

D: Yeah, um... Actually, not so much, I'm only active in groups.

T: What do you think most other people share?

D: Ah, yeah, yeah, ok. Like statuses, like text status, videos, photos.

T: And on Instagram?

D: Instagram, photos and videos, basically.

T: Of what kinds of things?

D: Of, um, of they going somewhere, like travelling, their food, friends and family, their dogs (laughs)...

T: (laughs) Ok. And LinkedIn?

D: And LinkedIn, I think it's more related to certain businesses. They are sharing news on businesses, they are sharing news on their, like, positions, maybe if they change positions, for example.

T: Ok and do you know what types of data you disclose on Facebook?

D: I only post in groups. Like, um, yeah. Other than that, I don't share data about photos and videos anymore. Like I changed my profile picture maybe four years ago last time and wrote something which I posted. I sometimes share something like articles and, yeah, that would be all for Facebook.

T: And Instagram?

D: Instagram I put mostly stories, Instagram stories. And sometimes, very rarely, I put some photos for upload and videos maybe, yeah.

T: Of yourself or?

D: Mm, sometimes, sometimes, yes. But usually for travel destinations and...

T: Ok and LinkedIn?

D: LinkedIn, I actually never share something.

T: But did you share, for instance, like your past experiences and?

D: Yeah, in the past I shared past experiences.

T: But not anymore?

D: Not anymore, not the last two years.

T: Ok. So, when you think of privacy policies of SNS what is the first thing that comes to mind?

D: I think they are pretty open with our data.

T: In what sense?

D: That they don't protect the data that much. They share it to companies, to agencies, so... Yeah.

T: So, would you say... If you could use one word what would it be?

D: Transparent? No, maybe it's not the right word. Like, open I would say, if I could use only one word.

T: Ok. Um, do you know someone who has read the privacy policies of a SNS?

D: No.

T: And if you were to think of such a person, what would that person be like?

D: Um, I think it's more like older generations probably.

T: Ok.

D: Maybe plus fifties, plus fifty years.

T: Ok, why? What do you think motivates them?

D: It's more like experience when I talk to, like, older people like for example my parents or parents of my friends. I know they talk about these kinds of topics because it's in the news, like data leaks. They talk to me like 'why did you post a photo? You know your data isn't protected' or something like that. And, um, so that's why I imagine these kinds of people probably read the policies.

T: Ok and what would make you read a privacy policy?

D: I wouldn't read it.

T: Never? (laughs)

D: No (laughs).

T: Does the privacy of your data concern you on SNS?

D: No.

T: How come?

D: Well, honestly, I know that the data is pretty open. Everybody's got the data. Especially, I work in advertising for social media, so I know that we basically can get all the data and it doesn't concern me because, I don't know, like... What can happen? It would concern me, if my banking data would be leaked or something because then I can lose something, but what can I lose if my data goes out? I don't have a problem with people knowing what kind of sites I like, what my age is or... Like, what can happen?

T: Or, for instance, your texts, the pictures you send to other people?

D: Well, that's what I think, if I wouldn't want somebody to see what I sent or share, then I wouldn't share it.

T: Mhm, ok.

D: It would be a problem, if my data like private conversations leaked. That's definitely a concern, but not open shared.

T: Yeah, yeah, yeah. Ok. Even though, for instance, when you agreed to become a member of these sites you also agreed for them to have access to your messages, private messages.

D: Um, yeah.

T: That is a fact.

D: Oh, ok.

T: Are you more concerned now or?

D: Well, yeah. (laughs)

T: (laughs) Did you ever look into alternatives for these sites? For instance, Facebook: Diaspora, Ello, EyeEm or Vero. For Instagram Flickr, Google Photos, Imgur or Pinterest. For LinkedIn: Meetup, Sumry, Jobcase, UpWork?

D: Yeah, but not for a constant use. Meetup, yeah. But not as an alternative, maybe yeah for events or something, but not for photo sharing or video sharing, like social media, connections or something.

T: How come you never looked into alternatives?

D: Because all of my friends, like the people who I connect with only use these sites.

T: Ok. Are there any other ways you inform yourself about data disclosure on SNS, such as reading blog posts or articles, discussing it with your friends, reading laws and regulations?

D: No, never.

T: Never at all?

D: It's never a topic.

T: Ok. For a marketer that's weird (laughs).

D: (laughs)

T: Do you feel that the privacy of your data is protected by Facebook?

D: No.

T: Why?

D: Um... Why? Because I heard many news about it over leaks of data and, um, many scandals. I don't know if it's the right English word. Um, yeah, so I don't think that it's protected that much to be honest.

T: And by Instagram?

D: No, it's the same company.

T: And LinkedIn?

D: LinkedIn, I really don't know. Probably it's more protected than Facebook and Instagram.

T: Why do you think so?

D: Only because I heard only scandals about only Facebook and Instagram.

T: Ok. For the next several questions we are going to pretend that I am a new user of each of the SNS and I am asking you for advice.

D: Ok.

T: Ok. Let's start with Facebook. Do you think that I can trust that Facebook will not use my data for other purposes?

D: I would say you cannot trust them, no.

T: Why?

D: Because they will probably sell the data to agencies, companies, yeah...

T: Do you think that they would do it without my consent?

D: I would think so.

T: So that I haven't consented to it anywhere? And they would still do it?

D: I might, I think so, yeah.

T: Ok.

D: I have the opinion that they don't care about data protection.

T: Ok. Do you think that I can trust that they will be honest in their dealings with me?

D: No.

T: Why?

D: That's just my opinion.

T: Ok.

D: I don't think they care about that. I think they care more about their benefits.

T: Ok. And do you think that they are transparent and clearly communicate about how my data is collected and what it's used for?

D: I think they try to appear like that, but I'm not sure that this is the truth.

T: Do you think that I should trust Facebook in general?

D: No.

T: And do you trust Facebook in general?

D: I would like, as I said, I would never give any data which shouldn't be shared, like, any information which shouldn't be shared.

T: Ok. Now the same questions for Instagram. Do you think that I can trust that Instagram will not use my data for other purposes?

D: In my opinion, all the strategies of Instagram are the same as Facebook.

T: Ok, so the same answers?

D: All answers would be the same for Instagram. It's basically the same company.

T: And LinkedIn?

D: LinkedIn, I'm not sure. I think it's not the same company, right?

T: No, it's not.

D: No.

T: Ok, let's go through the questions.

D: Yeah, yeah.

T: So, can I trust that Instagram will not use my data for other purposes?

D: I wouldn't.

T: No? Why?

D: I don't, I don't... I really don't know. It's just a suspicion that they might do the same strategies as Facebook and Instagram in order to grow the same pace as Facebook and Instagram maybe.

T: And do you think that they would also share my data with third parties without my consent?

D: Yes.

T: Yes. And do you think that they will be honest in their dealings with me?

D: No.

T: And transparent and clearly communicate?

