Karri Haapaniemi

PRIVACY POLICY FACTORS: THE EFFECTS ON USE CONTINUANCE IN SOCIAL NETWORKING SERVICES

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Haapaniemi, Karri
Yksityisyyskäytäntötekijät: Vaikutukset käytönjatkuvuuteen sosiaalisissa verkostoitumispalveluissa.
Jyväskylä: Jyväskylän yliopisto, 2022, 86 s.
Tietojärjestelmätiede, pro gradu - tutkielma
Ohjaaja: Woods, Naomi

Kaikilla sosiaalisilla verkostoitumispalveluilla on palveluntarjoajan luomat yksityisyyskäytännöt. Ne kertovat käyttäjille, miten palveluntarjoaja kerää data käyttäjistä, mitä dataa kerätään, miten sitä säilytetään ja miten palveluntarjoaja käyttää kerättyä dataa. Käyttäjän on hyväksyttävä palvelun yksityisyyskäytännöt, mikäli hän haluaa käyttää palvelua. Yksityisyyskäytännön vaikutukset käyttäjän yksityisyyteen voivat kuitenkin muuttua, kun palveluntarjoaja tekee muutoksia yksityisyyskäytäntöihinsä palvelun käyttöönoton jälkeen. Tämä vaikutus voi olla joko positiivinen tai negatiivinen. Jos vaikutus yksityisyyteen on negatiivinen, se pakottaa käyttäjän uudelleenarvioimaan yksityisyyskäytäntöjen ehdot ja päättämään haluaako hän jatkaa palvelun käyttöä, yksityisyyttä heikentävästä vaikutuksesta huolimatta, nauttien edelleen palvelun hyödyistä vai lopettaa palvelun käyttö negatiivisen vaikutuksen takia ja menettää palvelun hyödyt. Käyttäjän käytönjatkamiskäyttäytymisen ja -päätöksenteon ymmärtäminen on tärkeää niin yksityisyyskäyttäytymisen näkökulmasta, jotta pystytään tukemaan käyttäjiä, kuin palveluntarjoajan tukemisen näkökulmasta, jotta kyetään avustamaan palveluntarjoajia palveluiden menestyksen takaamisessa. Aiempi tutkimus on löytänyt joukon tekijöitä, jotka vaikuttavat käytön jatkamisaikomukseen erilaisissa konteksteissa, mutta yksityisyysselkkausten kontekstia ei ole käsitelty aiemmassa tutkimuksessa. Tässä tutkimuksessa kehitetään tutkimusmalli, jolla pyritään tutkimaan ja ennustamaan käytönjatkamisaikomusta yksityisyysongelmien kontekstissa yksityisyyskäytäntöihin liittyvien tekijöiden ja aiemman tutkimuksen löydösten perusteella. Tutkimuksen kvantitatiivinen data kerättiin kyselytutkimuksen avulla. Analyysin tulokset osoittavat, että yksityisyysongelmien kontekstissa vaaditaan erilaista lähestymistapaa käytönjatkuvuuden ennustamiseen kuin tavallisen käytön kontekstissa. Tulosten mukaan luottamus palveluntarjoajaan ja yksityisyystietoisuus ovat käytönjatkuvuuteen vaikuttavia tekijöitä tässä kontekstissa. Nämä tulokset tukevat tutkimusta ja käytäntöä sillä ne osoittavat yksityisyysselkkausten erilaisuuden verrattuna muihin aiemmin tutkittuihin konteksteihin. Sosiaalisten verkostoitumispalveluiden tarjoajien tulisi huomioida nämä tulokset pohtiessaan, kuinka he käsittelevät ja tiedottavat käyttäjiään yksityisyyteen ja yksityisyyskäytäntöihin liittyvissä aiheissa.

Asiasanat: yksityisyys, yksityisyyskäytäntö, käytönjatkuvuus, sosiaaliset verkostoitumispalvelut

ABSTRACT

Haapaniemi, Karri
Privacy Policy Factors: The Effects on Use Continuance in Social Networking Services.
Jyväskylä: University of Jyväskylä, 2022, 86 pp.
Information Systems Science, Master's Thesis
Supervisor: Woods, Naomi

All social networking services have a privacy policy created by the provider of the service. It informs users of the data collection, storage and use by the service provider. Users have to accept the terms set in the privacy policy in order to use the service. Changes made to the privacy policy during long term service use can however change the way the privacy policy affects user's privacy. This effect can be either positive or negative. If the effect is negative, it forces the user to re-evaluate the terms of use and whether they would like to continue using the service despite the reduction in the level of privacy still enjoying the benefits of the service or abandon the service due to its negative effect on privacy and lose the benefits of the service in the process. Understanding the use continuance behaviour and decision-making of users is important in terms of both privacy behaviour to support the user as well as assisting the service providers in ensuring long term success of their services. In this study a literature review is conducted into the topics of privacy, privacy policies and use continuance. Previous literature has shown that there are various factors that affect use continuance intention within different contexts. However, the context of privacy incidents has not been addressed. In this study a research framework has been developed to examine and predict the users' use continuance intention in the context of privacy incidents based on privacy policy associated factors as well as factors identified in existing use continuance literature. A survey study collected quantitative data for purposes of the analysis. The results suggest that privacy incidents as a context require a different approach to predicting use continuance than regular use contexts. Trust and privacy awareness are confirmed to be affecting factors in use continuance in this context. These results have implications for research and practice as they highlight the disparity of the privacy incident context in comparison to other contexts studied in previous literature. For practice the results of this study should be taken into account when SNSs providers consider how they address and inform their users about privacy and privacy policies.

Keywords: privacy, privacy policy, use continuance, social networking services

FIGURES

TABLES

CONTENTS

1 INTRODUCTION

Internet has changed over time from the network, which mainly connected universities for the purposes of researchers sharing information, to the complex system it is today. Initially, internet was used by researchers to communicate their findings and other scientific information. After the search engines made internet accessible to everyone and enabled for example e-commerce the nature of Internet changed. In addition to providing a search engine to make internet use less demanding and simultaneously enabling ecommerce, Google changed service providers' approach to financing services they offer to the users. Instead of asking a fee for access rights many services are currently financed by targeted adds. However, in order to be able to effectively target adds, websites and services need data about their users. This has led to the current situation where vast amount of personal information is exchanged between different operators.

The growth of social network services and blogging has increased the amount personal data available online making gathering easier for companies. As the latest development, relating to personal information disclosure by users, the adoption of the smart phone has allowed users to ubiquitously use apps. These small applications have again revolutionised the use of internet and further increased the amount and quality of personal information collected. (Camenisch, 2012) These changes have made information one of the biggest businesses in the modern era. It is also connected to the growth of the service industry which thrives on information and data gathered on the customers and users as it allows services to be delivered more effectively. (Wacks, 2010) However, as the Internet was designed to be an open environment with little security in mind, privacy protection was also not considered in the early stages. After all, it was initially meant to be a communication channel for researchers. The openness provided by this design allowed the growth of Internet but at the cost of security. The limited protection is very apparent in the modern society as new privacy incidents and breaches are frequently reported. (Camenisch, 2012)

Internet has made it effortless for users to communicate with others. Sending messages via messaging services and interacting with one another in social networking services (SNSs) are daily events for many users. (Camenisch, 2012)

By definition, SNSs are services that gather information on user's social contacts, simultaneously construct interconnected social networks and reveal these connections to other users as well (Adamic & Adar, 2003). While users often have a very clear idea who they want to receive the data and information they send, they cannot be sure that the intended receivers are the only ones having access to them. Users have limited possibilities to control who in the end receives their data and to identify all the additional parties who might also have access to it. (Camenisch, 2012) This sets their privacy at risk. Privacy can be defined as the ability to reach preferred levels of solitude, intimacy, anonymity, and reserve in the current context. (Buckner and Knowles, 2012)

In this insecure environment organisations such as service providers utilize what is called a privacy policy to gain the trust of users. (Wu, Huang, Yen & Popova, 2012) Privacy policy refers to a statement providing information on how personal and sensitive information is handled and what information is collected (Gerlach, Widjaja & Buxmann, 2015). In digital services, users control and manage the handling and collection of their personal data by accepting or declining these privacy policies (Pratt & Conger, 2009). Essentially, this sets the rules by which the service provider can utilise user's data (Gerlach, Widjaja & Buxmann, 2015).

All individuals should have the right and the means to control their own lives. For this to be achieved two conditions need to be met: a capacity for intentional action and independence of controlling influences. In social media and other digital services individuals make the decision to disclose their personal data. Making the decision should be based on the principles of informed consent. (Custers, Van Der Hof & Schermer, 2014) The behaviour of users is however affected by various factors from the perspective of privacy behaviour (Child, Haridakis & Petronio, 2012; Acquisti & Gross, 2006; Bechmann, 2014; Dowding, 2011) as well as privacy policy behaviour (Custers, Van Der Hof & Schermer, 2014; Gerlach, Widjaja & Buxmann, 2015; Obar & Oeldorf-Hirsch, 2020; Bechmann, 2014), which may cause individuals to act in an unsafe manner.

1.1 Research gap

There is a clear difference between the interests of users wishing to protect their personal data and service providers interested in utilising that data in their business activities. When users identify issues regarding the privacy practices or policies, there can be severe consequences to service providers in the form of legal action or users abandoning their service. However, even after the issues emerge some users may continue to use the service. (Gerlach, Widjaja & Buxmann, 2015) There are several models that explain use continuance behaviour and among the factors are security and privacy (Oghuma, Libaque-Saenz, Wong & Chang, 2016; Bhattacherjee, 2001). Use continuance refers to the continuing use of an IS product or service past the initial adoption. (Bhattacherjee, 2001) The research has not focused on the privacy policy change related aspects of use continuance despite

the problem of users continuing service use after privacy issues emerge described by Gerlach, Widjaja and Buxmann (2015). Kari, Salo & Frank (2020) state in their recent study that the overall the aspect of privacy incidents in services has not been sufficiently studied regarding user behaviour. This is the research gap targeted by this study.

The aim of this study is to first discover how research could be conducted into how much privacy and privacy policy issues affect use continuance in the context of social networking services (SNSs) and privacy incidents. Additionally, the related factors are to be further studied to determine other influencing factors. Based on the findings an empirical study will be conducted to test the theorised model. The results of this study aim to extent existing use continuance literature by providing more detailed information on the privacy aspects of it and by providing a research framework to be then used in an empirical study. The corresponding research question to these aims is:

- Which privacy policy factors affect use continuance in case of a privacy incident?

1.2 Methodology of the Literature Review

The chosen research method for the first part of the study is literature review. Google Scholar and Jykdok are used as the main search engines to discover relevant literature supported by Google search when necessary. The key words used in the search are “privacy”, “privacy policy”, “use continuance”, “use continuance intention”, “privacy behaviour”, “SNS”, “social networking service”, “data collection”, “privacy disclosure” and “Use continuance model”. These keywords are combined, adjusted and used alone during the search process. Additionally, the keywords are to be later combined with terms appearing from the literature findings to ensure a thorough review of the literature.

The articles are selected based two main criteria. First, the year of release is considered to ensure that the information and results in the literature are up to date. Due to the limited amount of research on use continuance in privacy context the desired range of publishing is set to be between 2010 and 2022. Certain literature does not meet this requirement but is used nevertheless as they are considered to be foundational to the topics discussed or provide useful insights. Second, articles which have been cited more frequently are preferred when possible.

Findings of the literature review will be evaluated and compared to provide insights into the topic of this study. The goal is to identify the relevant factors and aspects of use continuance and privacy topics to enable further analysis. The literature review will result in a research framework being constructed that will then be utilised in the empirical part of the study.

1.3 Structure of the study

The content of the study is as follows. First, the topic and concept of privacy in SNSs will be introduced and defined along with privacy behaviour related factors and theories. Second, literature on privacy policies and behaviour related to them will be analysed to provide further insight. Third, the topic of use continuance in information systems will be reviewed. This includes definitions and models, which will then be used in the next section. Finally, the research framework will be constructed based on the reviewed literature. This concludes the theoretical part of study.

The empirical part of the study is organised as follows. First, the methodology of the empirical study will be introduced in detail. This includes both the pilot study as well as the final study. Second, the analysis results will be introduced in a dedicated section.

Finally, the results of the analysis will be discussed. This includes their implications for the research framework itself as well as for practice and theory. The analysis also provides other observations which are discussed to provide more insights for future research. Limitations of the study are also reviewed to present the degree of criticality by which the results should be taken into consideration.

2 Privacy in Social Networking Services

In this chapter privacy will be discussed in the context of SNSs. First, the definition of privacy will be discussed in more detail compared to the definition provided in the previous chapter. Data collection is then presented as it is a common phenomenon in SNSs, which undeniably affects privacy (Bechmann, 2014). This includes the reasoning why service providers engage in such activities, the potential issues of data collection and how this affects users. To further elaborate these topics relevant studies regarding Facebook (Tuttle, 2018; Conger, 2009; Nyoni & Velempini, 2018; Riesch, 2012) will be reviewed. In a dedicated subsection the privacy behaviour of users will be discussed to create understanding on why users disclose personal information. Finally, a model, explaining privacy disclosure, by Xu, Michael and Chen (2013) will be presented. The objective of this chapter is to demonstrate the issues related to privacy in SNSs and to introduce the reasons for privacy disclosure in these services.

2.1 Definition of Privacy

Everyone has an idea what privacy is but defining it explicitly is a more difficult task. In the modern era privacy is paradoxical concept (Bechmann, 2014). While individuals want privacy, they at the same time desire or need convenience, discounts or services. The relationship between these two sides is called the privacy paradox. It creates a requirement for discussing privacy in context. In order to carefully define privacy context must always be taken into consideration. (Bechmann, 2014; Moore, 2008)

This means that over time it has had multiple definitions due to the changing circumstances. For example, privacy in pre-computer era had a different meaning than it has today. In addition to this, multiple disciplines utilise the concept, including philosophy, anthropology, political science, and communication science, and have debated over its definition. (Dowding, 2011) Based on the work by Buckner and Knowles (2012), it can be said that privacy is deteriorating in modern era. They identified technological innovations and advancements as the cause of the privacy control issues (Buckner & Knowles, 2012).

Social networking services and other new information and communication technologies have complicated the matter of defining privacy as the line between public and private has become blurred. The attitudes of individuals towards privacy and privacy practices have also changed due to these new services and technologies. In summary creating a single definition for privacy is not feasible as context has a significant impact on the meaning of the concept. (Dowding, 2011) This is also supported by the views of Moore (2008) who, after defining privacy, states that the provided definition will likely not satisfy everyone, and that privacy should be defined based on the context of the study in question. It has been

suggested that the term privacy should be avoided due to its vague nature and focus on the specific activities instead utilising a taxonomy approach (Solove, 2008). However, for the purposes of this study privacy has to be defined in order determine the factors that can be affected by privacy issues created by privacy policies.

One of the earlier definitions for privacy can be found in a book by Westin (1967). According to the definition, privacy is a person's withdrawal from society through physical or psychological means. An important aspect of this is that the withdrawal is voluntary and temporary. Withdrawal can also be either physical or immaterial. Westin (1967) uses clothes, walls or spatial distance as examples of physical withdrawal and choosing not to disclose certain information as an example of immaterial withdrawal. Wieringa et al. (2021) align their definition of privacy with Westin's (1967) definition. In their data analytics focused study, they define privacy as information privacy or the access to personal data which can be used to identify the individual. Both of these definitions are however lacking in terms of addressing the contextual nature of privacy discussed in the previous paragraph. As for the definition by Wieringa et al (2021) this can be justified as they only needed to define privacy in the specific context of data analytics. (Wieringa et al., 2021)

As mentioned, Moore (2008) provides a definition for privacy from the perspective of rights and, similar to Westin (1967), includes the physical and psychological perspectives to the definition of privacy. Privacy can be defined as the right to maintain control over and limit access to the more personal information regarding oneself and access to one's body, capacities and powers. However, it also includes the right over the use of the before mentioned. Even though access would be granted, the subsequent use of personal information for example is not justified without the permission of the individual. (Moore, 2008)

Prior to Moore (2008), Kang (1998) defines privacy in a similar fashion by including the aspects of physical space and control over processing of data. Kang (1998) refers to physical space as individual's territorial solitude which should not be invaded by unwanted objects or signals. The definition however includes a third aspect which is the ability to make decisions without interference. This is an interesting point of view to privacy, and it is utilised also by Buckner and Knowles (2012).

Regarding defining privacy, Buckner and Knowles (2012) refer to a number of authors who have attempted to form a definition. Some of them equated privacy with control of information disclosed to others about you in terms of what, when and how much. Overall, they conclude that there are differences between the definitions they reviewed, and no consensus can be found. They identify the cause of the differences to be the contextual nature of privacy. Even for an individual person privacy can have different meanings in different contexts. However, despite the difficulty of defining the concept, in order to assess privacy and study the topic it must be defined in context. Buckner and Knowles (2012) form their own definition of privacy for the purposes of their study. They define it as allowing individual with the degrees of solitude, intimacy, anonymity and

reserve they want. There are however some considerations associated with the definition. First, social context must be considered. The degrees of solitude, intimacy, anonymity and reserve are also not static even for a specific individual. There can be contexts where the individual seeks solitude while ignoring it in others. Additionally, the privacy related choices made by the user earlier should not impact the future decisions they make about privacy. After these considerations are added to their definition it takes the form:

> *"The ability of individuals to realize desired levels of solitude, intimacy, anonymity, and reserve in any given situation without impacting future desired levels."* (Buckner and Knowles, 2012, pp. 86)

While the above definition is made for a study on the legal context of privacy, it has implications to this study. It highlights the individuals' right and at the same time the need for individuals to define the concept of privacy themselves. It provides a clear frame to what privacy is. Additionally, it applies well in the context of online SNSs as SNSs set a social context which sets it apart from other environments.

As mentioned in the definition by Buckner and Knowles (2012) there are four dimensions to privacy. Interacting with others always has potential to affect our privacy in terms of solitude, intimacy, anonymity and reserve. Positive experiences with interaction may even lead to the desire to reduce the degree of solitude and increase interaction at the expense of privacy. Similarly, negative experiences will lead to desire to increase the degree of solitude. Interactions with close friends, family and romantic partners often involve intimacy and if there are intentional or unintentional violations to the boundaries of the interaction there can be significant consequences to trust between involved parties. (Buckner & Knowles, 2012). Regarding the topic of this study, this implies that if a user has a negative experience with an SNS may therefore wish to increase their privacy on some or all dimensions. If the privacy policy does not allow sufficient increase in the opinion of the user, it will result in the user attempting to reach the desired level in another way. Whether this way is reducing the amount of use, information disclosure or the complete termination of use is most likely dependent on the issue at hand, which is the topic of this study.

There are also four perspectives to privacy that explain the value it holds for individuals. Psychologically, a private space is at least occasionally required by people. In that space they can be themselves and not worry about opinions of others. Sociologically, there is an inherent need to be able to behave, interact and express oneself without being observed and constrained by the circumstances. Example of a circumstances where the social dimension of privacy was invaded is the countries behind the Iron Curtain during the Cold War. Economically, lack of privacy can reduce innovation as innovators feel that their ideas and projects are at risk of being stolen. Finally, politically there needs to be freedom to think, argue and act on political opinions. The feeling of not having privacy can undermine free speech and behaviour. (Healey, 2012)

Privacy can also be divided into types. Privacy of the Person addresses the integrity of one's body. In the context of this study the most relevant aspect of this type is the submission of biometric measurements as in some services fingerprints or facial recognition are used to identify the user. This is however not common in SNSs. In other contexts, this covers topics such as requirement of consent to medical treatment. Privacy of Personal behaviour, also referred to as media privacy, is concerned with the privacy of religious practices, politics and sexual preferences. Privacy of Communications refers to the right to communicate with others without being monitored no matter which of the possible communication media is used. (Healey, 2012) Last type is the Privacy of Personal Data. It is also referred to as data or information privacy. According to it data about an individual should not be automatically made available to others without their consent. This covers even situations where the data is owned by another organisation or individual. (Healey, 2012) The two latter privacy types are addressed by this study, particularly the privacy of personal data. However, there are elements of the other two involved as well. When services collect biometric data about the user's privacy of the person can be at risk. Similarly, if communication in or their belonging to a religious group in an SNS is disclosed without consent the privacy of personal behaviour is at risk.