D: I would think it's the same strategy.

T: Ok. So also...

D: For all online companies.

T: And out of the three, which one would you say you trust the most?

D: Ok, I would say LinkedIn.

T: Why?

D: Because I have never heard bad stuff about LinkedIn, yet.

T: Do you think that it might also be because you're sharing different types of data?

D: No, I wouldn't say so.

T: No? Ok.

D: Because I think LinkedIn data would be even more delicate, actually, to share. Because it's more important data, you know, about incomes and... Like, people would be more interested to see if you earn more money or less which you can get an impression from on LinkedIn rather than seeing like photos of dogs or something from Facebook, you know?

T: Yeah. So, do you think that trusting a SNS impacts how much data you will share?

D: Umm, I don't know. I'm not sure. Like, trusting... Can you just repeat the question?

T: So, trusting a SNS, does that impact how much data you share on that site? For instance, you don't trust Facebook, so you're not gonna share as much.

D: Ah, ok. I wouldn't say so. In general, for, like, online platforms things I wouldn't share, I wouldn't share anywhere because the things I wouldn't share, I wouldn't share anywhere. Because I think the link can be anywhere on the Internet. It doesn't matter if it's Facebook or if it's another company, I think.

T: So, do you think that it's a general distrust towards sharing your data online?

D: Yeah, yeah. That's the right answer.

T: Are you aware of, well you are, of any recent data breach scandals around these SNS?

D: I know that they are, but I wouldn't be able to name an exact example right now.

T: But you know them, so... Do you think that any of these impacted your behaviour?

D: No, no. Because I was sure that this happens anyway (laughs).

T: Yeah and do you think that it changed anyone's behaviour?

D: I think yeah. I think a lot, actually. Like, since these data leaks or these scandals were coming to the surface, many people talk about it and I think share less probably. Or use also less social media.

T: Ok. Do you know someone who stopped using SNS?

D: Yes. A few people.

T: And what do you think motivated them to stop using it. All the people I know that stopped using it... I would say 90 % because of time reasons, because they spend too much time on social media and, yeah, just because they realise they spend too much time on social media. You know, scrolling Facebook, Instagram. And then I would say 10 % of people because they just don't trust any more since these data leaks and scandals.

T: Mhm. And have you ever (laughs) thought of stopping using social networking sites?

D: Not because of data leaks. Not because I'm afraid of my data. Just because of time reasons.

T: And what do you think would have to happen, data wise, for you to stop using SNS?

D: Maybe for example, if my email gets, like, well that probably happens anyway. Like, if my emails get around and I just get spammed with emails, for example. Which happens already probably. But there wouldn't be anything that I would stop it because of that reason. As I said, because I think it's open anyway, so.

T: Ok, well, thank you for participating.

10.4 APPENDIX D

Interviewee name: Mila

Age: 27

Sex: female

Nationality: Croatian

Location: Wommelgem, Belgium

Duration: 26'' 46'

Date: 07.09.2019.

T: Hi! Thank you for participating in this interview. I would just like to assure you that all of your data will be used anonymously and only for the purposes of this thesis.

M: Ok.

T: So, do you use Facebook?

M: Yes.

T: Do you use Instagram?

M: I do.

T: And LinkedIn?

M: I do.

T: Ok, so why would you say that you use Facebook?

M: Well, mostly for connecting with people. I mostly use Facebook Messenger rather than the actual app or desktop version. So, for chatting I suppose.

T: Ok, why do you use Instagram?

M: Umm, that's a good question. For stalking people (laughs). Uh, and watching dog videos and watching interesting tutorials. So sometimes exercise videos or food prepping videos.

T: Ok and why would you say you use LinkedIn?

M: Uh, for work purposes, you know. Searching for jobs or connecting with other colleagues and also for work.

T: And how often would you say that you use Facebook?

M: Facebook... Messenger app probably daily and the actual Facebook app, desktop, once or twice a week.

T: And how often do you use Instagram?

M: Instagram pretty much daily, but not for very long. Maybe a few minutes a day.

T: And LinkedIn?

M: LinkedIn I'm on daily. Just checking up and also for work purposes, like I mentioned earlier.

T: And how much would you say that you disclose – oh, I'm sorry. Do you know what types of data other people usually disclose on Facebook?

M: A lot, I would say. You know, date of birth, some people, well city they live in, some people even put their addresses and mobile phones in there and then obviously all major life events, um, are recorded on Facebook by lots of people. Things like buying a house or having a baby or getting a new job, so I think a lot probably.

T: And on Instagram?

M: I think Instagram less so because you don't need to populate your profile in the same way. You know, you don't have all the, like, company or school et cetera options, but I think people, at least my age, use Instagram for posting photos more, so I guess if you wanna find stuff out on Instagram, you will. Things like where they are or where they're going on holiday or, you know, family events, so I'd probably say as much as Facebook, but maybe on a different level. If that makes sense.

T: Mhm. So, what, how would you say on a different level, like more personal or?

M: I'd say, well, more visual, if that makes sense. An example is a girl I used to work with has put a photo on Instagram recently that she bought a new house and, you know, the photo of her house showed her house number and she was stupid enough to include the street name in the capture of the, the image. So, in a different way that they might not upload their address saying my current place of living is XYZ, but they still disclose that information, perhaps unintentionally.

T: Yeah. And what would you say what type of data other people usually disclose on LinkedIn?

M: I would say LinkedIn is mostly used, at least by people I know, for disclosing work data. So, who you work for, when you work for them, you know, your role spec and company spec et cetera. And then obviously there is a different side of LinkedIn, the marketing solutions, but I wouldn't say a lot of people use that unless they work in marketing.

T: Ok. And do you know what types of data you disclose on Facebook?

M: Not very much anymore, I used to when I was younger. I had loads of personal stuff like current city and cities I lived in, school information and job title. And then I'd say that I became either more aware of it or started caring less or a bit of both, so my Facebook profile does not contain any information really other than my name and current city, I think. And I don't really upload photos or post. I use it mostly for communication, so I'd say I don't disclose that much.

T: Ok and what types of data do you disclose on Instagram?

M: Umm, Instagram, my, my handle is my name, so I suppose I disclose my full name and uhh... Yeah, it does say where I live, as in which city and then I post sporadically, so I think my last post was probably six months ago and it's mostly of places I go on holiday. So I guess I disclose all of my holiday adventures mostly.

T: (giggles) And what types of data do you disclose on LinkedIn?

M: Only my work data. So, the companies I work for, my job titles and job description. So, I use it mostly to get found by computers, slash, share my profile with potential employers.

T: Ok. So, when you think of privacy policies of SNS what is the first thing that comes to your mind?

M: I never read them. Ever. I always just click on accept terms and conditions and god knows what kind of data I might be disclosing that I'm not aware of. But, frankly, I don't care. And I probably should, now that you've asked the question.

T: So, would you, do you know someone who has read the privacy policy of any SNS?

M: No. No.

T: If you could think of a person that would do that, what kind of a person would that be?

M: I would say that they're a geek, probably, or paranoid. And it's probably the wrong way to describe them, but, probably, just very conscious of the fact that they're leaving a digital footprint. People just don't tend to care about these things because they don't think about the kind of data they're disclosing. So I would say we're ignorant and the people who try to read them are probably more down to earth, but I think it's very rare.

T: So, does, does the privacy of your data on SNS concern you?

M: Uh, it concerns me in a way. I know I don't disclose that much, like, looking at it naked eye. But if someone wanted to pull information off of three different platforms about me, I guess they could come up with a story knowing which city I live in and who I work for and when I'm on holiday. If someone really wanted to rob my house, I guess they could deduct a conclusion of when I'm not at home. Um, but I haven't really given this much thought until now.

T: Ok, so, did you ever look into alternatives for these sites. Like for instance Diaspora, Ello, EyeEm or Vero for Facebook? Flickr, Google Photos, Imgur or Pinterest for Instagram? Meetup, Sumry, Jobcase or UpWork for Linked In?

M: No, I must admit I haven't heard of most of them. I've heard of Google Photos and Pinterest. I don't have a profile on any of those... Like, Pinterest I use for ideas, like, design ideas for example. And I have heard of Upwork and I've used it as a potential employer rather than an employee, so I've searched for freelancers on there, but I haven't used it and I don't think it serves the same purpose as LinkedIn.

T: Ok, so how come you never actually looked into alternatives?

M: I wasn't aware there were any. Not in the same way. I think Facebook and Instagram dominate the social media sphere and most people use those. So, you tend to use what everybody else is using. If nothing so you can connect with the people you wanna connect with, I guess.

T: Ok. So, are there any other ways that you inform yourself about data disclosure on any of these SNS like reading blog posts or articles, discussing with friends, reading laws and regulations or something else?

M: Well, I, I work in marketing, so I tend to look at it from a marketer's perspective rather than a personal perspective. So, whenever I, for example, I know, I know professionally how much data Facebook harnesses because of all the social advertising that can be done, but I've actually, up until this interview, never thought about perhaps adjusting mine, so people like myself, can't market to me on these social sites (laughs).

T: Yeah.

M: But, frankly, to answer your question shortly. No, I don't really inform myself personally, privately.

T: And do you feel that the privacy of your data is protected on, by, by Facebook?

M: I doubt it, to be honest. They probably resell it and one thing I've recently found out, um, was, and I didn't know that. A friend of mine told me. That when you accept terms and conditions, privacy terms and conditions on Facebook Messenger, you also agree to them using your microphone. So, the way he proved that to me was talking about buying new underwear and then five minutes later he had underwear ads showing up on his Facebook feed and I found that quite scary. But it's mostly things I find out through conversation, rather than actually actively trying to inform myself. So it is, it is quite worrying, to be honest. And I don't think people give enough attention to it. People don't think about it.

T: Mhm. And do you feel that privacy of your data is protected by Instagram?

M: Oh, probably not. Instagram is even more public than Facebook. You can set your profile to private, but that just means other followers can't see it, but I'm sure Instagram can see it. I know that they're owned by the same person, Facebook and Instagram, so I'm sure that they feed data from one to another. So, if you're stupid enough to connect these profiles, which I'm sure most people are, then you are revealing much more about yourself than you maybe intended to in the first place.

T: And do you feel that the privacy of your data is protected by LinkedIn?

M: Honestly, I've never thought about LinkedIn. I know more about Facebook and Twitter, sorry, Facebook and Instagram, but LinkedIn never seemed like a social platform to me in the same way. I always thought of it as a job-hunting platform. I suppose people use it differently than me. I'm sure people post updates and photos the same way they do on Instagram, but I just don't do that. But it is fairly public, to be honest, if someone searched my name on Google, they would find my LinkedIn profile and they would know my work history. But I would say it's no different from any big job websites. Like, for example, I live in the UK and there are job websites like CV Library or Indeed and they work similarly to LinkedIn, as in your work information is publicly disclosed, but that is not something I would personally worry about, because I don't work for, you know FBI or CIA.

T: (giggles) Ok. Um, so, um, for the the next several questions we are going to pretend that I am a new user of each of the SNS and I will ask you for advice.

M: Ok.

T: So, let's start with Facebook. Can I trust that Facebook will not use my data for other purposes?

M: No. I would say no.

T: Why?

M: Because I don't think they would disclose it... Well, you're probably aware of the GDPR, so I don't think they would disclose it publicly. So, there's a thing we call PPI, personally identifiable info-, PII, personal identifiable information, um, so for example, if you've got someone's date of birth and address that makes it really easy for someone else to find out who you are. Um, so, I think Facebook probably wouldn't share PII with other companies, so they would never be able to find out it is exactly yourself who is interested in, I don't know, horse riding, Um, but they will definitely sell that information on in an anonymised way so companies can sell stuff to you. Um, so it's a bit of a grey area, I guess. I think anyone who really wants to would be able to put two and two together, so, in short, I would say that you couldn't trust Facebook.

T: You think that I can't trust Facebook in general?

M: Yeah. I, I would... If you were a new user, which is very unlikely in this day and age, I would probably advise you keep information you post and information you give about yourself when signing up to a minimum. So, I would probably tell you to try not to post things like your address, the city you live in, the school you went to or anything that people can use against you in one way. So, I would advise to proceed with caution.

T: Ok. Can I trust that Facebook will not share my data with third parties without my consent?

M: I think yes. But I think people, you give your consent when signing up. Facebook won't let you create a profile unless you sign up to their terms and conditions and even though I haven't read them, I'm pretty sure that somewhere in small print it says that this data might be used for marketing purposes, for example. So, if you ask me for advice, I'd say read the terms and conditions, I don't know, I've never read them.

T: Ok. And do you think that Facebook will be honest in its dealings with me?

M: Uh, I don't think any business is very honest. I think they all just want to make money. Um, so, probably not. I would always say read the small print, if you're concerned about how your data is being used, but as I said earlier in the conversation, I don't think a lot of people care or are aware of how much they're disclosing.

T: Mhm. Ok. And do you think that Facebook is transparent and clearly communicates about how my data is collected and what it's used for?

M: I would ask you define transparent. I'm sure that it's all laid out in terms and conditions and their privacy statement, but again they're probably, they're aware that no one reads them because they're long and they include legal language that people like myself wouldn't understand necessarily. So, they probably are honest, but they count on you not finding out more.

T: Mhm. Ok. Now for Instagram. So... Can I trust that Instagram will not use my data for other purposes?

M: Again, I would say the same thing as Facebook. Particularly because I know Facebook and Instagram are pretty much the same company.

T: So, you would respond the same to all the questions?

M: Yes. Yes. For Instagram pretty much the same, but I'm happy to go through it, if you'd like me to.