Burgoon (1982) identifies similar types to privacy. According to the findings physical privacy is the freedom from surveillance and unwanted breaches of personal space. This is comparable to Privacy of the Person by Healey (2012) which however does not include the freedom from surveillance. The second type by Burgoon (1982) is interactional privacy or control over social encounters and third is the psychological privacy which refers to the protection of one's thoughts, feelings, attitudes and values. These two types have no equivalent in Healey's (2012) collection of types. The fourth and final type by Burgoon (1982) is informational privacy meaning the ability to control collection, aggregation ad dissemination of information. This takes a different and deeper perspective to privacy of information and data but is comparable to the Privacy of Personal Data in Healey's (2012) types.

Dowding (2011) approaches the types slightly different than Healey (2012) and Burgoon (1982). According to Dowding (2011) information privacy is partly the establishment of rules to manage the collection and handling of personal data such as credit information and medical records and can also be called data protection. At the same time, it is also about preventing disclosure of that information to unauthorized parties. (Dowding, 2011) Based on this, privacy policy can be seen as an implementation of information privacy.

Related to privacy, transparency must be discussed. While it is desirable that the internet services would be transparent about the way they handle user data, there is another paradox associated with it. Without transparency the users do not know what data is collected, how is it distributed and who in the end has access. Yet, if all the information about user data flows within and outside services are disclosed to the users, there will be less transparency due to increased complexity and information overload. (Nissenbaum, 2011)

In the context of this study privacy is approached as a personal construct and not particularly closely defined as each participant has a different perception of what is privacy. What is import in this study is what type of privacy issues individuals see as an issue which would affect their personal use continuance. In short, privacy is defined in this study as the user's desired level of solitude, intimacy, anonymity and reserve regarding personal information they disclose in SNSs based on the above definitions; particularly the definition by Buckner and Knowles (2012).

2.2 Privacy and Data Collection

Extensive personal and sensitive user data collection is happening on SNSs (Bechmann, 2014). As mentioned, SNSs are services that gather information on user's social contacts, construct social networks based on this information and reveal the networks to other users as well. (Adamic & Adar, 2003) In these services users can create various types of information content in addition to connecting with others. For example, blogs, social networking sites and online sharing platforms are considered SNSs. A user of an SNS can have different roles, such as information creator, commenter or reviewer, in the community. (Chang, Liu & Shen, 2017)

The effort to gather this information is growing as it is beneficial to organisations (Qian et al., 2017). As mentioned, the information collected is used by companies to better target advertising and finance their services by doing so. (Camenisch, 2012) From the users' point of view, the data is also used for customer support and personalisation of services based on the users' constraints, needs and preferences (Carmagnola, Osborne & Torre, 2014). The data collection however raises concerns on users' privacy (Chen, Chiang & Storey, 2012).

The information is in some cases insufficiently protected which leads to the far too common privacy and security breaches. (Camenisch, 2012) Another issue from the perspective of the organisation collecting the data is balancing privacy protection and data aggregation. Data aggregation refers to the process of gathering and processing data to enable further analysis. (Qian et al., 2017) The data gathered however is usually already collected making data aggregation an indirect form of data acquisition. In its core aggregation is the activity gathering information about an individual. While a piece of information alone is not necessarily informative, combining multiple pieces can create a profile for the individual. Data aggregation relies on the synergies provided by combinations of data from different sources. When analysed the aggregated data can provide valuable new facts about the individual, who has not necessarily revealed such information about themselves. (Solove, 2006)

When the data aggregation is done in a way that effectively protects privacy of users, the data provides limited analysis possibilities. An example of this is when data is aggregated in a way that only allows summation preserving anonymity of the individuals whose data has been collected, the data does not

sufficiently support more detailed analysis types such as behaviour analysis. (Qian et al., 2017) This may lead to organisations using less privacy protecting aggregation methods putting users' personal and sensitive information at risk. In the context of this study risk is defined as the level of certainty of an event happening in relation to the impact of that event (Riesch, 2012).

On the internet users reveal personal information both intentionally, and unintentionally. When the data disclosure is unintentional it can be also unwilling if the user is not aware of the privacy policy (Camenisch, 2012). Users agree to the data collection by agreeing to end-user licence agreements or privacy policies. (Bechmann, 2014) It can be argued that, as users of a service are provided with a contract they agree to before using the service, the revealing of personal information is intentional in all situations. However, studies have indicated that users do not often read the privacy policies when signing up to digital services. In a study by Bechmann (2014) it was demonstrated to users what type of information third parties can retrieve on them based on collected data. The researchers were able to gain information on the users' networks of friends, newsfeeds, post feeds, likes and photos, groups they are included in, all the basic information including email and geographical data if enabled in the service by the user. Most of the participants, students, were not aware of the amount and detail of information that could be collected and retrieved by a third party. Surprisingly, the participants were not particularly disturbed by the fact that companies can potentially retrieve such data about them. Their primary concern was with their circle of friends instead of themselves. A common perception seems to be that younger individuals consider themselves merely as "numbers" to companies meaning that they are not personally threatened. The participants could also not imagine other risks than economic theft and photo-manipulation. (Bechmann, 2014) The number of participants in this study is low which leads to limited generalizability, but the results still demonstrate that there are clear issues regarding users' awareness of data collection and associated risks. Privacy policies and user consent will be discussed in more detail later in this literature review in a dedicated section.

Buckner and Knowles (2012) reach similar conclusion. According to them part of the privacy problem is that organisations such as SNSs providers are not being clear about their data collection and use, and this seems to be a preferred operating approach for organisations. The issue is that the user side is exchanging potentially personal and sensitive information for a service and the provider side is not clear about the terms of the exchange. While the part that data is being collected and stored by the provider is clear parties, the issue is what happens to the data afterwards. This asymmetric relationship needs to be acknowledged by the parties involved. (Buckner & Knowles, 2012) This issue is further discussed and visualised in section 2.3.

In the future the issues regarding privacy may be emphasized by new technology and new type of services. The number of devices connected to the internet is rapidly growing and currently it seems in the future almost all devices will be connected to the internet. This means that the amount of data collected, processed,

and communicated will increase as well. Privacy protection is therefore more crucial in the future than it is currently. (Camenisch, 2012)

It has also been discussed whether privacy should be nowadays perceived and defined differently than in the past. The founder of Facebook, Mark Zuckerberg, has wondered if privacy is even necessary in the same extent in the modern era as it used to be. Yet, it cannot be ignored that many people believe in the concept of privacy as an ethical, moral and common-sense case. This view rises from the fact that disclosure of personal or sensitive information can have dire consequences for individuals. (Dowding, 2011)

According to Camenisch (2012) there are ways security and privacy could be achieved in the future. He lists three design principles that should be followed in future services. First, applications should not gather any other data than what is necessary for the parties involved to complete their tasks. Second, users should understand and be able to control the use of information they have revealed. Third, encryption off collected information both at rest and in transit should be mandatory. There are issues related to these principles. Camenisch (2012) mentions that these are often difficult to achieve and, in some cases, may contradict with the functional requirements. He uses access control without requestor identification and detecting denial of service attacks when communication is anonymous as examples of potential challenges. But as information is a profitable business to companies, it has been questioned whether privacy can be achieved sufficiently. (Camenisch, 2012)

2.3 Privacy and Data Collection Example: Facebook

Several studies have been conducted about Facebook regarding privacy (Tuttle, 2018; Conger, 2009; Nyoni & Velempini, 2018; Riesch, 2012). Due to this, the service will be used as an example of privacy issues and data collection in practice. This will allow the issues and perspectives discussed earlier in this section to be further described.

In 2014, a personality test was conducted on Facebook for the purposes of academic research. There was a privacy issue at the time in the terms of service and application programming interface (API). The app's developer had the right to collect information about the friends of the users who participated in the test. The function was later shut down in 2015. While this may seem like a breach to users' privacy, technically it is not. It is a violation to users' trust, but no part of Facebooks security measures were breached. Users agreed to this by accepting terms and conditions of Facebook. Facebook was aware that third parties were able to access such data but did not know that additional parties were also provided with the data. Additionally, while the participants of the study had the chance to identify this risk by reading the terms and conditions their friends had no idea their data was being collected. (Tuttle, 2018)

Conger (2009) created a model for information privacy on Facebook which is visualised in figure 1. This model describes the relationships between users,

operators and third parties. The main contribution of the model is the visualisation of the path of data from the user to third parties.

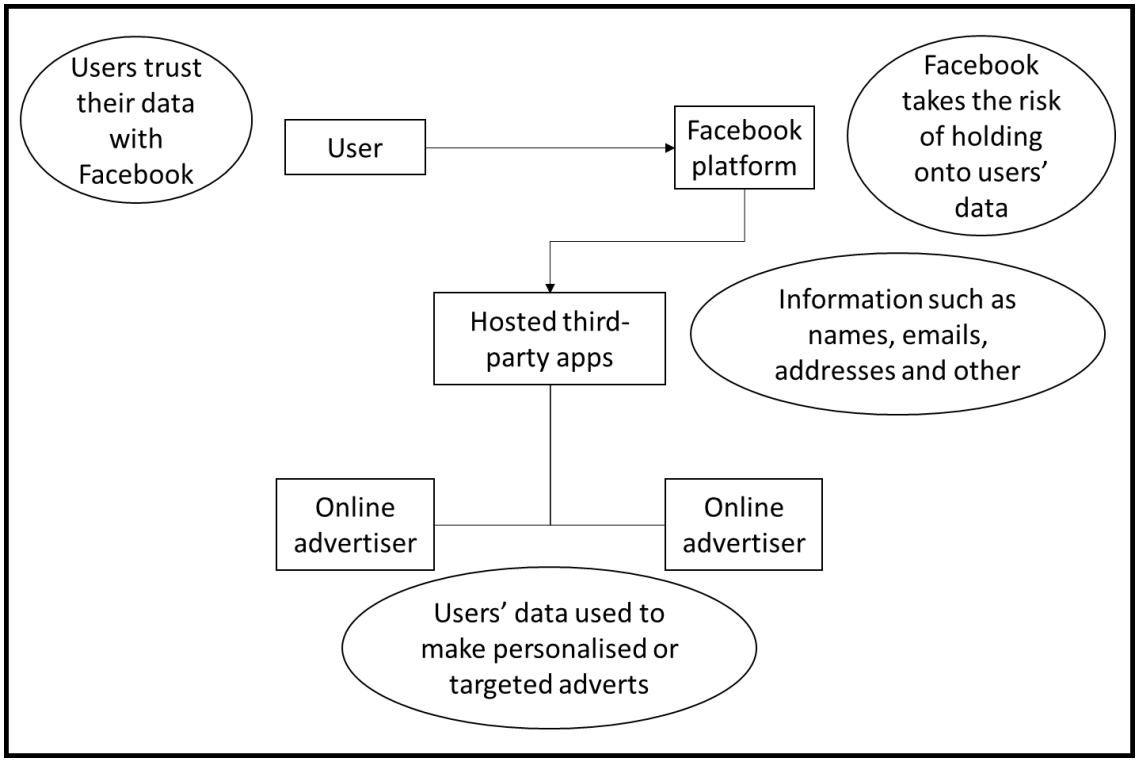

Figure 1 Information Privacy Model for Facebook (Conger, 2009)

In a study it was discovered that most users, in the study 67% or 240 individuals, have their personal data partially available and some, or 33% equalling 117 individuals, have their full personal details available on Facebook. This may be due to Facebook not blocking the visibility of personal details by default. While this makes it easier for users to view the information of others, it might reveal sensitive information depending on what the user shares. The data can be used to market products, various forms of deception or username and password mining. (Nyoni & Velempini, 2018)

The same study also revealed a need for users to be trained on the privacy settings on Facebook. For example, location data and other metadata can be misused by third parties. According to the study Facebooks privacy policy, at least at the time of the study, is not able to deal with the challenges to user privacy. Additionally, the privacy policy has other issues that will be discussed in the privacy policy section of this study. (Nyoni & Velempini, 2018)

For a point of reference, according to Riesh (2012) the threats associated with data disclosure on Facebook include profiling, scams and identity fraud, and surveillance and cyberbullying. Profiling refers to organisations such as advertisers and law enforcement agencies using user data to profile users. Various scams and identity fraud types such as account cloning and malicious users impersonating officials are common in Facebook. Riesch (2012) states that users may not be aware of the existence of these threats or their frequency.

2.4 Privacy Behaviour

Based on the uses and gratifications (U&G) perspective, people use social media to satisfy their needs and desires and are seen as goal directed, purposive and active. The perspective has been used in the study of media use and not just in the context of consumption but also in that of content creation and social interaction. (Child, Haridakis & Petronio, 2012). Thus, the relationship between privacy issues and social media use could be partially explained by the benefits the users perceive and to what extent the service fulfils their needs and desires. Communication privacy management theory (CPM) supports the views provided by the uses and gratifications theory (Child, Haridakis & Petronio, 2012). It breaks down the privacy and disclosure behaviour, similar to uses U&G theory, into before, during and after considerations. CPM views privacy management as a compromise between wanting to fulfil social needs by disclosing some private information in one hand and wanting to protect private information from others on the other. (Child, Haridakis & Petronio, 2012) Another relevant theory is the protection motivation theory (PMT) by Rogers (1975). PMT suggest that individuals base their self-protection behaviour on four factors that are perceived severity, perceived susceptibility, response efficacy and self-efficacy. Perceived severity is defined as the perception of how impactful the consequences of a risk would be. Perceived susceptibility refers to the individual's assessment of their personal likelihood of the risk. Response efficacy is the perception of how effectively an individual believes they are able to protect themselves from the risk. Finally, self-efficacy refers to the individual's confidence regarding the ability to adopt protective measures. (Rogers, 1975) These theories are commonly used in the studies on privacy and social media. They will be referred to later in this study.

Research has shown that individuals are guided in their privacy behaviour by cultural, gendered, motivational, contextual, and risk-benefit criteria. This includes both disclosure and protection behaviour. (Petronio, 2002) Based on this finding Child, Haridakis and Petronio (2012) suggested that the attitude and orientation would also be important factors in understanding privacy behaviour as they are connected to the combination of motivations and risk-benefit concerns.

User activity in an SNS is connected to different attitudes and behaviours as suggested in the previous paragraph. The behaviours can include involvement, attention and intentionality for example. In short people develop expectations about how useful media or content is in satisfying their needs and desires. The mentioned expectations also affect the choice and use of media. This also suggests that there are differences between individuals on how interested and involved they are in the use. (Child, Haridakis & Petronio, 2012)

The mentioned orientation can be divided into different types. The orientations reflect the activity, motives and attitudes of the user. The range of orientations is wide ranging from passive diversionary use to active and purposive utilitarian use. (Child, Haridakis & Petronio, 2012) This suggests that utilitarian orientation, where the service is seen as a tool of communication for example can

lead to different reaction regarding privacy issues in comparison to a hedonistic approach where the individual is simply looking entertain themselves.

Certain environments and circumstances can also cause individuals to act in a more unsafe manner. Child, Haridakis and Petronio (2012) state that social media related research has clearly demonstrated that social media use inherently includes varying degrees of disclosure and privacy management. SNSs tend to set the default privacy settings to minimal levels of privacy protection to support information sharing, which raises the need for users to configure their setting to ensure security of their personal information and establish their desired level of privacy. In their study they also suggest that further research in the privacy related decision making is needed, which supports the topic of this study. In their study on users' privacy behaviour in the context of blogging, Child, Haridakis and Petronio (2012) discovered that the users' background characteristics are an important predictor of media-use activity and therefore also affect the disclosure and protection of private information by the users. They suggest that in future studies a wider array of background characteristics should be considered. They also summarize existing literature and state that psychological differences, such as self-consciousness and self-monitoring, and demographic differences influence privacy management while blogging. Age is mentioned as an important demographic as different generations have different expectations of privacy based on their experiences and social influences. (Child, Haridakis & Petronio, 2012) Overall this suggests that there is a wide array of factors which may affect privacy management behaviour of the user. While the findings of Child, Haridakis and Petronio (2012) are in the context of blogging, they can be applied in other contexts as well, particularly in social contexts.

A study by Acquisti and Gross (2006) demonstrates issues in the privacy behaviour of Facebook users. While users care about their privacy, they are still willing to use Facebook and disclose personal information despite the obvious risks. However, the study also demonstrates that the users only have limited knowledge on the data disclosure patterns of Facebook. (Acquisti & Gross, 2006) The limited awareness could partially explain the unsafe privacy behaviour.

The findings by Dienlin and Trepte (2015) relate to those by Acquisti and Gross (2006). They study the existence of privacy paradox among the users of modern SNSs. Their results show that privacy concerns due not trigger specific privacy behaviours among users. There is no direct association between them. Users concerned with their privacy were not less likely to disclose their authentic name, phone number or political views on Facebook. The frequency of status posts is also unaffected by privacy concerns. They summarise their findings by stating that privacy concerns do not sufficiently predict privacy behaviours and conclude that privacy paradox is still a phenomenon in SNSs. (Dienlin & Trepte, 2015)

The findings by Dienlin and Trepte (2015) however have other interesting contributions. Attitudes are identified as a significant predictor of privacy behaviour. If the individual's attitude towards using authentic name on Facebook is that it is useful, they are likely to disclose it despite the privacy concerns. They

divided the attitudes and behaviours into three categories informational, social and psychological, which correspond to each other. In addition to this they also determine that attitudes indirectly affect behaviour through intentions. Overall, they conclude that attitudes are crucial for understanding privacy behaviour. However, they also state that while privacy concerns do not directly affect privacy behaviours, when operationalised properly, they have a meaningful role at explaining privacy behaviours. (Dienlin & Trepte, 2015)

Bechmann (2014) summarizes earlier work on privacy regarding Facebook. Facebook's default privacy settings have become more open over time, suggesting that the SNS desires to collect more information. In addition to this while users, particularly younger ones, seem to have started to care about their privacy and utilise the possibility to manage privacy settings, generally users do not actively choose privacy settings. However, according to Dowding (2011), younger individuals such as college students are more likely to behave in an insecure manner in terms of privacy. He argued that the reasons to this behaviour could be the more frequent use of new technologies and the fact that younger individuals are native to the technologies. In comparison, older users are generally more aware of the cost-benefit ratio of services. Additionally, younger users seem to be less aware of the risks associated with information disclosure or alternatively they perceive them to be less severe. (Dowding, 2011) This seems to be in conflict with the findings by Bechmann (2014). A potential explanation to this is the type of concern included in the studies. Bechmann (2014) states the concern of the users' regarding privacy is not towards how Facebook utilises their data, but about controlling the data their circle of friends sees, the reason for privacy control is different. Combining these findings, a conclusion can be made that while younger users are relatively unaware of the other risks associated with data disclosure as an activity, they control their privacy settings as they care about who sees their disclosed data as it risks their social image.

Overall, when questioned about the reasons for data disclosure Facebook users tend to refer to social reasons meaning that they want to interact with their friends (Bechmann, 2014). This relates to the risk-benefit approach mentioned earlier, that the users see sufficient value in the service to disclose information to the SNS provider. This view is supported by Rule (2007), who states that people seem to be willing to exchange private information for benefits. While the desire to have more privacy is obvious, an offering of time savings, convenience or comfort can make the users disclose personal information. (Rule, 2007) This topic is further discussed in association with privacy policies in the form of cost-benefit thinking.

2.5 Model of Privacy Disclosure

There are several models to predict privacy disclosure behaviour in literature (Xu, Michael & Chen, 2013; Ajzen, 1991; Culnan & Armstrong, 1999). As continuing the use of a service that has considerable privacy issues can be considered as

privacy diclosing behaviour on the part of the user, including the factors associated with privacy disclosure is important for the goals of this study. Xu, Michael and Chen (2013) suggested a model, visualised in figure 3, that could explain privacy disclosure behaviour and their findings supported their model. Combining the Theory of Planned Behaviour (TPB) (Ajzen, 1991) depicted in figure 2 and Privacy Calculus Theory (Culnan & Armstrong, 1999), the authors created an integrated model to explain privacy disclosure better than existing theories and models.

Privacy calculus theory is created by Culnan and Armstrong (1999) as a sidenote in their study. They discuss privacy and fairness and use the term "privacy calculus" to describe a phenomenon of individuals making assessments based on the economic or social benefit provided in exchange for their personal information identified in prior literature. Theory of privacy calculus contributed the direct privacy disclosure determinants of privacy concern and perceived benefit to model of Xu, Michael and Chen (2013). Privacy calculus has been used to predict privacy disclosure behaviour in online settings by other researchers as well (Keith et al., 2013; Krasnova, Veltri & Günther, 2012; Li, Sarathy & Xu, 2010) A common nominator for these studies is that they all build upon the privacy calculus theory by including cost-benefit calculations in their research frameworks. Privacy concern is also present in all of the frameworks, but its role varies. Keith et al. (2013) and Krasnova, Veltri and Günther (2012) use it as a determinant similar to Xu, Michael and Chen (2013), while Li, Sarathy & Xu (2010) apply it as a control variable.

TPB builds on the idea that intention causes individuals to behave in a certain way. Intentions reflect motivational factors that influence behaviour through them. They also indicate willingness to try and the amount of effort an individual is willing to exert. In the theory three factors affect intentions. Those are attitude towards behaviour, subjective norm, and perceived behavioural control. In this the attitude towards behaviour refers to the positive or negative mental stance the individual has towards that specific behaviour. Subjective norm is defined as the social pressure perceived by the individual to behave in a certain way in the given situation. Finally, perceived behavioural control is summarised is the individual's perception of how easy or difficult it is to behave in their desired way in the given context. (Ajzen, 1991)

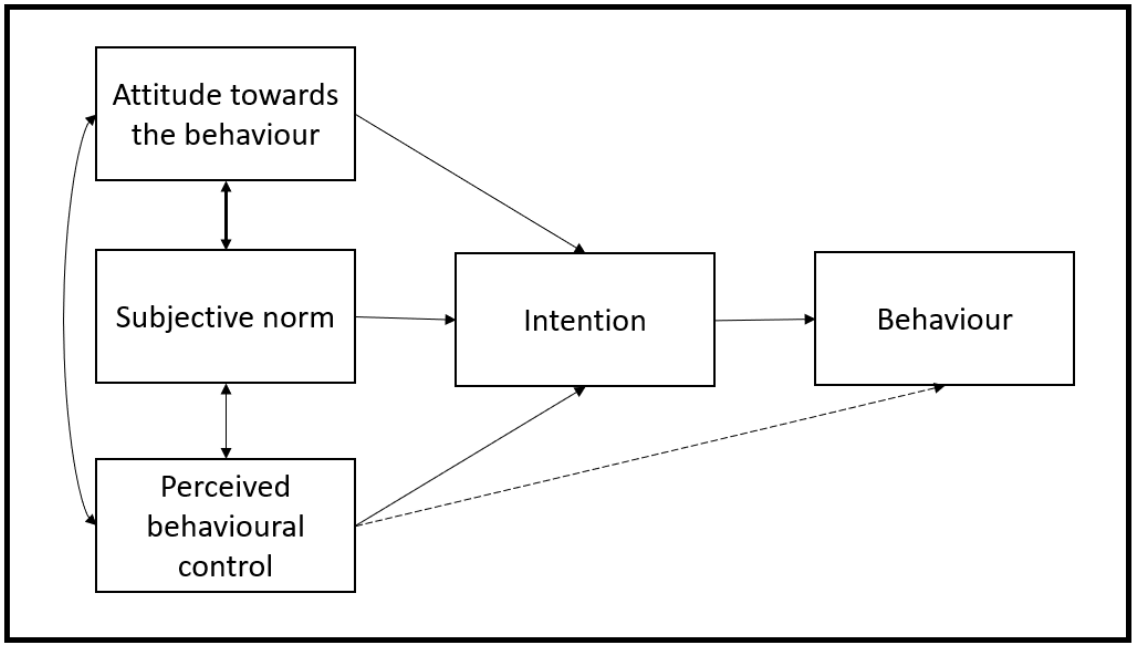

Figure 2 Theory of Planned Behaviour (Ajzen, 1991)

The latter relies on the fact that available resources and opportunities affect the likelihood of certain behaviour. In its core it is about the perceived ease of behaving in a certain way. (Ajzen, 1991) Ajzen (1991) also adds that it reflects past experience and expectations regarding the behaviour. Additionally, unlike the other two factors, perceived behavioural control and behaviour share a direct connection in some cases. If there are simply no resources to behave in a specific way intention will not form. Attitude towards the behaviour is defined as an individual's evaluation of the specific behaviour and to what degree it is agreeing or disagreeing towards that behaviour. The third factor or subjective norm refers to the social pressure associated with the behaviour. (Ajzen, 1991)

TPB allows the predicting and understanding of specific behaviour in context. Additionally, the three factors have high accuracy at predicting behavioural intention. (Ajzen, 1991) The theory has been used, applied and extended for a wide variety of topics from health (Milton & Mullan, 2012) and tourism (Quintal, Lee & Soutar, 2010) to ethical dilemmas of SNSs (Jafarkarimi et al., 2016) and in-app advertising (Cheung & To, 2017) explain the behaviour of individuals. More relevant to the topic of the study Xu, Michael and Chen (2013) the theory has been also applied, prior to their study, to predict online privacy protection behaviour (Yao & Linz, 2008; Yousafzai, Foxall, & Pallister, 2010). Findings by Yousafzai et al. (2010) provide limited support for the role of subjective norm but display significant support for the other two factors of intention.

Due to the proven usefulness of the TPB in predicting behaviour in various contexts the theory is utilized by Xu, Michael and Chen (2013) and provided the constructs of behavioural control, subjective norm and factors of attitude to create the remainder of their model.

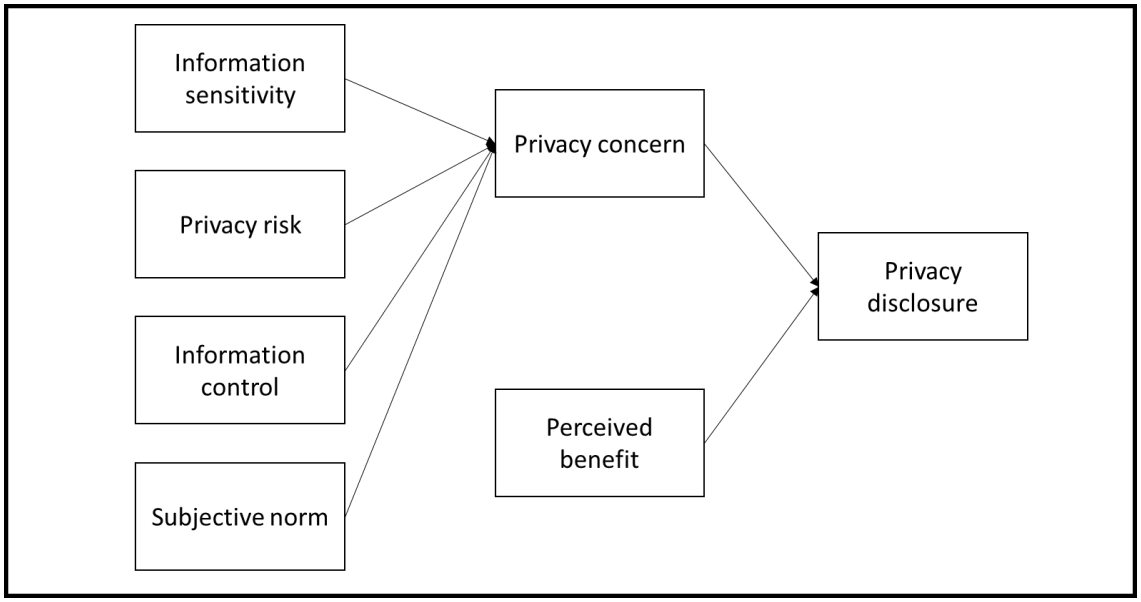

Figure 3 Integrated Model of Privacy Disclosure (Xu, Michael and Chen, 2013)

As seen in figure 2, privacy disclosure is determined by two factors: privacy concern and perceived benefit. While perceived benefit is not further divided into subfactors, privacy concern is affected by four other factors. Information sensitivity, privacy risk, information control and subjective norm all affect privacy concern. Information sensitivity refers to the type of information being shared by the user. Privacy risk is the perception of the user about the risk associated with sharing information. Information control means perception of being able to control information being released. Four factors determine the how well individuals perceive their information control: (1) the presence of a privacy policy on the online site; (2) knowing that information is being collected; (3) voluntary/involuntary submission of the personal information in question; and (4) the openness of the type of information usage by the online organization. Subjective norm refers to the social pressure the individual feels towards behaving in a certain way. This can be either positive or negative. (Xu, Michael & Chen, 2013)

According to the study Xu, Michael and Chen (2013) conducted using the model, perceived risk and information control are the most significant influencers of privacy concern, while the other two factors were determined insignificant. Other results showed that perceived risk of privacy invasion had more influence on privacy concern than unauthorized disclosure of personal information. Additionally, as the results suggest that perceived benefit has significant effect on privacy disclosure. (Xu, Michael & Chen, 2013) This effect has been identified in recent literature as well (Meier, Schäwel & Krämer, 2020).

3 PRIVACY POLICIES

This section will review earlier literature on privacy policies. Based on the reviewed literature the concept will be defined and the purpose discussed. Additionally, benefits, issues and implementation of privacy policies will be analysed to provide background for the research framework.

3.1 Privacy Policy Definition and Purpose

In general, the purpose of the privacy policy is to provide the user with a description of the way the service collects and uses their data and inform them of the security measures and protection systems implemented to protect the data. (Wu, Huang, Yen & Popova, 2012; Aïmeur et al., 2016) At the same time it offers users the possibility to inform themselves of these actions and the potential privacy costs of using the service in question (Meier, Schäwel & Krämer, 2020) The concept can be defined as a statement which informs the users how the service provider handles their personal and sensitive information (Gerlach, Widjaja & Buxmann, 2015). In EU for example it is a legal requirement for service providers to provide the users with the mentioned information (Custers, Van Der Hof & Schermer, 2014; Meier, Schäwel & Krämer, 2020). Privacy policies can be divided into external privacy policies, that are the mentioned legal obligations and inform the user about data collection and use, and internal which regulate the use of sensitive information within an organisation. (Ghazinour & Albalawi, 2016)

However, as the format in which the information is to be presented is not specified, it is not legally required for a service provider to have a separate privacy policy. The information is sometimes presented within a user agreement or a terms and conditions document for example. The aim of providing the information is to allow the users to make informed decisions regarding their privacy. (Custers, Van Der Hof & Schermer, 2014) The EU General Data Protection Regulation obligates the use of understandable language in the privacy policies, which supports the decision-making by the users. (Meier, Schäwel & Krämer, 2020)

As a legitimate action, privacy policy should fulfil certain requirements (Soumelidou & Tsohou, 2020). There are widely adopted principles based on which privacy policies are often built. They are provided originally by US Federal Trade Commission. The principles are notice, choice, access, security and enforcement. Notice refers to informing the user before any data or information is collected or obtained from them. Choice principle aims to ensure that the user is provided with options to choose from regarding how information is collected about them. Access means that user should have access to their own data and review it to ensure it is accurate and complete. Security refers to data itself which should be accurate and protected. Finally, enforcement is necessary to ensure that privacy protection measures are implemented. (Wu, Huang, Yen & Popova, 2012)

Earlier literature has clearly demonstrated that the influence of privacy policies is significant when users evaluate online services. Therefore, it is critical for service providers to assess the content of their privacy policies. The main reason for this is the controversy between the benefit of the user and the service provider. While the content of the privacy policy may be designed according to the service providers business interests, it may interfere with users' desire of privacy. The issues identified by the users in the content of the privacy policy are reflected on their behaviour. (Gerlach, Widjaja & Buxmann, 2015)

An example of this is when Facebook bought Instagram. Facebook changed the privacy policy of Instagram in a way that would allow them to utilize images shared by users without notification or compensation. This caused a reaction in the user base and many users informed the company that they were going to abandon the service. The changes were cancelled by Facebook to avoid the loss of users. (Gerlach, Widjaja & Buxmann, 2015) What is to be considered about this case is that some of the users would have been willing to continue the use of the service despite the obvious privacy violation.

As mentioned earlier in this section, the purpose of the privacy policy is to increase users' trust towards a service provider and reduce privacy concerns. However, in order to succeed in this the information in the privacy policy needs to be read, understood and utilized by the users. If the content of privacy policy is not easy to understand, it is likely that the users will not read it. On the other hand, a clear privacy policy will be read and will lead to increased trust and reduced privacy concern. (Wu, Huang, Yen & Popova, 2012) This view assumes that there are no perceived issues in the content of the privacy policy.

The earlier example of Instagram privacy policy referred to a situation where the privacy policy of the organisation is changed. This is common in social media software. Individual users are affected by the changes in the system-wide policies which influence the privacy policies targeted at them. Users of social media have to rely on the privacy policies provided by the service providers without the ability to configure or enforce the content based on their desires. While the policies do often offer the user with the ability to reduce the visibility of their data to a controlled number of people, such as their circle of friends, the data may be disseminated further through re-sharing by the friends. In the end it is difficult to tell who can in the end see and process a specific user's data. (Baeth & Aktas, 2018) Data may be shared without the consent of the individual.

3.2 User Consent and Perceptions of Privacy Policies

When privacy policies are discussed, it is important to define consent as well. Consent is referred to as informed consent when the individual in the process of providing consent is provided with two types of information: information on what they are specifically consenting to and the consequences of that consent. (Custers, Van Der Hof & Schermer, 2014) The term informed consent is usually the type of consent which is referred to when consent is discussed and is the aim

for privacy policies. If the consent is determined to be informed consent the decision is considered to informed as well. For our society consent is an important notion. It is based on idea of autonomy and respect towards it. (Bechmann, 2014; Custers, Van Der Hof & Schermer, 2014; Rule, 2007) All individuals should have the right and the means to control their own lives. For this to be achieved two conditions need to be met: a capacity for intentional action and independence of controlling influences. In social media and other digital services individuals make the decision to disclose their personal data. Making the decision should be based on the principles of informed consent. There are, however, study results which suggest that users do not fully understand the consequences and risks of disclosing their personal data and the decisions are not always made according to informed consent. (Custers, Van Der Hof & Schermer, 2014) There are several reasons for this.

In her study Bechmann (2014) presents social reasons for accepting privacy policies. Much of the individuals reasoning seems to be guided by group decision making. Even though it is the individual themself pressing the accept button in the end, the fact that their social circle has accepted the terms influence the decision. However, it has been studied that group decision making may lead to poor and misinformed decisions. Consensus-based and rapid decision making are characteristic to group decisions. Additionally, groups are likely to simplify the information they use to make decisions. For example, group decision making is likely to make the individuals in the group belittle the negative consequences and their impact. (Bechmann, 2014) This may be an important aspect for use continuance as well as the choices made by an individual's social circle regarding the use of a service affect the individual.

Custers, Van Der Hof and Schermer (2014) suggest similar reasons for accepting privacy policies, which also supports the claim that use continuance may be affected by social influences. According to them it is difficult to tell whether the consent of a user is based on an independent decision. Many users seem to join SNSs due to forms of peer-pressure meaning that the consent is not given based on their individual opinion. These users often become low-frequency users after they have adopted the service. The authors do however add that the existence of peer-pressure does not necessarily indicate that the decision is not independent. The level of user's dependency on the SNS in association with perception of peer-pressure does. If the user feels that they will not miss the SNS if it was to be removed, it is likely that the consent decision was not made independently. There are no empirical results available on this, however. (Custers, Van Der Hof & Schermer, 2014)

While social effects may affect the decision to consent to a privacy policy of a service, there is a more concerning issue regarding privacy policies. Providing users with the privacy policy information is a commonly accepted requirement for consent (Custers, Van Der Hof & Schermer, 2014). For example, the European Union has an article which requires service providers to enable users to make informed decisions about the disclosure of their data in the service by providing information on how they collect and utilize user data (Angulo, Fischer-Hübner,

Wästlund & Pulls, 2012). The issue is that, as discussed earlier, the format is not specified and users may not concern themselves with the provided information (Custers, Van Der Hof & Schermer, 2014). According to Custers, Van Der Hof and Schermer (2014) existing literature indicates that public levels of privacy issue awareness and concern are low. Dong, Cheng and Wu (2014), however, claim that security of digital services is a common concern among users but do not address the level of awareness among users. Despite this conflict between findings both studies suggest that users' behaviour does not address the issues regarding privacy. Dong, Cheng and Wu (2014) state that users commonly rely on the service providers to protect their privacy instead of concerning themselves with it.

The type of behaviour described may cause users to overlook the need for reviewing the privacy policy. Bechmann's (2014) case study results show that younger users do not read the privacy policies suggesting a non-informed consent culture. Similarly, Obar and Oeldorf-Hirsch (2020) reported that in their study of 543 individuals 74% reported not reading the privacy policy and related documents at all. Of the remaining 26%, 20% opened the documents but spent less than two minutes reading the documents that had an estimated reading time of approximately 30 minutes, before accepting them. This is further supported by Custers, Van Der Hof and Schermer (2014) who in their study concluded that in addition to not reading the privacy policy, users often disregard reading the terms and conditions document as well. The findings of these studies suggest that the users are unaware of what they consent to.

It has also been discussed that even though the users would be made aware of the privacy policy and its content the relationship between Facebook and the user would still be too unequal. To interact and socialise with their friends, users would still have to accept the privacy policy. Additionally, a study concluded that students seem to have trouble imagining risks. Data disclosure is seen simply as a part of the agreement the users make when signing into a service. This seems to be a general opinion on all free social media services. Despite the researchers suggesting several threats to the participants they only found few troubling. Account information written in their inbox being shared is one of the threats that were perceived problematic. Second, third parties falsely using personal data to demonstrate behaviour that is not truly conducted. Third and final one is that apps should not be able to identify friends and retrieve data posted by them through the app based on permissions given by the user. (Bechmann, 2014)

In addition to not reading documents and the potential difficulties of imagining risks, users display low levels of acceptance and significant dissatisfaction with the current practices and policies. This may be due to differences between expectations of consent and privacy among users and service providers. Service providers goal is to fulfil the legal obligations, while being able to gain their desired level of data for business purposes, rather than to meet the needs, interests and preferences of users. (Custers, Van Der Hof & Schermer, 2014) One could easily conclude that dissatisfaction and low acceptance would lead to individuals not accepting the policies. However, in the study by Custers, Van Der Hof and Schermer (2014), the authors note that while dissatisfied and reluctant to accept

the policy some of the individuals still join the service. Users seem to regard the privacy policy and other documents simply as a nuisance (Obar & Oeldorf-Hirsch, 2020).

A partial reason for the users not reading the documents could be media. Media frequently reports on privacy policies of service if there are issues discovered issues, which leads to a situation where the users believe they are not required or do not see it necessary for them to read the documents. Users simply rely on the media to report on the potential privacy issues. (Gerlach, Widjaja & Buxmann, 2015) Disregard towards privacy policies could also be a part of a larger trend. Studies on information security issues from the perspective of stock market have revealed interesting facts (Gordon & Loeb, 2011). Studies suggest that the cost of security breaches to companies has reduced over time. After the year 2001, the drops in stock prices caused by security breaches have been less significant than before. Investors have begun to see them as a persistent issue and believe that consumers share this opinion. As this lowers the impact of security incidents from the service providers point of view, there may be significant consequences to privacy as well. (Gordon & Loeb, 2011)

Findings by Soumelidou and Tsohou (2020) present issues in the conventional form of privacy policies. According to them, existing literature reports, as presented by the literature findings earlier in this subsection as well, that the current form of privacy policies does not contribute towards increasing users' privacy awareness. They state that a more attractive way of presenting the information would be needed. The results of their study indicate that a visualised format would improve users' privacy policy awareness over the conventional format. It seems that statement in words is more difficult to comprehend than a statement made with images, which draws more attention. (Soumelidou & Tsohou, 2020) However, as the transition to visualised privacy policies would most likely take time, a simpler approach could be taken in the meantime. Meier, Schäwel and Krämer (2020) suggest based on the findings of their study that simply reducing the length of the document will improve both reading accuracy and knowledge.