T: Well, if it's the same, then it's ok.

M: Ok.

T: And LinkedIn?

M: LinkedIn, I think I perceive LinkedIn differently. If you ask me, I know it is social media, but I never thought of LinkedIn as a social channel in the same way. I always considered it more professional media sharing rather than social and I think LinkedIn has changed a lot recently. People have started using it for different purposes. You know, things like posting about themselves and updating their statuses. But when I first joined LinkedIn it wasn't like that. So, back then I would say 'yes, you can trust them' and 'yes, they're honest and transparent', but I would probably advise again to proceed with caution simply because we live in a capitalist society and all these three channels are free to use. Yet they all make millions, therefore they all make money on advertising and how are they advertising? Using your data. So, you know,

it depends what you want to see, I guess. If you don't want to be spammed with ads, you would have to minimise the information you give, but then what's the point of using the network?

T: Ok. Let's just summarise. If you could choose one of the three. Which one would you say you trust the most and which do you trust the least?

M: I would say I trust LinkedIn the most, although that might just be a biased opinion and not based on facts. And of the three I'd say I trust Facebook the least, but as I said, I know they're the same company, so I can't really explain why I trust Facebook the least. Because they're probably dealing with their customers the same way as Instagram.

T: And would you say that you maybe trust LinkedIn the most because of the different type of data that people usually disclose on the network?

M: I would say that is probably correct. Not probably, that is correct. It's more work based so I can't see how your work information can be exploited in the same way as your personal information. You know, saying you work as a sales coordinator for Microsoft for three years, I wouldn't say that's as worrying as disclosing your address, for example.

T: Ok, thank you. Would you say that how much you trust a SNS impacts how much you share on that site?

M: I think probably yes. But I think also, until this interview, I didn't really give this much thought, but I... So, I stopped sharing on Facebook simply because I lost interest, I guess. Because I grew up and I just couldn't understand the point of sharing. I mean why are other people, I'm not interested in what they're sharing, why would they care about me? But I think, I think it comes down to more than just trust. I think people are ignorant. The majority of people are ignorant and they don't think about this, so I think the main driver on whether they share or not share stuff on social media is more psychological and related to how much they want to expose themselves and make themselves look perfect rather than trusting a site.

T: Mhm.

M: But yeah, I might be going off the charts here, so I do apologise.

T: That's ok. Um, ok. So, are you aware of the any recent data breach scandals revolving around any of these sites?

M: Of the three we talked about, Facebook, Instagram...

T: Yeah.

M: No, no. I remember one that was WhatsApp fairly recently. And I know that WhatsApp is owned by Facebook so that's quite worrying because if there's a breach in one of the things they manage there might be a breach in another. But to be honest, I don't read the news that much, which is my fault, so no, I'm not aware of any.

T: And if there were any, would that change your behaviour?

M: It probably would. But one thing I do know, well actually, I don't know it. I wouldn't say it as a fact, but I'm pretty confident that is the case. I was very young when Facebook started, I was about 16 and that was, you know, before GDPR and before privacy became such a big deal and I remember my parents telling me 'be careful what you post there, blah, blah, blah' and I remember all the people saying that Facebook never deletes your data. So, even if you delete a photo you posted, you deleted it from your profile, but it still exists somewhere on their servers. I think that's probably correct, but I don't know if it's true.

T: It is true.

M: Yeah. And I know you cannot delete your profile. I know you can deactivate it, so it's publicly unavailable, but it still exists. So, changing my behaviour, I don't think it would impact the data that I've already shared. That's why when you asked me what I would advise you as a new user, I would say proceed with caution 'cause I can't change the things that I've already shared, but I can be mindful going forward.

T: Yeah, ok. Do you know someone who has stopped using SNS?

M: Quite a lot of people my age particularly.

T: And what motivated them to do it?

M: I think it's the same as me. Not the trust or distrust towards the site, but more the fact that they just don't care about getting approval from people they don't know. You know like likes and comments and shares and stuff. But, for example, I know my boyfriend, who is a bit older than myself, um, never really used the sites. Well never had Instagram, has LinkedIn, but uses it to a minimum extent. You know, just his job titles, no details. And Facebook, his Facebook is bare, you know. No photos, no uploads, no information. And I guess that might be because he's from an older generation and when you ask him, he says 'I just don't want to share my information with Facebook'. So, I guess it might be a correlation with age as well, the older you get the less likely, the more you think before you speak. In this case before you post. So perhaps it is age and attitude, but also awareness in a way.

T: Ok. Have you ever thought yourself of stopping, completely stopping using SNS or at least one of them?

M: Yes, I've deactivated my Facebook account last year because, well, for a long time I didn't know that you can still use messenger. Um, so that's why I didn't delete it, but then I found out you can continue using messenger without Facebook, so I deleted it. But as I mentioned, I work in marketing and I manage my companies Facebook site and in order to manage it I need to have a Facebook profile that I can log into with which is why I've deactivated my Facebook. For a long time, I've been thinking about stopping Instagram simply because I don't really post anymore, but on the other hand, all those dog videos aren't gonna watch themselves, so I'm probably gonna continue having an Instagram account and I never even thought about deleting LinkedIn because I think it's super handy for job hunts.

T: Ok, great, thank you so much.

M: You're very welcome.

T: Do you have anything else that you'd like to add?

M: No, no. I think it's a very interesting topic!

T: Cool, thank you so much!

M: Thank you! Bye, bye!

10.5 APPENDIX E

Interviewee name: Ana

Age: 29

Sex: female

Nationality: Croatian

Location: Wommelgem, Belgium

Duration: 33” 01’

Date: 07.09.2019.

T: Hi, so thank you for participating in this interview. I would just like to assure you that all of your data will be used only for the purposes of this thesis and it will be kept anonymous. So, do you use Facebook?

A: Yes, I do.

T: Do you use Instagram?

A: Yes.

T: And LinkedIn?

A: Yes.

T: Why do you use Facebook?

A: Facebook I use privately to connect with friends, especially because I used to live in different countries, so that was the best way to connect to them. I am a generation that mostly uses Facebook and Facebook Messenger rather than some new types of messengers that have since appeared.

T: Ok. And why do you use Instagram?

A: Instagram I use professionally, exclusively. So, I am a visual artist and illustrator, so I have my own business and that’s how I mostly promote myself through Instagram. So that’s only business related.

T: Ok. Why do you use LinkedIn?

A: LinkedIn is also business related. Although LinkedIn is a bit less well-known in my particular industry, but I still use it because it’s a good way to connect with art directors and other people in my industry.

T: Ok. How often do you use Facebook?

A: Every day.

T: And Instagram?

A: Every day as well.

T: And LinkedIn?

A: Once a week, once every two weeks. Much, much rarer.

T: Ok.

A: I...

T: No, say, say, sorry.

A: No, no, I was just about to say, just occasionally. Yeah, every two weeks. Let's put that down.