For companies, compliance to legal obligations regarding privacy policies is important as it allows them not only to avoid sanctions, but also to build trust and reputation among users (Custers, Van Der Hof & Schermer, 2014). Privacy policy is one of the common measures service providers use to increase trust of users towards their services along with third party certifications and references for example. After all it is a simple and inexpensive approach to the matter. (Sigmund, 2021) Meeting the legal obligations and increasing trust seem to be the main focus areas for companies to implement privacy policies. However, focusing also on the users' needs, interests and preferences regarding the policies could help companies further increase users' trust. A way forward for social media could be to better answer the wishes of the users to build trust and improve the transparency and responsible use of user data. (Custers, Van Der Hof & Schermer, 2014) However as discussed earlier, increasing transparency is not necessarily to answer to improving transparency. Revealing the full data collection

and use an organisation engages in, may result in an information overload and decrease transparency and trust. (Nissenbaum, 2011)

3.3 Cost-Benefit Perception

On Facebook the users control their data by agreeing or disagreeing to policies and by choosing settings as already mentioned. The settings can be divided into three groups (Vishwanath, Xu & Ngoh, 2018). First, there are those that control information privacy, such as the social media account and identity information. Second, accessibility privacy, or anonymity, settings control who can connect with the user for example. Third, are settings that control expressive privacy meaning who your posts are shared to for example. The use of the settings is however often a trade-off between being accessible and being protected. While high privacy could be considered desirable, it often reduces the benefits generally associated with social media use. (Vishwanath, Xu & Ngoh, 2018) Vishwanath, Xu and Ngoh (2018) use the two theories, U&G theory (Child, Haridakis & Petronio, 2012) and PMT (Rogers, 1975) to investigate the users' perceptions towards cost-benefit perceptions of Facebook use.

Their results show that perceived severity and perceived susceptibility of privacy incursions have a significant impact on privacy management. Of the two, perceived susceptibility affects the accessibility privacy behaviour and perceived severity leads to expressive and accessibility privacy increasing behaviour. They analyse that this could be caused by the social nature of use. Self-presentation is a common use for Facebook as a platform and social losses caused by inaccurate self-presentation or public embarrassment are therefore considered significant by the users. Information privacy loss is perceived as important but not as impactful as the loss of the two other types. According to the authors this may be due to the private nature of the costs; other users may not notice such losses. This raises the interesting realization that social embarrassment caused by a photograph is considered more significant than the loss of digital information or a password. (Vishwanath, Xu & Ngoh, 2018)

Moving on to the benefits, the results suggest that the most significant benefit is the fulfilment of social needs. It influences the way the settings are managed the most out of the benefits of use. Social needs in their study include finding and maintaining relationships with others and getting social support. Other type of benefits in the study are information and entertainment needs do not have as significant impact on settings management as no disclosure of personal information is needed to fulfil these needs. Regarding benefits, the results also suggest that privacy management is more determined by the perceived benefits of use than be the perceived costs. Users seem to weigh the benefits before taking the costs into account. (Vishwanath, Xu & Ngoh, 2018)

The idea of cost-benefit thinking is not new. As early as 1999 Culnan and Armstrong use in their work the term "privacy calculus", which refers to individuals making considerations regarding disclosing personal information based

on the perceived benefit and cost. They make this conclusion and define the term based on prior literature that had identified such behaviour. However, they emphasize the role of fair use of that disclosed information. According to their literature review the invasion of privacy is regarded less significant if the collection happens in an existing relationship, individual feels that they can control future use of disclosed information, the collected information is relevant to the transaction and reliable and valid inferences will be drawn from the information. (Culnan & Armstrong, 1999)

4 USE CONTINUANCE

Much of the existing IS literature focuses on the adoption and initial use of systems. This means that the post-adoption use behaviour has received limited attention. (Bagayogo, Lapointe & Bassellier 2014) Use continuance is the most widely recognised post-adoption behaviour type (Kari, Salo & Frank, 2020). Use continuance has been identified as an important aspect to IS success (Kari, Salo & Frank, 2020; Bagayogo et al., 2014; Bhattacherjee, 2001) It is considered valuable as it influences the creation and maintenance of customer relationships. This means that it should be in the best interest of the service providers to maximise use continuance and minimise use discontinuance of their services. (Bhattacherjee, 2001) Understanding use continuance from multiple perspectives is therefore essential for research to be able to support practice.

Use continuance can be shortly defined as the continuing use of an IS product or service past the initial adoption of that service or product by a user (Bhattacherjee, 2001). Use discontinuance is naturally the opposite of this meaning the end of use by the user at any point after the adoption. According to Salo and Frank (2017) use continuance and discontinuance are affected by single-use experiences. Particularly, when the experience is unusually positive or negative in the user's opinion, the influence is emphasised. These experiences are called critical incidents in the literature. (Edvardsson & Roos, 2001) It is obvious that these incidents need to be studied as they have a significant meaning to IS success and relationship management with customers (Salo & Frank, 2017). While there is research on the topic, it mainly focuses on the incidents themselves in terms of mitigation and avoidance for example and does not address the actual use behaviour regarding critical incidents. (Kari, Salo & Frank, 2020) Privacy policy changes which cause significant impact to user privacy could be considered critical incidents and are therefore a factor in use continuance based on literature described in this paragraph. The perception of the negativity of the change is likely to be associated with the type of change or the dimension of privacy affected in other words.

In this chapter existing models explaining IS use continuance are introduced. These models serve as the base for the research framework described in chapter 5. First, however, some additional findings from existing literature regarding use continuance are reviewed to support and provide additional perspective to the framework.

4.1 Information System Use Continuance Models

Existing literature has identified some key factors to use continuance. Bhattacherjee (2001) discovered that satisfaction and perceived usefulness influence use continuance. A study by Vatanasombut, Igbaria, Stylianou and Rodgers (2008)

shows that relationship commitment and trust are factors which need to be taken into account. They mention perceived security as a key element to trust. Wang, Asaad and Filieri (2020) extent these findings by making similar discoveries regarding the role of trust and further dividing it into subfactors which are technical quality, social benefits, perceived efficiency of the privacy policy and economic benefit. Hong, Kim and Lee (2008) identified attitude and switching cost to be significant factors. Bhattarcherjee and Lin (2015) associated reasoned action, experimental response and habitual response with use continuance behaviour, and Salo and Frank (2017) proved that situational context is relevant as well. Additionally, a recent study be Kari, Salo and Frank (2020) showed that social setting influences IS usage along with the use orientation. More specifically negative incidents are more likely to lead to discontinuance of use when they occur in an individual setting when compared to a group setting. Utilitarian or a combination of utilitarian and hedonistic use orientation were found to be associated with increased use continuance intention after positive experiences. The study conducted in the context of exergaming, but it is likely that the influence exists in other contexts as well. (Kari, Salo & Frank, 2020)

While Wang, Asaad and Filieri (2020) identified the perceived efficiency of the privacy policy as a key factor in trust which in turn affects use continuance, they did not specify what it means and what type of factors are associated with it. As mentioned earlier Vatanasombut et al. (2008) identified perceived security as a factor to use continuance. They also divide it to subfactors; one of which is violations of privacy by the service provider. There are also some conflicting findings on the role of perceived security. Oghuma et al. (2016) assumed in their study that perceived security would affect user satisfaction in the context of messaging services, but the results proved this assumption to be incorrect. As these results show there is clear connection between security and privacy and use continuance and there is a clear need for further research.

In the context of mobile applications prior research on use continuance has utilised Technology Acceptance Model, extensions and variations of it, expectation confirmation model, combinations of different adoption theories and IS use continuance model for example. In the literature factors such as perceived usefulness, perceived ease of use, trust, perceived risk, self-efficacy, mobile application customizability, and attitude of the user have been identified to have an effect on use continuance in this context. (Lumor, Pulkkinen & Hirvonen, 2020)

In the coming subsections, some of the above models will be introduced for the purposes of the study. The models will be further analysed in the next main section to create a framework for the empirical part of this study. The introductions will not be extensive as the aim is not to use the models as they are.

4.2 Post-Acceptance Model of Information System Continuance

One of the earliest use continuance models is the post-acceptance model of information system continuance (PAMISC) introduced 2001 by Bhattacherjee. It

is based on the expectation confirmation theory (ECT), which is visualised in figure 4. Originally it was introduced by Oliver (1980). According to Bhattacherjee (2001) ECT is commonly used in consumer behaviour literature. Some of the main research topics inlude consumer satisfaction and post-purchase behaviour. (Bhattacherjee, 2001) Oghuma et al. (2016) summarize the process assumption of the model as a process which begins prior to purchase when initial expectations are formed of a product or service and ends with repurchase intention.

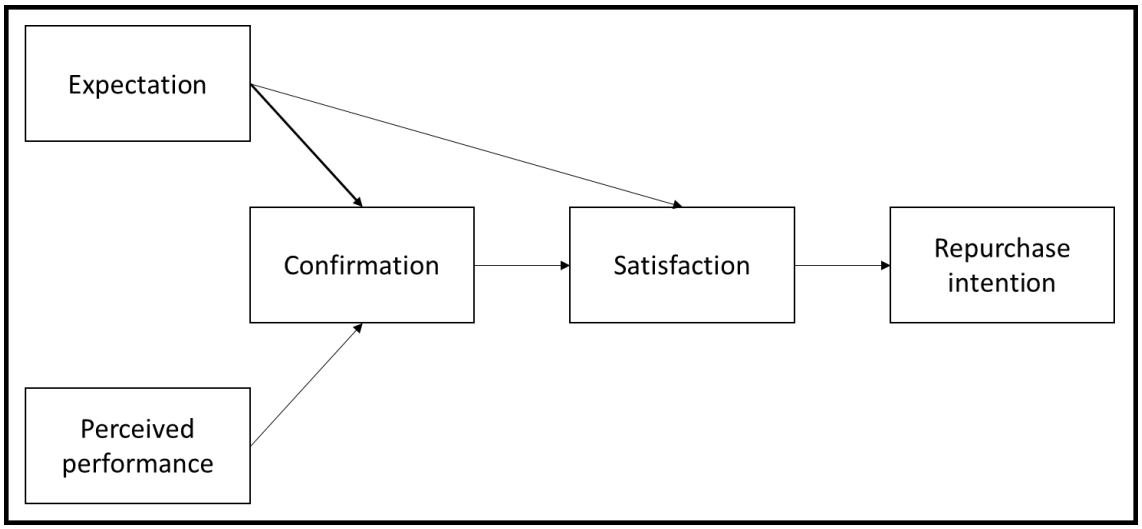

Figure 4 Expectation Confirmation Theory (Oliver, 1980)

The elements of ECT include satisfaction as the single predictor of repurchase intention, confirmation and expecation as predictors of satisfaction and expectation and perceived performance as predictors of confirmation. Based on earlier literature Bhattarcherjee (2001) determined that including perceived performance would cause the model to be overspecific. Additionally, the technology acceptance model (TAM) suggests that the post-consumption expectations in IS are represented by perceived usefulness. Based on TAM the perceived usefulness and perceived ease of use are main factors in IS acceptance and are therefore determined as factors of use continuance in the PAMISC represented in figure 5. Confirmation is in the PAMISC regarded as a determinant of perceived usefulness as the perception is based on the expected usefulness. (Bhattacherjee, 2001)

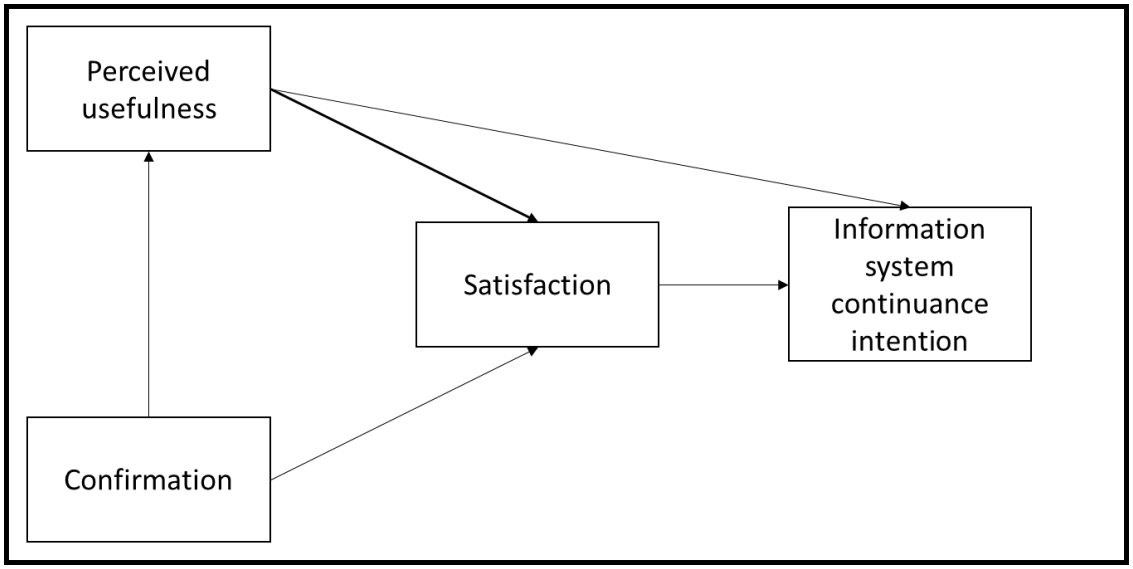

Figure 5 Post-Acceptance Model of Information System Continuance (Bhattacherjee, 2001)

Similar to ECT, PAMISC views satisfaction as the primary predictor of IS continuance intention. However, there is also a direct relationship between perceived usefulness and continuance intention. Satisfaction is determined by the combination of perceived usefulness and confirmation which is in line with the ECT. The relationship between confirmation and perceived usefulness is reversed in comparison to ECT, which had expectations influence confirmation. (Bhattacherjee, 2001)

4.3 Model of Continuance Intention among AirBnB hosts

In contrast with the model by Bhattacherjee (2001), Wang, Asaad and Filieri (2020) determine in their research model that the main predictor of use continuance is trust instead of satisfaction. Their model is presented in figure 5. Trust has been mentioned in multiple occasions throughout the literature review of this study. Its role regarding privacy and privacy disclosure behaviour is undeniable and therefore this model is introduced. In addition, perceived effectiveness of privacy policy is included in the model increasing its potential contribution to this study. The model focuses on sharing economy context.

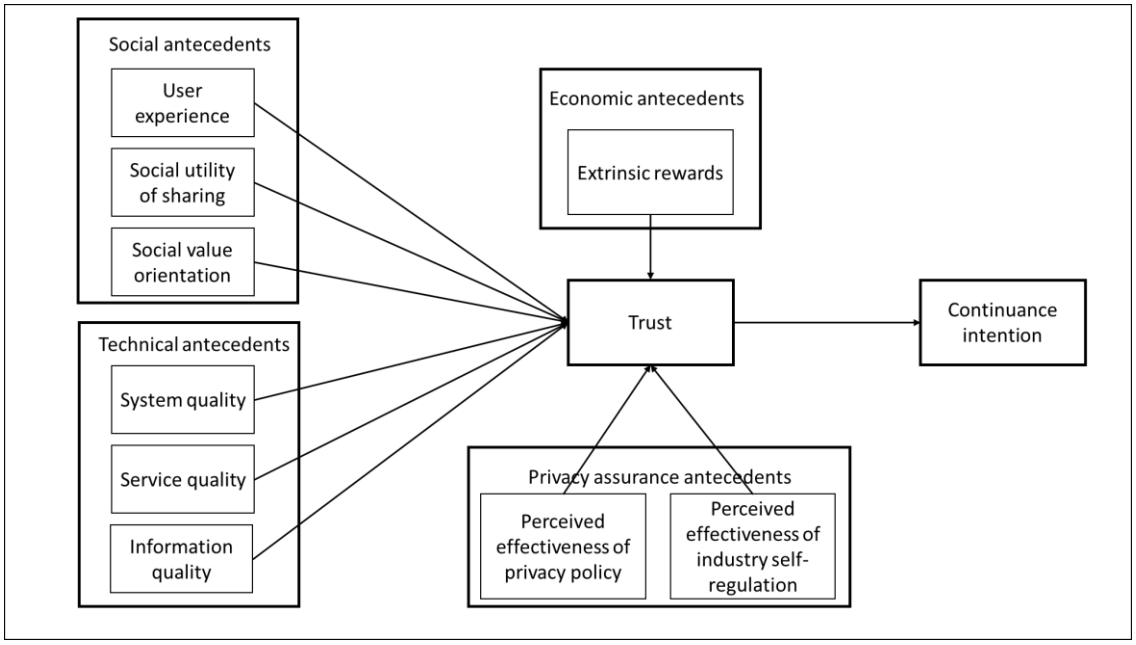

Figure 6 Model of continuance intention in host-side of Airbnb (Wang, Asaad & Filieri, 2020)

The model by Wang, Asaad and Filieri (2020) divides the determining factors of trust into four categories: economic, social, technical and privacy assurance antecedents. Extrinsic rewards form the economic antecedents. Extrinsic reward means receiving direct or indirect monetary benefit from using a service. Social antecedents included in the model are user experience, social utility of sharing and social value orientation. Social utility of sharing refers to the social benefits gained by participating in sharing. It suggests that if sharing is a socially accepted behaviour the trust towards the service increased. Social value orientation is the user's perception of the value of sharing and the associated orientation. For example, pro-social orientation means that an individual is willing to participate in sharing. Technical antecedents are system, service and information quality. Finally, privacy assurance antecedents included in the model are perceived effectiveness of privacy policy and perceived effectiveness of industry self-regulation. Perceived effectiveness of industry self-regulation refers to the individual's perception of how effectively government institutions and third parties, such as certifying organisations and banks, regulate the service. Perceived effectiveness of privacy policy, on the other hand, can be defined as an individual's perception of how accurate and reliable the information on the firm's privacy practices documented in the privacy policy is (Xu et al., 2011).

4.4 Expectation-Confirmation Model of Continuance Intention in Mobile Instant Messaging

Oghuma et al. (2016) study use continuance in the context of mobile instant messaging (MIM). They combine the before mentioned and adapted ECT with the PAMISC to create a novel model to explain use continuance. They also add factors to the combined framework. The model is visualised in figure 7.