T: Ok. Do you know what types of data other people usually disclose on Facebook?

A: Umm, I guess, I guess I do, yes.

T: So, what kind of data?

A: Oh, what kind of data. Well, I think a lot of people disclose, in my personal experience, a lot of private data, such as their date of birth and their email addresses and their phone numbers and, but also where they live and, like, in more detail rather than just the city and so on. Do you want me to go into more detail or? Is this like the basic data that Facebook asks from you to put up or is it something that people do through posts?

T: Ah, either. Either is good. What comes to mind.

A: So, yeah. That's what I meant. There are some things that Facebook asks from all of its users, which is fine, I guess. But there are some things that, you know, people share photos of their very, very young children, um.... And they don't really understand there are many precarious groups on Facebook that could abuse that data. And once you put data on, it stays there. You can't really remove it, even though you feel as if though you have control over it, so... Yeah.

T: And do you know what types of data other people usually disclose on Instagram?

A: Ah, I... I presume it's similar, but I don't use it privately, so I don't really... I know people share a lot of personal photos and so on. But since I only use it for business purposes then I really tailor it to my needs, so everything I put up, I want to be left there. I want that to stay there and I want that to become as viral as possible, so in that sense, um, I think a lot of people do that as well. They deliberately tailor their lives to the needs of their business. They share some seemingly private things, but they've been shared with preconception, whereas... But I presume a lot of people, like, share their private thoughts. I know people have this whole using Instagram like people used blogs before, like, literally writing everything about their lives and embellishing their lives and becoming influencers in that way. But I don't really follow those people, so I don't really have the best notion in the sense that I can say 'oh yes, definitely. This is what they put up or don't put up', but I presume it's quite similar to Facebook actually.

T: Ok and what types of data do people usually disclose on LinkedIn?

A: Umm, more professional data. I mean there is a lot of seemingly private data on there as well because it is your CV (inaudible). But you really focus on your business. I meant that's the whole point of LinkedIn, so... You know, you won't have, for example, you know, pictures of your very young child and so on (laughs) up there or, like, something that cannot be found and shouldn't be disclosed in a way. For example, like, where you went to school. That's something that any potential professional connection would benefit from or you would benefit from them knowing this. In that sense, it's a bit less private or private data used for professional purposes.

T: Ok. So, uh, when you think of privacy policies on SNS, what is the first thing that comes to mind?

A: Fuck. Um, well...Anything? I can say anything?

T: Yes, anything.

A: So, the first thing that comes to mind is, um, um, what comes to mind is, like, corporate manipulation because I feel that all of these, like, pop-ups that tell me ‘oh, we care about your privacy. You should do this here in settings’ and so on and then ‘you’ll be more private. We won’t share this with any third party’ and so on and so forth. It’s, um, sure, if I do sign something and agree on something that is literally, explicitly not to be shared with third parties, I do believe that it’s gonna be like that. But then Facebook, for example, has had many breaches, security breaches and they have shared marketing data with third parties that they shouldn’t have done, shouldn’t have shared. So that’s the kind of thing that comes to mind, like, I choose not to put private things on Facebook because I never know who’s watching, in a way. And I know this sounds more paranoid than it actually is and I use Facebook like any other person. It’s not just like a blank page, but, um, some things are, I feel, really irrelevant for people who I communicate with, because my main purpose in using Facebook is to use the Facebook Messenger. I actually sometimes don’t even use the Facebook app particularly separate, separately, so...

T: Mhm.

A: So, that’s, I guess, the first thing that comes to mind. It’s a bit precarious, the whole thing. It’s not exactly... Because I know you have all of these privacy policies that are very, very detailed and I’m sure that if I went through it and took my sweet, sweet time in going through it, that I’d find some loopholes where they can actually share something with someone or whatever. So, it feels like you’re private, but you really aren’t.

T: Mhm. Ok, uh... Do you know someone who has read privacy policies of SNS?

A: In detail, no I really don’t. I mean maybe someone has, but we’ve never talked about that, you know. I think people just like see it, scroll, agree. ‘Cause no one has time basically (laughs).

T: If you would think of a person that would do that, what would they be like?

A: The person who reads privacy policies?

T: Yeah.

A: Oh my god. Super paranoid. Like extremely...

T: (laughs) Ok. What do you think would motivate them to do it?

A: Fear.

T: Mhm.

A: Anxiety. Um. The notion that our data, that we’re constantly being monitored. Like, we know this, but we’ve kind of learned to live in this society. But, you know, we know our microphones are listening to us, like to put it bluntly. Like, there’s an algorithm that processes keywords that we’re saying. So, if I mention something to my friends and my phone is near me, I will get an ad with a specific product later on and she will get an ad with a specific product later on. So, it’s very, very omnipresent in that sense. So, I do get that someone might be a bit fearful of it because it is a bit insane, if you think about it.

T: And how come you don’t, how come you haven’t read the privacy policies?

A: That's a very good question. Umm... I, I don't know. It's just... I guess when you see all of that... There were some instances where I tried reading them. Like, I went through it. Like, for example, with Spotify I did that. And then I stopped using it because there were some... Like, I didn't use Spotify in Croatia because there is no Spotify in Croatia and they explicitly say, in their privacy policy, they explicitly say that you cannot use Spotify in other countries. So, I don't do that because I'm one of these paranoid people (laughs).

T: (laughs)

A: But I don't, that was one time because I got an email notification. Um, and I made Spotify when I was in the UK which was, you know, perfectly fine then, so I stopped once I moved back. Like for Facebook, I just never... I don't know. If they don't pop up and they're not legible and easy to understand and, um, reduced to the basic important things, I will not read them. I just get lost in them, in a sense that, not that I can't understand them. I guess I don't have enough concentration or interest to go through it. And I think 'oh, everyone's using this app and if everyone's still using it, I guess they had to press agree so it's fine' because like it has millions and millions of users, so I'll be fine as well because it's not, you know, something underground. Which is completely stupid, but you kind of get... You kind of think that way. Like sheep basically. Everyone else is doing it and they're fine, therefore I'll be fine if I do it, therefore I don't have to read it.

T: Mhm. So, would you say that that concerns you still though?

A: Well, yes, I guess, but not as much as I maybe made it sound. Like, I am very much aware of these things, but I don't really, I don't become anxious over them. I don't think about them on a daily basis. I do, I don't really share anything on social media. I really am cautious about what I share. I don't like, for example, people just putting photos of me and tagging me. I don't like that, if I don't have control over that. Um, so, yeah, in that sense, I do try to have as much control as I possibly can, but I do understand it's limited, but no, I'm not overly concerned about it.

T: Mhm.

A: Like, weirdly.

T: And have you ever looked into alternatives for these sites? For instance, for Facebook: Diaspora, Ello, EyeEm or Vero. For Instagram Flickr, Google Photos, Imgur or Pinterest. For LinkedIn: Meetup, Sumry, Jobcase, UpWork?