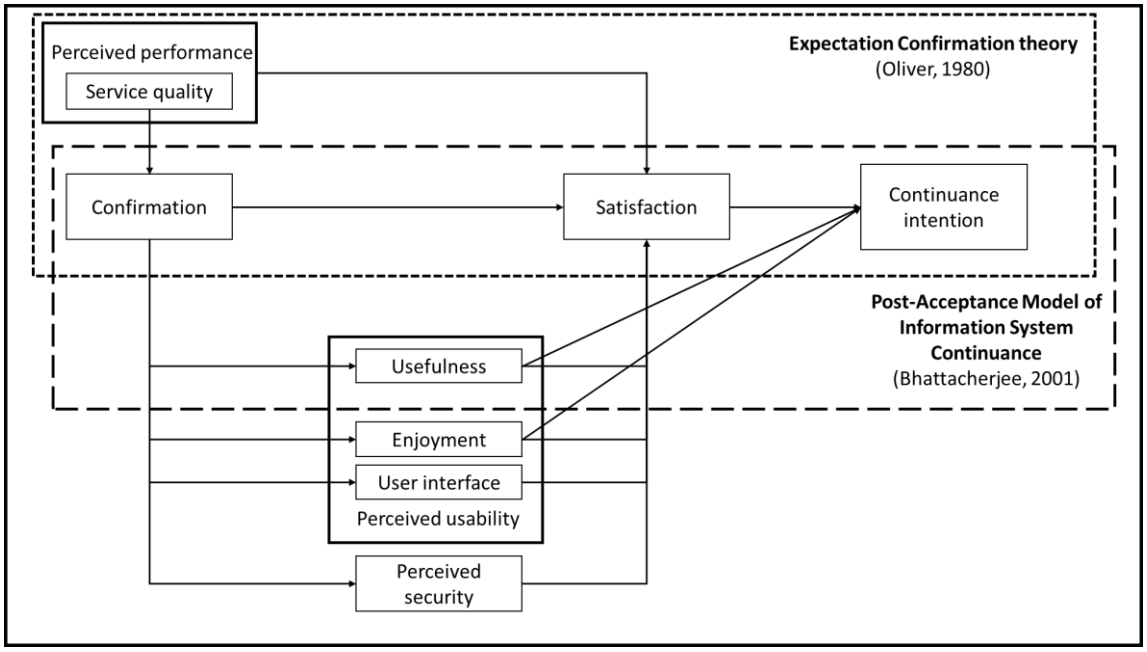

Figure 7 Expectation Confirmation model of continuance intention to use Mobile Instant Messaging (Oghuma et al., 2016)

As described in the PAMISC introducing section, the models overlap regarging confirmatin satisfaction and continuance intention. The relationships between confirmation, satisfaction and continuance intention are the same as described in both models. From the ECT Oghuma et al. (2016) include the perceived performance factor, which is measured by service quality alone, which affects confirmation and satisfaction. From PAMISC, usefulness is included in the model. This is defined to be a utilitarian view of the usefulness of the service in this model. Usefulness is influenced by confirmation and in turn influences satisfaction and continuance intention. This is in line with PAMISC. As new factors, enjoyment and user interface were added to the model. Enjoyment refers to the hedonic value of the service and user interface to the features included. Together with the usefulness they form the measures for perceived usablity of the service. Similar to usefulness enjoyment is influenced by confirmation and affects satisfaction and continuance intention. User interface is also affected by confirmation but only influences satisfaction. Perceived security is the final new factor of the model. It is defined by the authors as the perceived ability of the

service provider to protect the user from security breaches. It is influenced by confirmation and is connected to satisfaction as predictor. (Oghuma et al., 2016)

Based on the analysis of the results of their study, their model is supported. All other relationships are supported by their data except for the perceived security. The results do not show a significant association between security and satisfaction. (Oghuma et al., 2016)

5 CURRENT STUDY

Vishwanath, Xu and Ngoh (2018) suggest in their conclusions that the future experiments should assess what type of settings the users change in response to privacy breaches. This study aims to take the topic one step further and investigate in the context of critical negative incidents how the privacy breach type effects use continuance.

In their study, Wu, Huang, Yen and Popova (2012) suggested that the type of information may influence the willingness of individuals to provide personal data. Their study did not address this aspect of data disclosure. They did discover that willingness to provide personal information is associated with privacy concerns and trust. As willingness to disclose personal data is associated with the use of a digital service and the connection between trust and use continuance has been acknowledged, this study will focus precisely on the effect of the information type on use continuance.

Reviewing privacy literature to determine what privacy is, how it is perceived and what are the different factors associated with it, provided insight to how the effects of privacy breaches could be studied. The four dimensions of privacy are to be used in the survey to determine the differences between privacy policy change types. Dividing changes into solitude, intimacy, anonymity, and reserve affecting changes, based on the definition by Buckner and Knowles (2012), can help identify differences between users' perceptions. In a study, privacy issues that risk user's social image were as the most influential towards privacy management. (Vishwanath, Xu & Ngoh, 2018)

The role of social effects as modifiers of the use continuance decision making must be also investigated. For example, Bechmann (2014) stated that one of the main reasons for disclosing personal information is the will to interact with friends. Additionally, the use orientation and attitudes (Child, Haridakis & Petronio, 2012) need to be addressed to determine whether they have effect on the behaviour after negatively perceived privacy policy changes. The inclusion of attitudes is also supported by the findings of Dienlin and Trepte (2015) as discussed in the privacy behaviour subsection. As mentioned earlier, orientations and attitudes are interconnected and affect expectations. While the age of the user seems to be a factor in privacy behaviour, this study focuses on the youngers, who according to the existing literature are more likely to behave in an unsafe manner in SNSs (Dowding, 2011; Bechmann, 2014).

Cost-benefit perspective to SNS use is also to be investigated. As described by Rule (2007), the users seem to be willing to disclose their personal information and data to gain various potential benefits from services. Perceived benefit has been identified as significant factor to privacy disclosure. (Xu, Michael & Chen, 2013) Of the benefits, social benefits are to be considered most significant in comparison to information or entertainment benefits. On the cost side of these considerations perceived severity and perceived susceptibility have been discovered to have the most significant impact. (Vishwanath, Xu & Ngoh, 2018) As

mentioned earlier in this study, Child, Haridakis and Petronio (2012) suggest that the attitudes and orientations are connected to the cost-benefit considerations. Additionally, they combined motivations with these considerations. Awareness of the users about the potential risks of SNS use must also be considered as it has been questioned on many occasions in literature.

Reviewing the privacy policy literature revealed the potential issues and challenges regarding the use and effectivity of those policies. While this revealed that users are unlikely to read the policies and are not aware of the issues of privacy policies (Acquisti & Gross, 2006), the topic of this study remains important as privacy breaches caused by privacy policy changes can be reported through other channels such as news media. The users are required to act in accordance with these revelations. On the other hand, the users disregard towards privacy policies also suggests that SNSs can quite freely choose what type of data they wish and how they utilize it if it does not provoke a reaction from the media.

Expectation and confirmation approach could be included in the research framework as it would reveal what type of data collection and use younger users consider to be acceptable and "normal". Literature suggests that users see data disclosure as a part of the deal they make with the service provider to gain free access to their SNS (Bechmann, 2014). This also relates to the discussion in the privacy section where Mark Zuckerberg is quoted saying that maybe privacy should not be considered the same way as it used to be in the past (Dowding, 2011). This would also enable future studies to investigate whether the expectations have changed over time as suggested by the changes in the stock market and media reactions to security breaches.

Based on the before mentioned studies and discoveries, a research model for studying the effects of critical negative privacy policy changes is suggested. The model is depicted in figure 7. It builds on the integrated model of privacy disclosure (Xu, Michael & Chen, 2013), model of Continuance Intention in host-side of Airbnb (Wang, Asaad & Filieri, 2020) and expectation-confirmation model of continuance intention in mobile instant messaging (Oghuma et al., 2016).

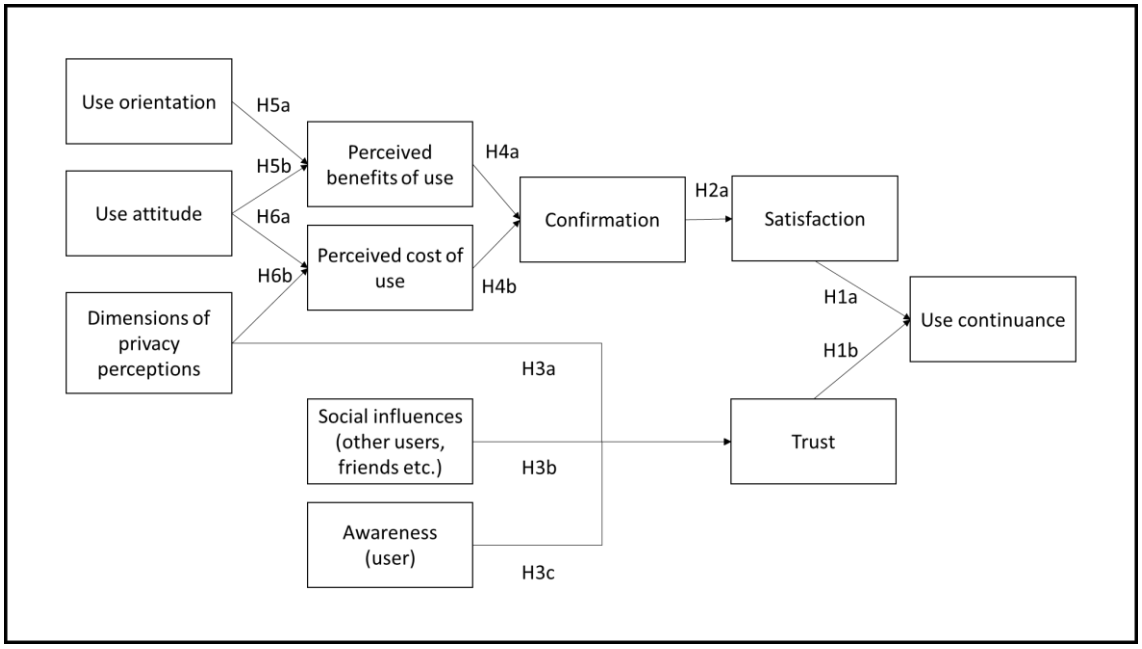

Figure 8 Suggested research framework and hypotheses

The combination of confirmation, satisfaction and use continuance, which has been used in several models introduced in this study is also utilised in this model (Oghuma et al., 2016; Bhattacherjee, 2001; Oliver, 1980). Confirmation in the model refers the expectations of the user to be confirmed by the service use. As an additional factor to directly affect use continuance, trust is introduced from the Airbnb host-side model (Wang, Asaad & Filieri, 2020). This refers to trust of a user towards service provider. Based on earlier literature the following hypotheses are formed:

H1a: Satisfaction has a positive effect on use continuance intention
H1b: Trust has a positive effect on use continuance intention
H2: Confirmation has a positive effect on satisfaction

The role of trust has been discussed in privacy literature and it is associated particularly with the social influences (Wang, Asaad & Filieri, 2020) and awareness based on the trust increasing effect of privacy policy reading (Custers, Van Der Hof & Schermer, 2014; Wu, Huang, Yen & Popova, 2012). Awareness can be surveyed by investigating whether users are aware of privacy policies and their perceived awareness of risks related to SNSs. Additionally, dimension of privacy perceptions is hypothesised to be another factor that directly affect trust. This refers to the perceived severity of a certain type of privacy violation. The four dimensions used are derived from the definition of privacy by Buckner and Knowles (2012). From these literature discoveries the following is hypothesised:

H3a: Awareness has negative effect on trust
H3b: Social influences have a positive effect on trust
H3c: Dimensions of privacy perceptions have a negative effect on trust

As discussed earlier in this section cost-benefit considerations are connected to confirmation and expectations. Perceived cost of use is to be measured by items focusing on perceived severity and perceived susceptibility. Based on literature attitude towards use influences privacy concerns side of the cost-benefit considerations (Xu, Michael & Chen, 2013; Dienlin &Trepte, 2015). Similarly, dimensions of privacy perceptions are expected to affect perceived cost as perceptions of the severity of certain type of privacy breach is connected to perception of severity of a breach. Perceived benefit is hypothesised to be influenced by use orientation, which is divided to utilitarian, hedonistic and the combinations of the two, and use attitude meaning the users attitude towards privacy in an online and SNSs setting. These literature findings result in the final six hypotheses:

H4a: Perceived benefit of use has a positive effect on confirmation
H4b: Perceived cost of use has a negative effect on confirmation
H5a: Use orientation has a negative effect on perceived benefit of use
H5b: Use attitude has a negative effect on perceived benefit of use
H6a: Use attitude has a positive effect on perceived cost of use
H6b: Dimensions of privacy perceptions have a positive effect on perceived cost of use

6 Methodology

The goal of the empirical study was to provide a model which could predict use continuance behaviour in SNSs after a privacy incident while taking into account privacy policies factors. Quantitative research has been identified as the method to achieve such goals (Vilkka, 2007). The focus of quantitative research is to study relationships that exist between variables (Punch, 2003). Survey approach for this study is also supported by research method literature as it is identified as the suitable method for studying individuals' opinions, attitudes and behaviour (Vilkka, 2007). Survey also allows fast and efficient data collection from a large number of people (Hirsjärvi et al, 2007). The study was conducted as a cross-sectional study meaning that data collection is only performed ones, at one point in time (Punch, 2003)

In this section the methodology of the empirical part is described in detail. First the demographics of the participants are described followed by the measures used in the study. The latter includes details and examples of the items used to measure specific variables. After the introduction of the items a description of the pilot study and its results is presented. Following the pilot, details of the main study are also summarised in a dedicated subsection. Details include the results of Cronbach's alpha and factor analysis. The final part of this section introduces the procedure used to recruit the participants and how they completed the study.

6.1 Participants

134 participants were recruited from the students at the University of Jyväskylä. The stage of their studies varied between first year bachelor's degree students to master's students. The participants were all either students of the faculty of information technology or in the degree program of political science. The participants included mostly Finnish nationals and some exchange students. No further demographic data was collected from the participants.

6.2 Measures

The empirical part of the study was conducted as a quantitative survey. Quantitative survey was chosen as the method of this study as parts of the topic have been covered by previous literature meaning that most of the survey items can be built based on existing literature. This is a common approach in quantitative research (Vehkalahti, 2019). The connections between variables can be found in existing literature meaning there is no need for explorative qualitative research on the topic. However, as there are new aspects of use continuance to be

investigated some items have been created for the purposes of this study based on the findings of previous literature. This is also a common approach in quantitative surveys (Vehkalahti, 2019). The statistical approach will test hypotheses suggested in the research framework (figure 8) designed for this study.

The item set used in the survey can be found in appendix 1 for the pilot study and in appendix 2 for the main study. For both surveys there are at least three items measuring each variable in the research model. Table 1 includes item examples for each variable along with a reference to the original author who used the item in their study or whose findings assisted in the creation of the item. The same information can be found in both appendix 1 and 2 for their corresponding surveys. All of the examples in table 1 are from the appendix 1 as presenting the items used in the pilot supports the next subsection introducing the pilot study.

Table 1 Examples of items used to measure variables

Variable	**Item example**	**Reference**
Use continuance intention	I might stop using the service in the future if the service had experienced a privacy incident	Oghuma et al. (2016)
	I will continue using the service as regularly as I do now	Wang, Asaad & Filieri (2020)
Trust	I believe that the service provider acts in my best interest	McKnight et al. (2002)
	I trust that the service provider provides enough safeguards for me to be safe using the service	McKnight et al. (2002)
Satisfaction	I feel satisfied with the service	Oghuma et al. (2016)
Confirmation	The cost-of-service use is as I expected it to be	Oghuma et al. (2016)
Perceived benefit of use	The service allows me to pass time easily and entertain myself	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	I enjoy using the service	Oghuma et al. (2016)
Perceived cost of use	I disclose personal information to the service provider in exchange for use	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
Privacy awareness	I'm aware of the privacy issues related to Social Networking Services	Xu et al. (2008)
	I have read the privacy policy of the service I use	Based on Wu et al. (2012), Bechmann (2014), Obar & Oeldorf-Hirsch (2020), Custers, Van Der Hof and Schermer (2014) and Acquisti & Gross (2006)
Social influences	Members of my social group convinced me to join the service	Based on findings of Custers, Van Der Hof and Schermer (2014)

Dimensions of privacy perceptions	It is a serious problem if the privacy policy limits my ability to control my personal level of solitude in the service	Adapted from Buckner & Knowles (2012)
Use orientation	I mainly use the service to entertain myself (videos, memes, etc.)	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
Attitude	I should only reveal the required personal information to set up a profile	Adapted from findings by Dowding (2011), Child, Haridakis and Petronio (2012), (Dienlin & Trepte, (2015), Ajzen (1991), Xu, Michael & Chen (2013), and Hong, Kim and Lee (2008)
	To me, it is most important to maintain privacy online	Xu et al. (2008)

Use continuance intention items aim to measure the likelihood and the strength of the intent of a user continuing using a service in the future. In the context of this study the privacy incident aspect has to be addressed as well. Oghuma et al. (2016) studied use continuance in the context of mobile instant messaging and the items used in their survey are utilised in this study for a similar purpose. The first example in table 1 is an item used in their survey modified to better fit the context of this study. Their original item was "I might stop using the service in the future". With the addition of "if the service had experienced a privacy incident" the privacy incident context is addressed. To have more variety in the items measuring use continuance the item "I will continue using the service as regularly as I do now" was also added. This item is originally used in a survey study by Wang, Asaad and Filieri (2020). It adds another dimension to measuring use continuance in this study as it addresses the frequency of use instead of simply the continuation or discontinuation of use. There are three other items used to measure use continuance as well. They were all used by Oghuma et al. (2016) and in comparison to the first example they measure use continuance intention within different time frames.

Trust is to be measured using a total of three items as can be seen in appendix 1. The items are originally from a study by McKnight et al. (2002). Table 1 presents examples of the items used in this study to measure trust. Wang, Asaad and Filieri (2020) use "I trust that the service provider provides enough safeguards for me to be safe using the service" to measure trust which directly based on the items by McKnight et al (2002). In the context of this study, it covers the security and privacy dimensions of trust that needed to be included in the measuring. McKnight et al. (2002) also used other items in their study. The first example of trust items is not used by Wang, Asaad and Filieri (2020) but is utilised in this study to deepen the measuring of trust. "I believe that the service provider acts in my best interest" takes a more a general approach to measuring trust of the user towards the service provider.

Oghuma et al. (2016) also measured satisfaction in their survey and the items from their item set are suitable for the purposes of this study as well. The goal of the satisfaction items is to measure how satisfied or content the users are with the service. Oghuma et al. (2016) utilised the item set with success in their study and no changes were made to the items for this study. As an example of the items one of them is "I feel satisfied with the service". The remaining three items can be found in appendix 1 and they include aspects such as user experience and ease of use in the measurement.

Confirmation refers in this study to the confirmation of expectations regarding benefit and cost of use and the items reflect this. Oghuma et al. (2016) measured confirmation using two items: "my experience with using the MIM is better than what I expected", and "the service level provided by the MIM is better than what I expected". These items were used as inspiration to design the items to measure confirmation in this study. The items could not be directly used as the structure of the research framework differs from that of Oghuma et al. (2016). Example of the items designed for the purposes of this study can be found in table 1. The remaining two items are designed to measure benefit of use, and the trade-off between benefit and cost using a similar approach as the example item.

Four items are used to measure perceived benefit and they are based on earlier work of either Oghuma et al. (2016) or Vishwanath, Xu and Ngoh (2018). As the first example of perceived benefit of use items in table 1, is an item that has been adapted from the findings by Vishwanath, Xu and Ngoh (2018). They studied the topic of privacy on Facebook from a cost-benefit perspective and conducted a survey, but do not provide the individual items used in it in their article. They divided the benefits of use into three categories that are covered by the designed items. The example in table 1, "The service allows me to pass time easily and entertain myself", addresses the entertainment dimension, while the remaining two, that can be found in appendix 1, address the information and social benefits. To compliment these three items a fourth item is also included. While measuring the variable perceived enjoyment in their study, an item by Oghuma et al. (2016) is added to the item set. Presented in table 1, "I enjoy using the service" takes a different approach to perceived benefit as it measures the enjoyability of use.

Perceived cost of use measurement items are, similar to perceived benefit, adapted from the work of Vishwanath, Xu and Ngoh (2018). They discuss in detail the different aspects of perceived cost in their article. As can be seen by examining perceived benefit row in appendix 1, the three items measure the different approaches to how the user can perceive the cost-of-service use and the acceptability of that cost. In table 1, "I disclose personal information to the service provider in exchange for use" is given as an example of these items.

"I'm aware of the privacy issues related to Social Networking Services" and "I have read the privacy policy of the service I use" are provided as examples of items that measure privacy awareness. The first item is directly from the survey of Xu et al. (2008) where it is used for the exact same measurement purpose. It measures the participant's awareness of privacy issues in general. The second

example item measures privacy awareness from a more service specific level as it surveys whether the participant has familiarised themselves with the privacy policy of the service to any extent. Users not reading the privacy policies has been identified as a common issue for privacy awareness and should therefore be surveyed (Wu et al. (2012); Bechmann (2014); Obar & Oeldorf-Hirsch (2020); Custers, Van Der Hof and Schermer (2014) & Acquisti & Gross (2006).