A: For Facebook, no, I haven't heard any of them. For Instagram, I'm unfortunately, like, whenever I do something that's professional, I'm drawn to the site that gets me, that my potential clients are drawn to as well. For example, if I wasn't doing what I was doing professionally, I would never have Instagram. Like, I wouldn't have it, I wouldn't have an account, I wouldn't use it. So, I chose it, not because of Instagram, but because this particular app was really used in my industry and therefore I just joined it once I was doing my MA and realised everyone was using it and this was a way to get jobs and clients. Which is the truth, I do get jobs and clients through Instagram most often than not. Actually, that's my main source of income in a way. Um, um, and LinkedIn, to be honest, I made it because people told me it's good to have it, but I don't really use it as much, like... I never post anything, I never do anything on it and I feel like it's a bit... I've thought of closing my account because I don't really see how relevant it is in my job industry, but I still, I'm still keeping it. But I've never heard of any of the alternatives that you mentioned. For Facebook I went to WhatsApp before it was, you know, bought by Facebook (laughs) because they had, like, a better encryption than Messenger, but then it was bought by Facebook.

T: (laughs)

A: Instagram was also not Facebook's, but it was bought by Facebook a couple of years back and it has since really become a much worse app.

T: Yeah.

A: So, in that sense, um, yeah. I haven't really looked into any of these mentioned alternatives.

T: And any other maybe?

A: Yeah, besides WhatsApp as an alternative to Messenger for this particular reason of, like, double encryption and so on. Uh, but then it was bought by Facebook, so I guess that kind of...

I know there's Telegram, that's apparently one of the best messengers out there for, with like, encryption wise and privacy wise, but I don't use it. Marko uses it.

T: Yeah. Ok. Are there any other ways that you inform yourself about data disclosure on any of these SNS such as reading blog posts or articles about data protection, discussing with friends or reading the laws and regulations or anything else?

A: Um, I mostly read articles. So, I'm quite up to date in regard to what's happening, like all these data breaches that have recently happened, for example, Facebook specifically. So, I do, I've read a lot of articles, even like 'here's how to quit Facebook' for example or 'how to switch to another social media' or 'what to do to fully close your account' because I was thinking of stuff like that. And then I thought, you know, I will lose all these connections. I really use Facebook Messenger a lot, you know. And I can't expect everyone to switch to another Messenger just because it's me, so it's a bit, like, you're in it without wanting to be in it.

T: Ok. Um, so, do you feel that the privacy of your data is protected by Facebook?

A: No.

T: Why not?

A: Because of all the data breaches that they've had. Well it wasn't just a breach, right. Some of it was just literally them sharing some data with third parties that they shouldn't have shared. So, it's obviously like a conscious decision being made, like conscious decisions being made somewhere in the back. A lot of these policies, like, there's always like a front side and that's made, you know, public in a way, and there's always a lot that's happening, like, uh, in these grey zones. In the sense that a lot of things have double meaning and I think that a lot of these policies are deliberately a bit vague so that they can be exploited in other directions if needed. If, you know, Facebook is free, but they earn a shit-ton of, pardon, I shouldn't say shit-ton.

T: That's alright, you can say that.

A: A lot of money. They earn a lot of money for like a free app. So, they obviously have to go down the marketing route and, and...

T: Monetise.

A: Yeah, exactly. Capitalise on this whole thing. They're capitalizing on the marketing aspect, on the demographic that they have, and they can share all of this. Because they have a, because that's what they have. From a sociological standpoint they have a huge demographic, like a different, many, many different demographics, demographics that they can share with third parties and that can be used in, in any type of promotional purposes for any product or

anything... By product I don't necessarily mean a physical thing, but anything that can sell and, you know, earn money.

T: Mhm. And do you feel that the privacy of your data is protected by Instagram?

A: Well, no, but I'm less concerned about it because of what I use it for. Instagram is Facebook, so I presume it's the same thing.

T: And LinkedIn?

A: I honestly don't know. Is there an answer where I can say I don't know? Because I don't know. I don't really understand LinkedIn as much. I haven't really looked into it as much as I should've maybe.

T: Mhm.

A: Because I don't use it.

T: Um. So now, for the next several questions we are going to pretend that I am a new user of each of the SNS and I will ask you for advice.

A: Mhm.

T: So, let's start with Facebook.

A: Ok

T: Can I trust that Facebook will not use my data for other purposes?

A: No.

T: Why not?

A: Because of what I said before. Because Facebook will, uh, definitely have very vague privacy policies that will misguide you in a way. It will feel as if though you can share very, very private moments, but they will actually, potentially, be exploited. Also, Facebook has a lot of private groups that, you know, Facebook personally doesn't control, but the way it's made you can easily make a private group that they cannot put down that's, for example, focused on taking photos of other people that are of children, paedophilic and so on. Like, Facebook is notoriously known for that huge problem and they're trying to crack down on it, but it's a big problem because of the private aspect of each of the group that can be made. So, there's that and there's also Facebook as a corporation where they have these vague policies where they and, um, use a lot of sponsored material. Use like a lot of your own personal demographic that you've put up willingly, they use it for sponsored material and so you don't really where it goes and how. I mean, you don't know, that's the thing. You don't know. It's not like, oh, I'm gonna show up with this particular company that's gonna advertise things to you. They kind of assume a lot of things based on my gender and the things that I've liked and so on, based on the things that I've googled, uh... All of these sponsored posts appear just because I've googled something or... So, it's, it's very instant. It does not take any time at all for one thing to result in another thing, to result in a sponsored post, so obviously, you know my data is constantly being shared, so yeah.

T: And do you think that they would share your data with third parties without your consent?

A: Well, yes, because they have, right? I mean, the whole, what was it called, oh my god? There was a scandal and Mark Zuckerberg even went to trial and he was horrible at it.

T: The one it 2017.

A: Yes. What was it called? The guy with the pink hair? It was in the UK, like, that UK company. They shared data with... Anyway, I can't remember. There was a whistle blower from the company. Anyway, obviously it happened and there was a scandal, and nothing was done really. So, yeah.

T: Ok. Can I trust that... No, sorry. Will Facebook be honest in its dealings with me?

A: What do you mean by dealings?

T: Yeah. In, in, in kind of like relationship... In whatever, mm, in my interactions with Facebook, hah (laughs).

A: (laughs)

T: Wait. Oh, it's late, I'm sorry.

A: I know, I know.

T: In the interactions that I have with Facebook and that Facebook has with me, can I expect that what they're telling me is honest (laughs)?

A: Well, I presume, I presume, no, no, I get it. I presume some of the things are in that very, very basic frontline type of sense. Like, for example, other users will not, like, if they say this is not gonna be visible to other users, it will not be visible to other users, but they are the ones that are connecting the (inaudible). In that sense, like, the front line is honest, like that's what it is. But like, deleting pictures, deleting stuff off of Facebook. Like that stuff never disappears, that just stays on there. Like, you delete your account and unless you go through the whole, like through the motions, like, apparently, it's like more complex than it should be, to fully, actually delete your account. Otherwise you actually just kind of freeze it.

T: Deactivate.

A: Yeah and then you can come back and everything. And the whole weird thing where people die, and Facebook still posts notifications in their stead sometimes like memories or something. That's just very weird. Sorry, I just remembered that's a very weird thing that Facebook does. So, yeah, I don't think, it's a very, like, I can't really give, it's maybe not a straightforward answer, but I would say that no they would not be as upfront with you as you would expect, like, it would seem that they're upfront with you, but they're really not.

T: Ok and should I trust Facebook in general?

A: Um, well no. But if you just use it for very basic stuff, that, you know, that...

T: Mhm.

A: Today it's very hard to go off the grid, you know, to go off the grid fully. To have this moment where you advertently without thinking and without consenting constantly share anything you do online. With someone, through someone, with one corporation to another for the purposes of marketing. Because, for example, I google stuff that, for example, I need for research and I will get sponsored posts right away. But it's very hard not to do that, so I guess my answer would be, no, but I'm still somehow not worried and I still use it. Which is very, very worrying now that I actually have to verbalise it (laughs).

T: (laughs) Now the same questions for Instagram. So, can I trust that Instagram will not use my data for other purposes?

A: I guess not, no.

T: And can I trust that Instagram will not share my data with third parties without my consent?

A: I honestly don't know. Like, Instagram has been taken over by Facebook, but I've honestly never looked into it. You know, like, Facebook was everywhere in that sense and I read the news and I'm up to speed with those things, but, like, one company owns the other, so I presume the same policies apply. Like, the same algorithm, not the same algorithm, but the same type of thinking.

T: Yeah, like a principle.

A: Yeah. Exactly. The same principle would be used. Exactly, that's the word. Thank you. So, I presume all of my answers would be the same just because of that, but I haven't actually looked into Instagram separately, but I have read about how it came to be bought by Facebook. I read an article about that and about WhatsApp as well because it was such a shame that Facebook ate up all of these companies and has a monopoly now. Umm, so yeah. My answer would be I don't know, but actually thinking about it, it's probably the same.

T: Ok, so you would also say that you wouldn't trust Instagram in general?

A: Well, yeah, as I said, I presume, like, in regards to data privacy I think it's really the same as Facebook, but since the application is different, you don't really share as much on Instagram as you do on Facebook. Even though people do post their whole lives on Instagram, that's true, so...

T: Well yeah, people post stories where they are and what they're doing...

A: Yeah, they do, they do. No, that's the thing. I don't really have a... Like, my Instagram is very niche, but I guess I would say all the same answers as Facebook.

T: And LinkedIn?

A: I don't know. I honestly don't know. LinkedIn is a mystery to me, I use it, but I don't really use it.

T: Would you say that trusting SNS impacts how much data you share?

A: Umm, well I think yes, yes. I think when you know, you know, when you kind of need to use them, but you know that they cannot really fully be trusted, you will try to share a bit less data if you can. Like, you will try to control it as much as you can.

T: Mhm. So, you are aware, obviously you are, we've talked about it, about the recent data breach scandals. Um, so, did any of these actually change your behaviour?

A: Um, well I did remove some of my... Even though I didn't really have a lot of personal details, like, on Facebook to begin with, but I was actually thinking about dropping Facebook all together, but as I mentioned, that was quite difficult for me because of why I use it and that's, like, connecting with people. And, I, I reduced like, the amount of things that I put up. I've never really used Facebook for posts, I was either liking things or sharing things I thought were, like, generally beneficial. For example, there's a protest that I am going to and I wanna share it or, you know, I wanna share an article that I find interesting and I think is, like, of value or whatever. So, it's not like private moments in general. But, yeah, I became really annoyed when people started posting my photos without my, you know... I mean, no one asks you, no one asks you 'can I post this photo?', but people, people just do it. But it is annoying to kind of, like, know what's up out there and you kind of want to control it. But then I don't really have,

these photos are, like, whatever. It's fine. I mean, I prefer them not being there, but it's whatever.

T: Mhm. So, do you know someone who has stopped using SNS?

A: Fully, no. I know people who have just stayed on Messenger, not really using Facebook, but that doesn't really mean that lot to be honest. So, no, I don't really know anyone.

T: And you said that you thought of stopping using Facebook because of the data?

A: Yes, yes, because I find it a bit annoying. I find that using something that I feel like I have no control over in a way is, you know, annoying and I don't like the feeling that I'm pressured into doing something, which we all are. We're, like, peer pressured into, not peer pressured in the classical sense, but generationally pressured. Like, that's the way people communicate these days. Like, I use Instagram for jobs, I use WhatsApp to communicate with my client, so you can't really escape it. You have to have these particular things, I guess. Accounts and so on.

T: Mhm. Ok, well, that's it from my questions. Do you have anything you would like to add?

A: Uh, no, I think I talked enough (laughs).

T: (laughs) Ok, thank you so much for participating!

A: Thank you!

10.6 APPENDIX F

Interviewee name: Yusuf

Age: 26

Sex: male

Nationality: Belgian

Location: Wommelgem, Belgium

Duration: 13” 45’

Date: 19.09.2019.

T: Ok, so, thank you for participating in this interview. I would just like to assure you that all of your data will be used anonymously and only for the purposes of this thesis.

Y: Thank you.

T: Ok, so do you use Facebook?

Y: Yes, I do.

T: And Instagram?

Y: Yes.

T: And LinkedIn?

Y: Yes, also.

T: Why would you say that you use Facebook?

Y: Uh, Facebook I use mostly for my artist profile, not so much for personal use. In the past I used it also for personal use, but over the years it shrank.

T: Do you also use it to connect with friends or?

Y: Yes, in the sense of Messenger, yes, but I don't really visit other people's profile or anything. Like, it's mostly to send messages, receive messages, maybe on Facebook look for events.

T: Ok. And why would you say that you use Instagram?

Y: Instagram only for my artist profile. I don't use Instagram for my personal life because it doesn't really interest me, but it's a very good tool that I use for promoting my music and my general music career.

T: And LinkedIn?

Y: LinkedIn I use mostly if I'm unemployed to look for jobs, to check out employers or courses.

T: Ok, great. How often would you say that you use Facebook?

Y: Um, every day, probably. Not much, like ten to fifteen minutes, but yeah, every day.

T: And LinkedIn, oh, sorry. And Instagram?

Y: Instagram also daily, same amount as Facebook approximately.

T: And LinkedIn?

Y: LinkedIn only when I'm unemployed.

T: How much do you... No, sorry. Do you know what types of data other people usually disclose on Facebook?

Y: I guess they disclose way more than they think they do.

T: Ok, in what sense?

Y: In a direct or indirect way. In terms of personal information, location data, photos, probably stuff that happens in their life.