Social influences variable is represented by three items which are based on the findings by Custers, Van Der Hof and Schermer (2014). In their study Custers, Van der Hof and Schermer (2014) discussed the different aspects of social interaction within groups that can result in unsafe privacy behaviour. The items have been designed specifically for the purposes of this study. An example of the items is given in table 1. "Members of my social group convinced me to join the service" measures the impact of peer pressure, which is discussed by Custers, Van der Hof and Schermer (2014) in their article.

The dimensions of privacy perceptions items have also been specifically designed for this study. All of the items utilise the same template as the example "It is a serious problem if the privacy policy limits my ability to control my personal level of solitude in the service" in table 1. The four items cover the four dimensions of privacy included in the definition of privacy by Buckner and Knowles (2012). The dimensions are solitude, intimacy, reserve and anonymity. This results in a good measurement of the participants perception of the importance of different privacy dimensions and overall desired level of privacy in SNSs.

Use orientation can be divided into hedonistic, utilitarian and mixed use (Kari, Salo & Frank, 2020; Vishwanath, Xu & Ngoh (2018). Adapting from the findings and discussion by Vishwanath, Xu and Ngoh (2018) a set of three items is designed to measure the variable from those three approaches. An example is given in table 1 and the two others follow the same structure. "I mainly use the service to entertain myself (videos, memes, etc.)" aims to measure the level of hedonistic use orientation. The other two items measuring mixed and utilitarian use are presented in appendix 1. Together the items provide a comprehensive measurement of the use orientation of the participant towards the SNSs of their choice.

The topic of use attitude is discussed in a range of articles (Dowding, 2011; Child, Haridakis & Petronio, 2012; Dienlin & Trepte, 2015; Ajzen, 1991; Xu, Michael & Chen, 2013; and Hong, Kim & Lee, 2008). However, no existing measurement items for the variable could be found and therefore the items to measure it are created based on the existing literature in order to meet the needs of this study. In most SNSs it is necessary to have a profile. This requires a certain amount information to be revealed but can be seen as a use requirement. Disclosing additional information is at the judgement of the user and largely based on attitude towards such behaviour according to the literature (Dowding, 2011; Child, Haridakis & Petronio, 2012; Dienlin & Trepte, 2015; Ajzen, 1991; Xu, Michael & Chen, 2013; and Hong, Kim & Lee, 2008). The first example item, "I should only reveal the required personal information to set up a profile", has been deducted from this literature finding. To form the item set for use attitude two other items

have been designed based the discussions. Finally, an item used by Xu et al. (2008) is also added into the item set to provide a fourth item. Adding "To me, it is most important to maintain privacy online" enables a degree of flexibility during analysis.

6.3 Pilot Study

A pilot survey was to be conducted prior the final survey to avoid potential issues regarding items, variables or scales. This is particularly important as some of the variables are being measured by items that have been designed specifically for this study based on the findings, not items, of others. The purpose of the pilot is to determine whether the items used in the survey reliably measure the variables they are designed to measure. The pilot participants represent the participants of the main study.

The full list of items used in the pilot can be found in appendix 1. The order of the questions in the survey is as it is in the table. The existing literature sources used to formulate the questions are marked for each item. If only the source is provided with no further explanation the author or authors have used the same item or very similar item in their study. In other cases, the items have been specifically created for the purposes of this study based on literature findings of existing literature.

Reliability of the variables is evaluated with Cronbach's alpha calculations. They provide indication on the reliability of the variable based on covariance of the items designed to measure that variable (Singleton & Straits, 2018). The weakness of the Cronbach's alpha is that it measures mainly the homogeneity of the data meaning whether the participants have answered consistently to each item. This means that some answers despite being correct and truthful can affect the alpha value negatively because it is in controversy to other answers by that participant. (Cortina, 1993) Yet the alpha reveals the interrelatedness of the measurement items (Sijtsma, 2009). For the purposes of this study that is sufficient.

The Cronbach's alpha values indicates the potential need to redesign some of the items in the survey for the final survey. After ensuring that the reliability of the variables is sufficient, the main study was conducted. All values should be above .700 after redesign changes.

6.3.1 Cronbach's alpha values - pilot

The results of the Cronbach's alpha analysis led to the following conclusions on the items used in the pilot. The alpha values for each of the variables are summarised in table 2. Some of the items have been reversed or an item has been removed after negative alpha or low alpha value in the original results (see second column in table 2). In this section the actions and changes taken to improve the low alpha values are described.

Table 2 Cronbach's alpha values - pilot

Variable	Original Alpha	Actions	New Alpha
Intention to continue use	.776	-	-
Trust	.486	remove item 2	.566
Satisfaction	.881	-	-
Confirmation	.675	remove item 2	.802
Perceived cost of use	.596	-	
Perceived benefit of use	.645	remove item 4	.831
Attitude towards use	.641	-	-
Use orientation	-.506	no significant improvement could be made	-
Dimensions of privacy	.828	-	-
Social influences	.657	-	-
Privacy awareness	.165	remove item 3	.715

Of the eleven variables satisfaction, dimensions of privacy perceptions and social influences are confirmed to have items that measure the corresponding variable with sufficient reliability and therefore require no changes. The alpha values are all above the threshold of 0.600. Additionally, reversing the answers to intention to continue use question 1 and attitude towards use question 3 improved the alpha values significantly. For intention to continue use the improvement is from .324 to .776 and for attitude towards use from -.217 to .641.

Some of the variables require items to be removed in order to be reliably measured by the remaining items. Trust variable is reliably measured by the remaining items after the removal of question 2. In the case of confirmation removing question 2 would make it a lot more reliable with three items remaining to measure the variable. After analysis the decision is made to remove it as there is no significant reason to keep it, such as the variable measuring a different aspect of the variable than the rest of the items. Perceived benefit of use, similar to confirmation, has a higher than threshold alpha value but can be improved by removing question for 4 from .645 to .831. After reconsideration of the question, it seems that it is irrelevant for some SNSs that the participants had considered. This leads to the conclusion that the item could be removed for the final survey. However, as there are 4 items in the variable the item remains but will be removed after final study results come in if it negatively affects the Cronbach's alpha value.

Awareness and perceived cost of use variables require redesign of some of the items in order to improve the alpha values. Question 3 of perceived cost of use is changed to "There would be severe consequences if my personal information was compromised". Additionally, item "There would be severe consequences if my account were breached" is added to provide an alternative for the analysis of the full survey. Question 3 of awareness should, based on the results, be either removed or redesigned. The problem with the question has been discussed frequently in the literature including the literature already reviewed in this study; users not reading the privacy policy document (Bechmann, 2014; Obar & Oeldorf-Hirsch, 2020; Custers, Van Der Hof & Schermer, 2014). Users, despite being privacy aware, do not read the privacy policies meaning most of the

answers to the question 3 are negative while answers to other questions are positive. This results in a low alpha value. To maintain three items for the awareness variable the question 3 is redesigned to "I am aware that the service has a privacy policy" which better measures privacy awareness.

Cronbach's alpha value for use orientation is negative. Reversing the items did not result in a satisfying alpha in any combination. Additionally removing items would not result in alpha value above 0.600. Analysis on item wording and coding revealed that they are designed wrong and need to be redesigned. The original items had been designed based on study findings of Vishwanath, Xu and Ngoh (2018) and influenced by several other surveys in terms of item wording and coding.

The redesigned items are based on the work by Kari, Salo and Frank (2020) In their study they use a single item to measure use orientation with answer options each representing different orientation, hedonistic, utilitarian or both. From this the original Likert scale of 1 to 5 with 1 being "completely disagree" and 5 "completely agree" is to be modified to 1 equalling "fully utilitarian" use and 5 equalling "fully hedonistic". In this scale three represents the "both" and "mixed use" alternative. To provide a more reliable measure three items using this scale are added to the survey.

6.3.2 Other results from the pilot

The pilot survey's open feedback results also suggest that in order to improve answer accuracy for some of the participants a Finnish translation of the study should be provided. Hence, for the final survey the whole content of the survey was translated from the original English language to Finnish as well. The translation was done by the author and by another individual unrelated to the study in order to reduce the effects of subjective interpretations by the author. The two translations were compared and based on the similarities and differences a combined translation was created.

The instructions for the participants were also revised after the pilot result analysis. Eight of the 31 participants reported that they had considered multiple SNSs during the survey in the compulsory question at the end of the survey. One of the open feedback answers also included a comment from a participant who had been confused whether they were supposed to select only one service, or they could consider multiple. Based on this the instructions were made more explicitly inform the participant to select one SNSs to consider during the survey.

6.4 Main Study

In this subsection the main study will be described in terms of data collection and analysis methods used. The items used in the main study can be found in Appendix 2. It lists all the variables to be measured with their related measurement

items. In comparison to the table of Appendix 1 describing the items used in the pilot there is a column that has the Finnish translation of the survey items. As mentioned in the previous subsection 6.1 several changes were made to the survey based on the results of the pilot. Similar to the pilot study the data is first analysed in terms of reliability by using Cronbach's alpha. After the reliability is determined factor analysis is to be conducted on the items to confirm the number of variables measured and that the factors are well structured. The purpose and results of the factor analysis will be reviewed in section 6.2.2. The following subsections describe the used methodology of the study in more detail and provide arguments to support them in the context of this study.

6.4.1 Cronbach's alpha – main study

First, the reliability of the variable measures is to be determined by using Cronbach's alpha. As can be seen in table 3, seven of the eleven variables have an alpha value of over .700. Despite the changes made to the items based on the pilot some of the variables could not reach the mentioned threshold. The alpha values listed are the highest that could be reached with three measurement items left for the variable.

Table 3 Cronbach's alpha values - main study

Variable	**Alpha value**
Intention to continue use	.869
Trust	.741
Satisfaction	.872
Confirmation	.794
Perceived cost of use	.613
Perceived benefit of use	.686
Attitude towards use	.629
Dimensions of privacy	.898
Social influences	.612
Privacy awareness	.739
Use orientation	.838

Some of the variables measured lower alpha values than the pilot study results analysis suggested. The adjustments made to the items based on the pilot study were not sufficient to ensure above .700 reliability in the final study. All of the variables do however have over .600 alpha value meaning that, while the reliability is suboptimal for some of the variables (< .700), the variables are reliable enough to be used in factor and regression analysis (Tavakol & Dennick, 2011). All of the results generated using the variables that display suboptimal reliability will have to be critically assessed.

6.4.2 Factor analysis

The aim of factor analysis is to help generate a more cohesive representation of the underlying constructs. This is done by identifying the number of latent variables, also called factors, in a set of measurement items. At the same time, it provides insight to the correlation structure by allowing the creation or confirmation of variables based on the factors that combine certain items within the item set. (Fabrigar & Wegener, 2012) In this study it is used to check whether the variables measured in the survey contain more than one underlying construct and should therefore be divided into multiple variables or have an item removed from them.

There are several criteria for the data to be used in factor analysis. Fabrigar and Wegener (2012) list adequacy of the of the items to measure the area of interest, soundness of measurement practices, and missing observation as these criteria. As the research framework has been constructed prior to survey items creation, the variables to be measured have been pre-identified during the literature review process. The measurement items are mostly directly based on existing literature while some have been designed based on theoretical findings. These items based on theoretical findings could potentially pose a problem. The issues are however addressed by the number of items and are mapped in the pilot study which revealed troublesome items that were then redesigned to better measure the targeted variable. These precautions should account for the adequacy of the items to measure the area of interest and offer a good baseline as for how many factors or variables there should be. Also, the items are designed based on prior published literature where they have either already been successfully utilised or where the topic has been discussed in detail which provided inspiration for item creation. This accounts for the sound measurement practices in combination with the data collection method being designed in a way that it follows the common guidelines of survey data collection. Additionally, an interval scale of 1-5 is used in all items to ensure that the measurement scale does not affect the analysis and in the end the results. Finally, the last matter in terms of data suitability is missing observations. This is taken into account during survey design as the survey does not allow the participant to submit the survey if there are missing responses in the survey document.

Under the conditions of my study, in terms of item quality (low reliability), a sample size of 200 would have been required according to Fabrigar and Wegener (2012). However, such numbers could not be reached during the data collection phase meaning that the results of the factor analysis and therefore the study should be critically considered. Additionally, as mentioned by Fabrigar and Wegener (2012) it is difficult to determine the quality of the data prior to actual analysis. All the necessary measures have been considered an attempt to ensure the quality of data. These measures are the mentioned pilot study, Cronbach's alpha analysis and the coming factor analysis.

The exploratory factor analysis is the chosen approach for this study to determine the constructs. A solid case could be made for confirmatory factor analysis to be used as there is a clear vision of the variables involved due to the

research framework being created using prior literature. However, as the research framework attempts to predict use orientation from a new perspective, that of privacy policies, there are many variables that have been simply identified from theoretical literature to measure this area of interest. Additionally, some of the items used have been merely inspired by theoretical findings in existing literature and there is no guarantee that the items truly measure the variable. Hence, the use of exploratory factor analysis and the need for it. This is supported by Fabrigar and Wegener (2012) who present a similar case as an example of a middle-ground situation where either approach can be used.

The factorability of the items is evaluated prior to assessing the results of the factor analysis. First, it is evaluated using a correlation matrix. The matrix results suggest that there is correlation higher than .300 between 37 of the 37 items with at least of other item in the item set. This suggests that the items have reasonable factorability. Second, the Kaiser-Meyer-Olkin measure and Bartlett's test of Sphericity are used. These values are displayed in table 4. The Kaiser-Meyer-Olkin measure of sampling adequacy is .733 which is above the recommended .6 further supporting factorability of the item set. Additionally, Bartlett's test displays statistical significance.

Table 4 Kaiser-Meyer-Olkin Measure and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.733
Bartlett's Test of Sphericity	Approx. Chi-Square	2745.857
	df	666
	Sig.	<.001

Third, the communalities table of the items is reviewed. The table is displayed in table 5. The table displays relatively high values for all items with very few exceptions. The extraction value for attitude measurement item 3 (Att3) is .313 but it is still above .300. The only item below the threshold is social influence measurement item 3 (SocInf3) which has the initial value of .288 and extraction value of .102. This suggests that SocInf3 does not have much common variance with other items in the item set. However, as the overall impression of the factorability of the items is reasonable, the item set is suitable for factor analysis.

Table 5 Communalities of survey items

Item	**Initial**	**Extraction**
UseCont1	.682	.618
UseCont2	.783	.873
UseCont3	.681	.648
UseCont4	.820	.777
UseCont5	.822	.845
Trust1	.587	.618
Trust2	.564	.509
Trust3	.462	.457
Sati1	.758	.704

Sati2	.715	.602
Sati3	.699	.628
Sati4	.690	.623
Conf1	.691	.592
Conf2	.572	.455
Conf3	.666	.564
PercCost2	.570	.441
PercCost3	.685	.732
PercCost4	.665	.700
PercBen1	.591	.525
PercBen3	.560	.573
PercBen4	.683	.551
Att2	.472	.573
Att3	.475	.313
Att4	.496	.497
Dimension1	.677	.685
Dimension2	.721	.759
Dimension3	.764	.815
Dimension4	.641	.644
SocInf1	.621	.690
SocInf2	.646	.654
SocInf3	.288	.102
Awa1	.574	.619
Awa2	.597	.615
Awa3	.544	.577
UseO1	.752	.765
UseO2	.652	.563
UseO3	.681	.734

Principal axis factoring is used as it allows an exploratory factor analysis to be conducted. This is the chosen method of factor analysis due to the reasons mentioned earlier in the previous section. Initial eigenvalues presented in table 6 show that the first five factors, that have eigenvalues above 2, explain around 17.9%, 12%, 9.2%, 7.2%, 6.6% of the variance respectively adding up to a cumulative variance explanation of 52.9 %. Factors up to ten have eigenvalues over one, and each explain between 4.4 % and 3 % of the variance. Adding these to the cumulative count results in 71.2 % of variance being explained. The ten-factor solution supports the research framework (figure 8) created for this study and vice versa, which is why the solution is selected as the one to be further analysed. The factors are mainly formed around the item combinations that have been planned to measure a particular variable. There are eleven variables in the research framework and the same number can be reached by separating the trust and satisfaction items from each other. Thematically the items are not close to each other, and common factor name is not easily recognisable and therefore the merging of the items is most likely caused by very high correlation.

Table 6 Factor analysis - Eigenvalues 1

	Initial Eigenvalues			**Extraction Sums of Squared Loadings**			**Rotation Sums of Squared Loadings**
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	6.635	17.932	17.932	6.256	16.909	16.909	4.621
2	4.424	11.957	29.889	4.056	10.962	27.871	3.757
3	3.399	9.187	39.076	3.108	8.399	36.270	2.469
4	2.659	7.188	46.264	2.340	6.324	42.593	2.437
5	2.465	6.661	52.925	2.098	5.669	48.263	2.492
6	1.639	4.430	57.356	1.245	3.366	51.628	2.149
7	1.544	4.173	61.529	1.104	2.984	54.612	2.052
8	1.356	3.666	65.195	.974	2.631	57.243	3.873
9	1.144	3.092	68.287	.798	2.156	59.399	2.886
10	1.102	2.978	71.264	.662	1.789	61.189	2.086
11	.974	2.633	73.898				
12	.933	2.521	76.419				
13	.815	2.204	78.623				
14	.722	1.952	80.575				
15	.640	1.729	82.304				
16	.601	1.624	83.928				
17	.558	1.507	85.435				
18	.507	1.369	86.804				
19	.489	1.321	88.125				
20	.438	1.183	89.308				
21	.427	1.155	90.463				
22	.416	1.124	91.587				
23	.344	.931	92.518				
24	.314	.848	93.366				
25	.298	.805	94.171				
26	.271	.734	94.905				
27	.262	.708	95.613				
28	.240	.649	96.262				
29	.218	.589	96.851				
30	.208	.563	97.414				
31	.179	.485	97.899				
32	.167	.451	98.350				
33	.155	.418	98.768				
34	.143	.388	99.156				
35	.125	.339	99.494				
36	.106	.286	99.780				
37	.081	.220	100.000				

After further analysis some of the items have been eliminated improve the factor structure of the survey. A total of six items do not meet the minimum

criterion of having factor loadings above .400 and no cross loadings above .300. SocInf3 does not reach the factor loading threshold with primary factor loading of -.235 and is therefore eliminated. Similar to SocInf3, Confirmation measurement item 2 has been eliminated as its primary factor loading is only -.320 and it also has a cross loading of .295 towards another factor. Due to a cross loading of .305 and a low primary loading at -.451 Confirmation measurement item 1 has been eliminated as the value surpasses the cross-loading threshold. Fourth item to not meet one of the criteria is Perceived cost 2. It has primary loading of only .378 and a close-to-threshold cross loading of -.279 meaning that it will also be removed. The final two items not to meet the criteria are Satisfaction item 3 (Sati3) and 4 (Sati4). Both have a cross loading over .300 with the factor consisting of Perceived benefit items. This is expected, as there is, according to theory, a strong correlation between perceived benefit and satisfaction among service users. However, as Sati3 has clearly over threshold cross loading of -.378 and only a moderate primary loading measuring .544 it will be removed. Sati4 will remain for further analysis as it is at the threshold with a cross loading of -.301 and also has a moderate primary loading of .568 meaning that it is not clearly an issue.

In addition to these four, two of the five items from the use continuance variable are to be removed. This is due to the items separating from the other three into their own factor. However, the main reason for removing the factor is that it is not necessary in terms of the topic of the study. After analysing the questions associated with the items, it appears that the remaining three items measure use continuance in association to a privacy risking incident, which is in line with the topic and the goals of this study. The two to be removed measure overall potential use continuance if nothing changes in the service.

After these changes further analysis on the item set is conducted. Again, the primary axis factoring is run on the item set that has been reduced to 30 individual items. The total variance explained table presented in table 7 demonstrates that the overall explanation value of the factors has improved over the first attempt after removing the items listed earlier. Earlier, ten factors were able to explain 71% of the variance and now 73% is reached with nine factors. Based on the items removed after the initial factor analysis the eleven-factor model has been changed to a ten-factor model due to confirmation measurement items being either removed or combined with other measurement items. Again, this ten-factor state can be reached by separating the Satisfaction and Trust items as argued earlier.