T: Ok, and Instagram?

Y: On Instagram, not that much. Because it's probably more, it's more image based, so I don't think people don't use, put a lot of personal information on it.

T: Do you think that they don't indirectly, like, when you look at people's stories?

Y: Yes, but different kind of information. More what they are doing or what they are pretending that they are doing. Yeah.

T: And LinkedIn?

Y: On LinkedIn not so much because it's a more professional environment, I think. More related to their job and their career in general. I don't think they'll be posting what they're eating for breakfast.

T: And do you know what types of data you disclose on Facebook?

Y: Yes, mostly promotional material, music, photos of myself, links to my music. It's all pretty marketing related.

T: And on Instagram?

Y: On Instagram exactly the same, but more visual.

T: And on LinkedIn?

Y: Only career wise. My past experiences, job titles, courses that I did, everything related to my professional life.

T: Ok and when you think of privacy policies of SNS what is the first thing that comes to mind?

Y: Um, that it's a lot of text and that it cannot be trusted and that probably no one reads it either way.

T: And if you would think of a person that would read it, what would they be like?

Y: Very geeky. I actually know only about one person that read the whole privacy policy and he does privacy for the police, but overall, I don't think anyone reads it.

T: And what do you think would motivate someone to read it?

Y: I don't think that you can motivate someone to read the terms of agreement because they're way too long and very, um, very vague and in terms that most people don't really understand.

T: Mhm, um...Does the privacy of your data on SNS concern you?

Y: Well the privacy used to concern me, in the beginning when this was all just starting and I was very, like, very much trying to get people aware of it, but it's a thing you can't really stop, so... In the end you just give up and go with the herd.

T: Uh, ok (laughs). Did you ever look into any alternatives for these sites? If you want, I can name a few? Did you look into any alternatives?

Y: Uh, yeah. I've used Minds which is a platform similar to Facebook, but less centralised. People can't really pay much for exposure, whereas Facebook only really shows you stuff that's been paid for. It's not super advertisement based and it's more, like, community centred.

T: Mhm. So, why did you actually look into the alternative?

Y: Because, for... Because of the reasons that Facebook can't be trusted, in my opinion, same for LinkedIn and Instagram and there should be a good alternative, but at this point they can't really compete with Facebook.

T: Why would you say that?

Y: Because Facebook is dominating the Internet market.

T: Ok. Are there any other ways that you inform yourself about data disclosure on SNS, such as reading blog posts or articles, discussing it with friends or reading laws and regulations?

Y: Uhh, if something pops up, I'll read it, but I don't actively search for it because it just makes you feel bad because you can't stop it and... So, why focus on something you can't change anyway?

T: Mhm. And uh, would you say that you're well informed?

Y: I think I know, I think I know... I think I know a thing or two more than other people because I've actually used the systems that Facebook uses for my artist profile. I've used the advertisement system which I think is, like, total spying. Facebook, like, really know everything about you in a few clicks they know which music you like, what pages you visited, what, what you like doing in your free time. And if you're the advertiser, in my case, me, for my music, it's very beneficial, but also very creepy.

T: Mhm. And do you feel that the privacy of your data is protected by SNS?

Y: No, not at all. I think there has been a lot of breaches, uh, proofs of breaches and similar stuff that happened that proves it's not protected.

T: For the next several questions we are going to pretend that I am a new user of each of the SNS and I will ask you for advice. So, let's start with Facebook. Can I trust that Facebook will not use my data for other purposes?

Y: No. They've proven in the past already that they can't be trusted.

T: Do you think that I can't trust Facebook that it won't share my data with third parties?

Y: I think you'll have your consent in terms and agreements, but I don't think anyone reads them, so no, but you should actually know.

T: And do you think that they will be honest in their dealings with me?

Y: Same answer, no. I think that if you actually read and understand all the terms, then yes. But it's so not understandable that, probably not.

T: So, you don't think that they're transparent and that they clearly communicate?

Y: No, definitely not.

T: And do you think that I should trust Facebook in general?

Y: No, absolutely not.

T: Ok. Now the same questions for Instagram.

Y: Also, same answers because Instagram is owned by Facebook.

T: And LinkedIn?

Y: Though, I don't really know that much about LinkedIn.

T: Ok, if you could which one of these three you trust the most and which one you trust the least, what would you say?

Y: Honestly, I think they're all in the same spot.

T: So, you would say that you trust none of them?

Y: No, I don't trust any of them because they make money of our data. That's like their main income to advertise and maybe even sell the data, I don't know. Probably happened.

T: Does trusting a SNS impact how much data you share?

Y: Sorry?

T: Does trusting a SNS impact how much data you share?

Y: Yes, now I don't share as much anymore, because I know our data might be misused and, in the past,, I was also younger so I didn't really think about it that much or didn't care, but now you grow up and... Well, yeah, you're kind of cautious about what you share online.

T: So, you are aware of any recent data breach scandals revolving around these SNS. Did any of these change your behaviour?

Y: Um, yes, I am aware of them. No, my behaviour already changed before the data, ale, before the known data breaches because there were probably some data breaches that get covered up very well. I already, like, after reading some articles and blogs, I already had the sense that social media in general is not to be trusted, so that really limited what I would share online.

T: Ok. Do you know someone who has stopped using SNS?

Y: Yeah, a few people.

T: And what do you think motivated them to do it?

Y: Not data breaches or disclosure. More personal reasons. Like trying to live a more offline life because you get really sucked into it and you start to live, you start to live your life for likes and for validation from other people. And I think more and more people are starting to become aware of that and don't want to live their life like that because it has proven in the past, by studies now, that it can actually make you really depressed or not feel good about yourself because you constantly see other people's lives glorified. Like 'hey, look what I'm doing', but they'll never post the bad stuff and the people feel like their life should be more perfect while no one's lives are perfect. But they try to pretend on social media that it is.

T: And have you ever thought of stopping using SNS?

Y: Well, if it wasn't for my artist profile, I would've probably already deleted everything. It's just a very valuable tool in promoting my music, in promoting my career and that's what keeps me locked into it, so to say. But I do try to not use it for personal use, apart from my career. I have actually tried to delete my profile, before I was making music. But it's, one, for starters, really hard to find how to delete it and also it gets reactivated like in an instant. Like, for example, I use Spotify and I deleted my Facebook account. And then when I logged into Spotify my Facebook account got reactivated because it's linked together, and I emailed Spotify customer service to check how I can delink it and it basically was a whole hassle. Like I would have to delete my Spotify account, lose all of my music, all of my playlists and make a new one that isn't linked to my Facebook account. So, they make it really hard for you to actually delete your Facebook account. Also, you have much websites which have log in with Facebook and don't really offer much alternatives. They make it really hard. They make it really a necessity to have Facebook.

T: Thank you so much, those are all of my questions. Do you have anything you'd like to add?

Y: No, not really.

T: Ok. Thank you!

Y: Bye, bye!