Table 7 Factor analysis – Eigenvalues 2

	Initial Eigenvalues			**Extraction Sums of Squared Loadings**			**Rotation Sums of Squared Loadings**
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	5.380	17.933	17.933	5.017	16.725	16.725	3.756
2	3.580	11.932	29.865	3.193	10.643	27.367	2.789

3	2.949	9.829	39.695	2.626	8.754	36.121	2.372
4	2.498	8.327	48.022	2.148	7.161	43.282	1.781
5	2.248	7.492	55.514	1.944	6.479	49.761	2.703
6	1.510	5.032	60.547	1.156	3.854	53.615	1.981
7	1.466	4.888	65.435	1.058	3.527	57.142	3.372
8	1.256	4.186	69.621	.908	3.027	60.168	2.298
9	1.094	3.648	73.268	.671	2.237	62.406	2.026
10	.900	2.999	76.267				
11	.779	2.596	78.863				
12	.699	2.330	81.193				
13	.571	1.903	83.096				
14	.537	1.789	84.885				
15	.503	1.677	86.563				
16	.449	1.498	88.061				
17	.415	1.383	89.444				
18	.387	1.291	90.735				
19	.361	1.205	91.939				
20	.324	1.080	93.019				
21	.294	.981	94.000				
22	.280	.933	94.933				
23	.258	.859	95.792				
24	.246	.819	96.611				
25	.203	.677	97.287				
26	.188	.626	97.913				
27	.171	.571	98.484				
28	.167	.558	99.042				
29	.150	.499	99.541				
30	.138	.459	100.000				

The changes resulted in a more structured model. There are only three items that do not meet the criteria thresholds of .400 primary loading and no cross loading over .300. The three remaining Satisfaction items 1, 2 and 4 have cross loadings of .335, .309 and .391 respectively towards the perceived benefit factor. As discussed earlier there is likely a strong correlation between the two variables which causes the cross loading. The first two Satisfaction items however have strong primary loadings measuring at .691 and .634 meaning that the cross loadings can be overlooked. Sati4 has a weaker primary loading measuring at .483 but after further analysis with the item removed the conclusion is reached that this nine-factor structure with these items has the best overall loadings.

After the minor change of satisfaction and trust items being separated into their own factors, the final variable structure for the regression analysis is reached. In summary, seven items are removed to improve the factor structure. These are Use continuance 4 and 5, Confirmation 1 and 2, Social Influences 3, Satisfaction 3 and Perceived Cost 2. The remaining item planned to measure confirmation of expectations is moved to perceived benefit variable item group as it

based on the factor analysis and careful inspection of the item coding measures the perceived benefit.

6.4.3 Changes to the research framework

Due to the issues that emerged during factor analysis regarding structure of the variables the model has been modified to better fit the data gained during data collection. The changes are necessary as there are shortcomings in the design of the survey items. The modified research framework is presented in figure 9.

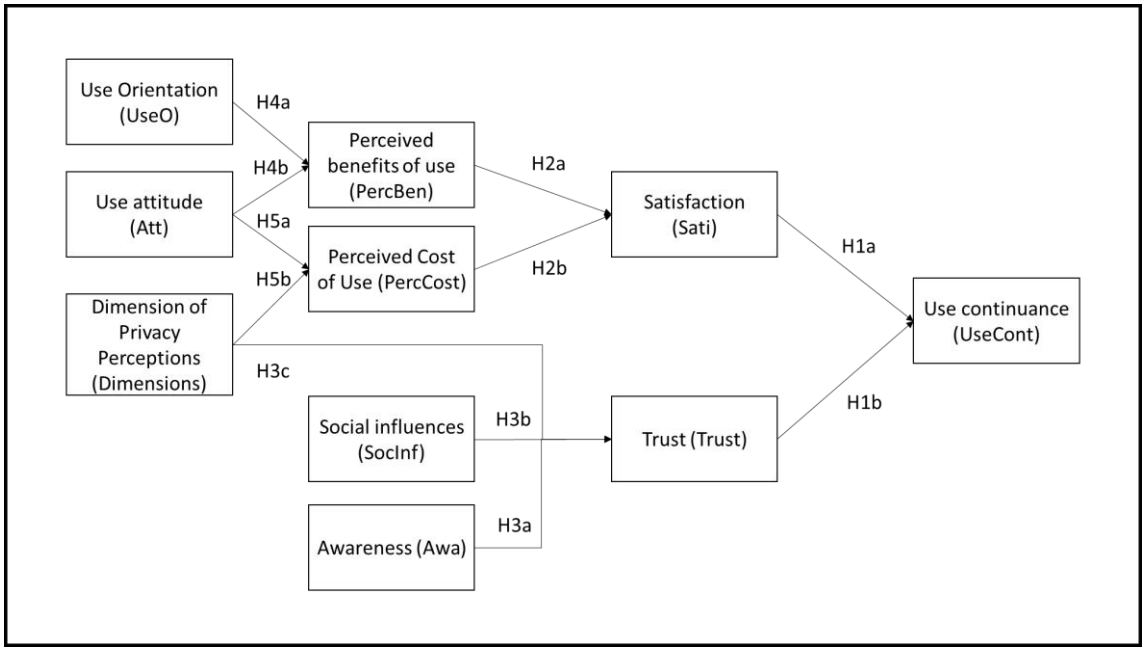

Figure 9 Modified research framework

In comparison to the original research framework illustrated in figure 8 the new altered framework does not have confirmation as a variable. Factor analysis demonstrates that the variable had a negative effect on the overall clarity of the factor and variable structure. As can be seen in figure 9 most of the hypothesis remain unchanged except for the hypothesised relationships between satisfaction, perceived benefit of use and perceived cost of use. The updated hypotheses are summarized in writing in table 8.

Table 8 Hypotheses for the analysis

Hypothesis	Description
H1a	Satisfaction has a positive effect on use continuance intention
H1b:	Trust has a positive effect on use continuance intention
H2a	Perceived benefit of use has a positive effect on satisfaction
H2b	Perceived cost of use has a negative effect on satisfaction
H3a	Awareness has negative effect on trust
H3b	Social influences have a positive effect on trust

H3c:	Dimensions of privacy perceptions have a negative effect on trust
H4a	Use orientation has a negative effect on perceived benefit of use
H4b	Use attitude has a negative effect on perceived benefit of use
H5a	Use attitude has a positive effect on perceived cost of use
H5b	Dimensions of privacy perceptions have a positive effect on perceived cost of use

6.5 Procedure

The participants were recruited via email. In the case of the pilot study the mailing list used only reached students of the faculty of information technology. For the main study the distribution was expanded by using other faculty mailing lists. In the email the potential participants were provided with two links to answer the survey either in English or Finnish. A short description of the topic and objectives of the study was also included in the email along with information on data use and anonymity. A more detailed version of the information was provided to the participants in the beginning of the survey with the addition of a notification that the participant may quit the survey at any point during the survey and no answers will be collected if the survey is closed before submitting.

Regarding answering and submitting the survey, submitting the online survey answer required the participant to answer every question apart from the open feedback and the enquiry on which service the participant considered during the survey. The mandatory questions utilised radio buttons which the participant needed to press to answer the question. The combination of these restrictions resulted in a data set with no missing or out of bounds values for any participant.

7 Results

This section contains a summary of the results. The chosen method of analysis is regression analysis and more specifically multiple regression. SPSS is used as the statistical tool of choice to conduct the regression analysis. Regression analysis is used to determine whether another variable or a set of variables can be used to predict the value of a target variable. Most common uses for regression analysis are modelling a relationship between variables, prediction of the target variable and hypothesis testing. (Chatterjee & Simonoff, 2012) The section is divided into two parts. First, the descriptive statistics of the collected data set will be reviewed. After that the chosen analysis approach and the results of the analysis will be introduced.

7.1 Descriptive Statistics

Table 9 contains the minimum value, maximum value, mean and standard deviation for each of the ten variables. The descriptive statistics for the variables were calculated based on the answers, provided by the 134 participants, to the questions in the survey. Most of the standard deviations are low (< 1) meaning that the participants' scores were close to the mean values presented in the table. Two variables, perceived cost of use and use orientation, display slightly higher standard deviations are still close to low. The minimum and maximum values suggest that low score (1) and high score (5) answers across all items can be found in almost all of the variables.

Table 9 Descriptive statistics for the variables

Variable	**N**	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
Use Continuance Intention	134	1.00	5.00	2.55	0.975
Trust	134	1.00	5.00	2.69	0.800
Satisfaction	134	1.00	5.00	3.66	0.821
Perceived Cost of Use	134	1.00	5.00	3.16	1.135
Perceived Benefit of Use	134	2.00	5.00	4.12	0.635
Attitude Towards Use	134	1.33	5.00	4.22	0.706
Dimensions of Privacy Perceptions	134	1.00	5.00	4.10	0.873
Social Influences	134	1.00	5.00	4.24	0.997
Privacy Awareness	134	1.00	5.00	4.11	0.772
Use Orientation	134	1.00	5.00	2.66	1.065

Several conclusions can be made from these statistics. Dimensions of privacy perceptions mean score of 4.10 suggests that users are generally interested in preserving their privacy in SNSs and the mean score of 4.22 for attitude towards use

supports this. Additionally, participants commonly report that their social group has affected their judgement when joining the SNS. Statistics also report relatively high mean scores for perceived benefit of use and privacy awareness. The rest of the mean scores for the variables are close to the middle value of 3.00.

7.2 Regression Analysis

A correlation analysis was conducted prior to regression analysis using Pearson's correlation to ensure that the required correlation between variables is there for at least one of the variables in each hypothesis pairing. The correlations will be discussed in more detail in section 8.2 as they provide interesting implications. The analysis showed that the required correlations to run regression analysis could be found. The results of the regression analysis are summarised in figure 10. Overall, the research model built based on existing literature has been mostly rejected. Four of the ten hypotheses are supported by the results. The explanatory power of the model is weak with only trust predicting use continuance and with a limited positive R^2 value of .037. Additionally, the statistical significance of the of the relationship is $p < .05$. This subsection contains a detailed description of the analysis results, which are summarised in table 10, for each hypothesis.

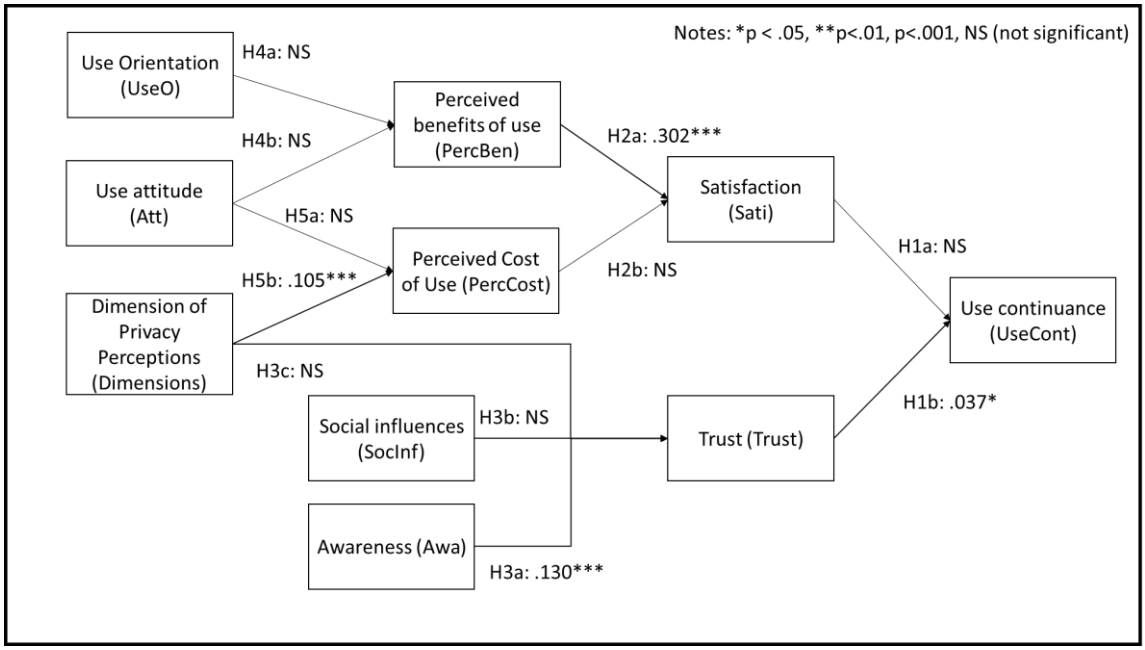

Figure 10 Summary of regression analysis results

Table 10 Regression analysis results

Dependent Variable	**Hypothesis**	**Independent Variables**	**Std. β**	**Sig.**
Use Continuance Intention	H1a	Satisfaction	.041	.686

R^2 = .037, $F(1, 132)$ = 5.100, p = .026, d = 2.217	H1b	Trust	.235	.026
Satisfaction R^2 = .302, $F(1, 132)$ = 57.101, p < .001, d = 2.205	H2a	Perceived Benefit of Use	.710	<.001
	H2b	Perceived Cost of Use	.023	.752
Trust R^2 = .130, $F(1, 132)$ = 19.780, p < .001, d = 2.213	H3a	Privacy Awareness	-.374	<.001
	H3b	Social Influences	.059	.472
	H3c	Dimensions of Privacy Perceptions	-.117	.158
Perceived Benefit of Use R^2 = .004, $F(1, 131)$ = .276, p < .759, d = 1.870	H4a	Use Orientation	-.009	.910
	H4b	Attitude Towards Use	-.039	.460
Perceived Cost of Use R^2 = .105, $F(1, 132)$ = 15.542, p < .001, d = 2.019	H5a	Attitude Towards Use	.119	.193
	H5b	Dimensions of Privacy Perceptions	.422	<.001

Multiple linear regression was used to test if satisfaction and trust significantly predicted use continuance intention. The overall regression was statistically significant (R^2 = .037, $F(1, 132)$ = 5.100, p = .026). It was found that satisfaction did not significantly predict use continuance (β = .041, p = .686). This means that H1a is rejected as the effect of satisfaction on use continuance intention is not statistically significant. It was also found that trust significantly predicted use continuance (β = .235, p = .026). Therefore, H1b is accepted as the results support the hypothesis that trust positively affects use continuance intention. The Durbin-Watson test value was d = 2.217, which is between the desired range of 1.5 < d < 2.5 and suggests there is no autocorrelation between the variables.

H2a and H2b concerned if perceived benefit of use and perceived cost of use significantly predicted satisfaction. The overall regression was discovered to be statistically significant (R^2 = .302, $F(1, 132)$ = 57.101, p < .001). The analysis revealed that perceived benefit of use significantly predicted satisfaction (β = .710, p < .001). This supports the hypothesis H2a which is accepted as it is. However, perceived cost of use did not significantly predict satisfaction (β = -.023, p = .752). H2b is hence rejected. The Durbin-Watson test value was d = 2.205, which suggests there is no autocorrelation between the variables of the overall model.

H3a, H3b and H3c suggest that privacy awareness, social influences and dimensions of privacy perceptions significantly predict trust. Based on the analysis the overall regression was statistically significant (R^2 = .130, $F(1, 132)$ = 19.780, p < .001). Privacy awareness significantly predicted trust (β = -.374, p < .001) according to the data. This results in hypothesis H3a being accepted. Privacy awareness has a negative effect on trust towards the service provider. It was found that social influences did not significantly predict satisfaction (β = .059, p = .472), and that dimensions of privacy perceptions did not significantly predict

satisfaction (β = -.117, p = .158) either. H3b and H3c are rejected as a result. The Durbin-Watson test value was d = 2.213 suggesting there is no autocorrelation between privacy awareness and trust.

H4a and H4b were tested to see if use orientation and attitude towards use significantly predicted perceived benefit of use. The overall regression was not statistically significant (R^2 = .004, F(1, 131) = .276, p < .759). It was found that use orientation did not significantly predict perceived benefit (β = -.009, p = .910). It was found that attitude towards use did not significantly predict perceived benefit (β = -.039, p = .460). The Durbin-Watson test value was d = 1.870 and suggests there is no autocorrelation between the variables. As the overall model is not statistically significant both H4a and H4b are rejected.

The final two hypotheses state that attitude towards use and dimensions of privacy perceptions significantly predict perceived cost of use. The analysis on the data revealed that overall regression was statistically significant (R^2 = .105, F(1, 132) = 15.542, p < .001). Attitude towards use was determined to not significantly predict satisfaction (β = .119, p = .193) resulting in H5a being rejected. The analysis revealed that dimensions of privacy perceptions significantly predicted satisfaction (β = .422, p < .001). H5b is accepted based on this result. The Durbin-Watson test value was d = 2.019, which means there is no autocorrelation between the variables.

Table 11 summarises the support of the hypotheses. As can be seen, only 4 of the 11 hypotheses are supported by the results. As the tested model is constructed from a very theoretical standpoint this result is not completely unexpected. There are some significant limitations to this study as well. The result does have several implications and interesting notions regarding the literature findings presented in the theory section of this study. Additionally, the result of the analysis presents the need for a set of new research topics in this area of interest. These will be discussed in detail in the following section.

Table 11 The hypotheses and their support

Hypothesis	**Supported**
H1a: Satisfaction has a positive effect on use continuance intention	No
H1b: Trust has a positive effect on use continuance intention	Yes
H2a: Perceived benefit of use has a positive effect on satisfaction	Yes
H2b: Perceived cost of use has a negative effect on satisfaction	No
H3a: Awareness has negative effect on trust	Yes
H3b: Social influences have a positive effect on trust	No
H3c: Dimensions of privacy perceptions have a negative effect on trust	No
H4a: Use orientation has a negative effect on perceived benefit of use	No
H4b: Use attitude has a negative effect on perceived benefit of use	No
H5a: Use attitude has a positive effect on perceived cost of use	No
H5b: Dimensions of privacy perceptions have a positive effect on perceived cost of use	Yes

8 Discussion

In this section the results presented in the previous section will be discussed. The findings have some interesting suggestions in terms of the relationship between privacy policy associated factors and SNS use continuance. The main findings will be discussed first. After the findings, the limitations of the study will be identified. Finally, the implications to both practice and theory will be discussed in dedicated subsections.

8.1 Main Findings

One of the main findings of the analysis is that satisfaction with the service has no effect on the intention to continue using the service if there is a privacy incident. Trust on the other hand has the hypothesised relationship with use continuance intention. However, trust towards service provider predicts only a small amount of variation in use continuance. All of these suggest that there are a limited number of factors that predict use continuance behaviour when the service experiences privacy issues. Most importantly, the factors that significantly predict use continuance in this context are different from the use continuance factors used to predict use continuance under regular use.

Based on the results the research question set in the beginning of the study can be answered, privacy awareness and trust influence use continuance after a privacy compromising incident. The role of privacy awareness is interesting as it negatively affects trust towards the service provider, meaning that a higher level of privacy awareness results in the user being more likely to stop using the service after a privacy incident due to lower trust towards the service provider. On the other hand, lack of awareness correlates with higher trust towards the service provider which in turn results in higher likelihood of the user continuing the use of service after a privacy compromising incident.

The results regarding the role of satisfaction are interesting as well. In prior research, satisfaction has been determined as a strong predictor of continuance intention (Bhattacherjee, 2001). Overall, satisfaction is considered to have an impact on user behaviour based on various studies according to Ofori et al. (2015). The results from Ofori et al. (2015) study indicate that in regular use, where no privacy incident is thought to occur, privacy concern and perceived risk do not directly affect use continuance intention. Instead, they affect satisfaction which then in turn affects continuance intention with high statistical significance. (Ofori, Fianu, Larbi-Siaw, Gladjah & Boateng, 2015) The research framework for this study was constructed based on that same expectation. However, the result of the current study suggests that there is no correlation between satisfaction in the service and use continuance intention. Based on the findings, a conclusion can be drawn about the significance of the incident aspect included in the current study.

In contrast to use behaviour under normal circumstances (when no privacy or security incident has taken place), use behaviour in the case of a privacy incident is significantly different as the level of user's satisfaction in the service no longer affects use continuance intention even though it is the main predictor of continuance intention when no incident occurs.

Another interesting finding concerns perceived cost and perceived benefit of use. Existing literature suggests that the two variables both affect satisfaction in the form of cost-benefit considerations (Xu, Michael & Chen, 2013; Dienlin & Trepte, 2015). The direct relationship between cost-benefit considerations and satisfaction in this study is however a result of confirmation item design issues. Confirmation of benefit and cost expectations variable was originally included as a connecting factor between cost-benefit considerations and satisfaction as the combination of variables has been used in past research as well (Oghuma et al., 2016; Bhattacherjee, 2001; Oliver, 1980). Factor analysis demonstrated that the confirmation items did not measure the same underlying factor. The items instead measured perceived benefit and perceived cost instead of the properly measuring the confirmation of expectation. The removal of the variable and combining of the items with other variables resulted in the modified version of the original research framework where perceived benefit of use and perceived cost of use are connected predicted to directly correlate with satisfaction without the confirmation variable in between. The results indicate that perceived benefit predicts with statistical significance around 30 % of the variation in user satisfaction. This is supported by existing literature (Bhattacherjee, 2001; Oghuma et al., 2016). Perceived cost of use however did not affect satisfaction. One potential reason for this is that the confirmation variable suggested by earlier research is a necessary factor to form the string of correlations leading from cost to satisfaction. The work of Susanto, Chang and Ha (2016), yet in the context of mobile banking services, relates to this topic as the original research framework for this study, in figure 8, included the confirmation variable. Their findings suggest that confirmation of expectations has a significant impact on trust and user satisfaction. Their approach to measuring confirmation is different than the one taken originally in this study. The need for confirmation to serve as a connecting variable does not affect perceived benefit similar to perceived cost. Despite the variables being associated by the cost-benefit consideration perspective the results suggest there is a difference in how they affect satisfaction and user's privacy behaviour.

The dimensions of privacy perceptions variable is central to this study as it addresses the privacy incident perspective by measuring how individuals value various aspects of privacy. Dimensions of privacy perception were expected to negatively affect trust. The results of the current study rejected the proposed relationship. However, dimensions of privacy perceptions are confirmed to positively affect the perceived cost of use. These relationships were formed based on the assumption that the perceived severity of a privacy incident affecting certain dimensions of privacy would affect perceived cost and trust (Vishwanath, Xu & Ngoh, 2018). The confirmed relationship between dimensions of privacy perceptions and perceived cost of use should however be taken critically as the

perceived cost of use variable has a below .700 alpha value which could affect the results.

All of the hypotheses with attitude towards use and social influences did not have significant relationships with other variables as was proposed. In the literature reviewed for the research framework design use attitude is often associated with cost-benefit considerations as was done in this study as well (Child, Haridakis and Petronio, 2012). Social influences are also frequently discussed in literature and included in models as an affecting factor to trust towards the service provider and use continuance (Wang, Asaad & Filieri, 2020; Child, Haridakis & Petronio, 2012; Custers, Van Der Hof & Schermer 2014). The reason for the result of this study could potentially be the insufficient alpha values of these two variables. As can be seen in table 3 the alpha value for social influences is .612 and for attitude towards use .629.

It was also predicted that use orientation would affect perceived benefit of use but the results did not support the relationship. The prediction was formed based on the discussions in the article by Child, Haridakis and Petronio (2012) where they associate use orientation with privacy behaviour. The connection with perceived benefit of use was suggested as an article by Vishwanath, Xu and Ngoh (2018) compared the types of benefits and discovered differences in the perceived value of different types of benefits. The type of benefit a user gain from using the service is dependent on the orientation of use as using the service for entertainment purposes will yield entertainment benefits. While the relationship is rejected, during regression analysis process a correlation between use orientation and use continuance intention was found. This relationship would also be supported by Kari, Salo and Frank (2020) who suggest in their study that use orientation does affect use continuance intention.

8.2 Limitations

The main limitation of this study is the accuracy of self-reported privacy concerns and behaviour towards an incident that has not happened. An experimental approach can be used to avoid this but with such an approach creating a realistic setting can be a challenge. This is a common issue for privacy studies when a survey approach is followed. The actual behaviour of the participants often differs from the behaviour the participants themselves report in the survey. This is further emphasised if the event, on which the participant self-reports, is infrequent such as privacy setting change in SNSs. (Kokolakis, 2017) Privacy policy change is similar in frequency to the privacy setting change by the user. Self-reported concerns only predict behaviour well when collected immediately before or after the actual behaviour as even time and context cause changes to behaviour (Chen, Ge, Li & Proctor, 2021).

Another limitation is in terms of variable measurement reliability as a satisfactory level could be reached. The items had sufficient reliability to enable further analysis on the data gathered. However, four of the eleven variables had the

measurement reliability less than .700 which would have been the desired value. All of the values are however above .600 meaning that all of the variables are measured with at least moderate reliability. Table 3 shows the four variables below the desired level of reliability: perceived benefit and cost, attitude towards use and social influences. The results of analysis conducted using these four variables should be particularly critically evaluated. However, the factor analysis should improve the reliability of the items as structure of the variables is improved. As a secondary Cronbach's alpha analysis has not been conducted after the factor analysis the results are still to be taken critically.

The sample size achieved in the online survey is also one of the limitations of the study. Due to the mentioned reliability issues of the items the participant count of 134 is not sufficient to compensate for the low reliability. With the reliability level of the items, 200 participants would have been desirable (Fabrigar & Wegener, 2012). This leads to the need to critically consider the results and raises the need to reconduct the study with the necessary changes based on this study. Additionally, as the sample consists of only students the generalisability of the results is to be assessed critically. This is further affected by the decision to not collect demographics from the participants which makes assessing the generalisability of results even more difficult.

Wide range of services considered can also be considered a limitation. SNSs cover a wide range of services as presented in the theory section. This is a limitation that had been identified early in the process, but the risk of mixed results was overlooked as the wider range of services enabled more individuals to participate in the study maximising the number of potential participants. The contextual nature of privacy seems to cause challenges for research when all types of SNSs are included. It has been suggested that contexts such as online shopping, SNSs and banking should be considered separately for example. (Kokolakis, 2017) However, such a broad divide into categories might not be sufficient. In this study the participants were free to choose the SNS as long as it is one that they commonly use in their everyday life. This resulted in SNSs ranging from instant messaging applications to complex social media platforms and even a gaming platform being included. Of the 134 total participants, 120 reported in a compulsory field which service they thought of when answering the survey. A majority of, or roughly 61 %, of the participants reported to have chosen WhatsApp as their service. The second most selected services were Instagram selected by 9 % and Facebook by 7.5 %. Other services selected had less than five participants. Those were Telegram, Snapchat, Discord, Signal and Steam. Additionally, 11 % of the participants reported to have considered more than one service despite the request to choose one at the beginning of the survey. Even under shallow analysis it can be discovered that there are considerable differences between the different types of SNSs on various topics such as use purpose and commitment. This results in the same questions being considered from multiple perspectives by the participants which could cause the answers to be inconsistent. The number of hypotheses rejected, and variable structure issues could potentially be caused by too many different types of SNSs being included.

8.3 Implications to Practice

The results of this study provide implications for SNS providers and practitioners. The finding that trust affects use continuance intention in privacy incident context highlights the service providers need to build trust with the users. As discussed in the section 3.2 the main purpose of privacy policies is to reduce privacy concern and build trust (Custers, Van Der Hof & Schermer, 2014; Sigmund, 2021; Wu, Huang, Yen & Popova, 2012). Therefore, the role of privacy policy should not be overlooked, and the information included in the policy should be made easily available to all users. Other forms of trust building should also be considered to ensure use continuance in the event of privacy incidents as trust is identified in this study as the single direct predictor of use continuance intention. Satisfaction in the service will not, based on the results, affect use continuance intention in the context of privacy incidents meaning that increasing user satisfaction and ensuring good use experience should not be valued over trust. Service providers need to carefully consider how they address user privacy in their service and privacy policies as well as changes to the privacy policy.

The results also have implications for practitioners whose goal is to promote safe privacy behaviour among individuals. Increasing privacy awareness of individuals has a negative effect on trust towards the service provider. Therefore, by increasing privacy awareness users will more likely abandon a service that no longer respects their privacy. The role of increasing privacy awareness in achieving better privacy behaviour is widely accepted and suggested in existing literature as it increases individuals' knowledge of matters related to their privacy from multiple perspectives (Soumelidou & Tsohou, 2020).

8.4 Future Research

The limitations of this study and discussion of the results raise several suggestions for future research. In this study the survey items were designed in a way that the selected service should not have significant effect on the answers, and this was further improved based on pilot study open feedback and data. In open feedback of the final study some of the participants reported difficulties at considering some of the questions based on their selected service. However, these were a minority with only six participants reporting such issues. Despite the item design and low number of issues reported the wide variety of different services likely affected the quality of data and results. The issues that emerged in the empirical part of study despite the counter measures indicate that future research should consider examining narrower ranges of SNSs. Additionally, in order to even better ensure the reliability of the results a larger sample size would also be recommended.

In terms of variable relationships to be investigated in future research, the combination of perceived cost of use, perceived benefit use, satisfaction, trust,

confirmation and use continuance intention should be further investigated particularly in the context of privacy. The parts of the research framework addressing these variables were constructed based on existing models (Oghuma et al., 2016; Wang, Asaad & Filieri, 2020) and earlier literature findings (Xu, Michael & Chen, 2013; Dienlin &Trepte, 2015). The context of privacy incidents seems to require a different approach, however. The prediction relationship between perceived benefit of use and satisfaction was confirmed in this study while perceived cost had no significant impact on satisfaction as was hypothesised. Also, the confirmation variable could potentially provide better results. In this study its role was not studied due to item design issues as discussed in the previous subsection and the methodology section. A study could be conducted also on the relationship of satisfaction and use continuance in this privacy incident context to either support or deny the lack of association between the two variables suggested by the results.

The discussion of the results offers one more topic for future research. The potential direct relationship between use orientation and use continuance intention should be addressed in future research. The relationship has been suggested by existing literature in a different context than that of this study (Kari, Salo & Frank, 2020). Empirical investigation into the relationship in the context of privacy policies and privacy incidents could be provide interesting results.

9 Conclusion

As information has become one of the biggest businesses in the modern world the privacy of users is now at risk (Wacks, 2010). SNS service providers benefit from information collected about their users and user behaviour (Camenish, 2012). Service providers do provide the users with the information on what type of data is collected, how it is being collected, how it is stored and what is the data used for. The document which contains this information is called a privacy policy. (Gerlach, Widjaja & Buxmann, 2015) Privacy policies should be seen as a tool for building trust with the users and informing them on matters that affect their privacy (Wu, Huang, Yen & Popova, 2012. Privacy policies are however often ignored by the users as they are seen as difficult to understand, too time consuming to read and not worth reading (Bechmann, 2014; Obar & Oeldorf-Hirsch, 2020; Custers, Van Der Hof & Schermer, 2014).

During continuous use of a SNS it is likely that there will be changes to the privacy policy of the service as service providers commonly adjust the documents (Baeth & Aktas, 2018). The changes to the privacy policies can potentially cause privacy issues to emerge. These issues, if severe enough, can be considered to be critical incidents. Critical incidents have been identified as a factor that negatively affects use continuance (Kari, Salo & Frank, 2020). Supporting continuous use of the service is important to the service providers to ensure success of the service (Kari, Salo & Frank, 2020; Bagayogo et al., 2014; Bhattacherjee, 2001). Understanding the relationship between privacy policy changes and use continuance is therefore important to service providers. It is also important for users as it can help understand the privacy compromising behaviour of users.

The aim of this study was to investigate that relationship by: identifying privacy policy associated factors that, based on existing literature, affect use continuance, facilitating the construction of a research framework and empirically testing it. The research question set in the beginning of the study: which privacy policy factors affect use continuance in case of a privacy incident? The results suggest that trust and privacy awareness are the only affecting factors of use continuance intention when there is a privacy incident. Trust towards service provider positively affects use continuance intention of the user while privacy awareness has a negative effect on trust.

The main implication of these results is that the role of trust during privacy incidents emphasizes the need for service providers to build trust with the users. Trust building is identified as the only direct way the service provider has to improve the likelihood of a user continuing service use after a privacy incident. One way to build trust is by creating a privacy policy the users will read and understand (Wu, Huang, Yen & Popova, 2012). The purpose of a privacy policy is to build trust and inform the users of matters that affect their privacy (Custers, Van Der Hof & Schermer, 2014; Sigmund, 2021; Wu, Huang, Yen & Popova, 2012). This naturally requires that the users read and understand the privacy policy.

The results also suggest that privacy awareness had a negative effect on trust towards service provider. The role of privacy awareness suggests a complicated relationship between use continuance and privacy policies particularly from the perspective of the service provider. Users who are more aware of the privacy issues related to SNSs are less likely to trust the service provider and therefore more likely to abandon the service. However, an easily understandable and clear privacy policy could potentially build sufficient trust to ensure continuing use despite privacy issues. On the other hand, the more privacy aware the users are the more likely they are to protect their privacy by abandoning the service that has privacy issues.

This study has its limitations mainly due to survey item design issues and number of participants. Despite the limitations, the findings and discussion on the results do provide interesting suggestions for future research in terms of relationships to be investigated.

REFERENCES

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. In: G. Danezis., P. Golle (editors) *Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science*, 4258(1). Springer, Berlin, Heidelberg. https://doi-org.ezproxy.jyu.fi/10.1007/11957454_3

Adamic, L. A. & Adar, E. (2003). Friends and neighbors on the Web. *Social networks, 25*(3), 211-230. https://doi.org/10.1016/S0378-8733(03)00009-1

Aïmeur, E., Lawani, O. & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in human behavior, 58*, 368-379. https://doi.org/10.1016/j.chb.2015.11.014

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior & Human Decision Processes*, 50(2), 179–211.

Angulo, J., Fischer-Hübner, S., Wästlund, E. & Pulls, T. (2012). Towards usable privacy policy display and management. *Information Management & Computer Security*, 20(1), 4-17. https://jyu.finna.fi/PrimoRecord/pci.emerald_s10.1108%2F09685221211219155

Baeth, M. J. & Aktas, M. S. (2018). An approach to custom privacy policy violation detection problems using big social provenance data. *Concurrency and Computation: Practice and Experience*, 30(21).

Bagayogo, F. F., Lapointe, L., & Bassellier, G. (2014). Enhanced use of IT: A new perspective on post-adoption. *Journal of the Association for Information Systems*,15, 361–387.

Bhattacherjee, A. (2001) "Understanding Information Systems Continuance: An Expectation-Confirmation Quarterly, 25(3), pp. 351-370.

Bechmann, A. (2014). Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of media business studies, 11*(1), 21-38. https://jyu.finna.fi/PrimoRecord/pci.informaworld_s10_1080_16522354_2014_11073574

Buckner, T. K. & Knowles, B. L. (2012). *Privacy: Management, legal issues, and security aspects*. Nova Science Publishers. https://jyu.finna.fi/Record/jykdok.1513927

Burgoon, J. K. (1982). Privacy and communication. *Communication Yearbook*, 6, 206– 249.

Camenisch, J. (2012). Information privacy? *Computer networks, 56*(18), 3834-3848. https://jyu.finna.fi/PrimoRecord/pci.elsevier_sdoi_10_1016_j_comnet_2012_10_012

Carmagnola, F., Osborne, F. & Torre, I. (2014). User data discovery and aggregation: The CS-UDD algorithm. *Information sciences*, 270(C), 41-72.

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. https://doi.org/10.1016/j.chb.2016.12.013

Chatterjee, S. & Simonoff, J. S. (2012). Handbook of regression analysis. John Wiley & Sons, Incorporated. Retrieved 2.12.2021 from https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=1108688

Chen, H., Chiang, R. & Storey, V. (2012). Business intelligence and analytics: from big data to big impact. *Mis Quarterly*, 36(4), 1165-1188. https://doi.org/10.2307/41703503

Chen, J., Ge, H., Li, N. & Proctor, R. W. (2021). What I Say Means What I Do: Risk Concerns and Mobile Application-Selection Behaviors. *Human factors,* 187208211004288. https://doi.org/10.1177/00187208211004288

Cheung, M. F. & To, W. (2017). The influence of the propensity to trust on mobile users' attitudes toward in-app advertisements: An extension of the theory of planned behavior. *Computers in human behavior, 76*, 102-111. https://doi.org/10.1016/j.chb.2017.07.011

Child, J. T., Haridakis, P. M. & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in human behavior, 28*(5), 1859-1872. https://jyu.finna.fi/PrimoRecord/pci.elsevier_sdoi_10_1016_j_chb_2012_05_004

Conger, S. (2009). Emerging technologies, emerging privacy issues. In: R. Luppicini, R. Adell, (editors). *Handbook of research on technoethics.* Hershey, PA: IGI Global. 767–793. https://doi.org/10.4018/978-1-60566-022-6.ch050

Cortina, J. M. (1993). What is Coefficient Alpha? An Examination of Theory and Applications. Journal of Applied Psychology, 78(1), 98–104. https://doi.org/10.1037/0021-9010.78.1.98

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104– 115. doi:10.1287/orsc.10.1.104

Custers, B., Van Der Hof, S. & Schermer, B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies. *Policy & Internet, 6*(3), 268-295. https://jyu.finna.fi/PrimoRecord/pci.wj10.1002%2F1944-2866.POI366

Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. https://doi.org/10.1002/ejsp.2049

Dong, T., Cheng, N. & Wu, Y. J. (2014). A study of the social networking website service in digital content industries: The Facebook case in Taiwan. *Computers in human behavior,* 30, pp. 708-714. doi:10.1016/j.chb.2013.07.037

Dowding, M. R. (2011). *Privacy: Defending an illusion*. Scarecrow Press. https://jyu.finna.fi/Record/jykdok.1709387

Edvardsson, B., & Roos, I. (2001). Critical incident techniques: Towards a framework for analysing the criticality of critical incidents. *International Journal of Service Industry Management*, 12, 251–268.

Fabrigar, L. R. & Wegener, D. T. (2012). *Exploratory factor analysis*. Oxford University Press.

Ghazinour, K. & Albalawi, T. (2016). A Usability Study on the Privacy Policy Visualization Model. In the *proceedings of Computing and Cyber Science and Technology Congress*, Auckland, August 8–12. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2016.109

Gerlach, J., Widjaja, T. & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The journal of strategic information systems, 24*(1), pp. 33-43. doi:10.1016/j.jsis.2014.09.001

Gordon, L. & Loeb, M. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), pp. 33-56. doi:10.3233/JCS-2009-0398

Healey, J. (2012). *Privacy and information rights*. Spinney Press. https://jyu.finna.fi/Record/jykdok.1747745

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2007). *Tutki ja kirjoita* (13. edition). Helsinki: Tammi.

Hong, S., Kim, J., & Lee, H. (2008). Antecedents of use-continuance in information systems: Toward an inegrative view. *Journal of Computer Information Systems*, 48, 61–73.

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H. & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on Theory of Planned Behavior. *Computers in human behavior, 62*, 545-561. https://doi.org/10.1016/j.chb.2016.04.024

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review, 50*(4), 1193-1294. https://doi.org/10.2307/1229286

Kari, T., Salo, M., & Frank, L. (2020) Role of situational context in use continuance after critical exergaming incidents. *Information Systems Journal*,30(3),596–633. https://jyu.finna.fi/Record/jyx.123456789_68744

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B. & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies, 71*(12), 1163-1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security, 64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Krasnova, H., Veltri, N. & Günther, O. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering, 4*(3), 127-135. https://doi.org/10.1007/s12599-012-0216-6

Li, H., Sarathy, R. & Xu, H. (2010). Understanding Situational Online Information Disclosure as a Privacy Calculus. *The Journal of computer information systems, 51*(1), 62-71. https://doi.org/10.1080/08874417.2010.11645450

Lumor, T., Pulkkinen, M. & Hirvonen, A. (2020). The Actual Adoption and Use of MobileApps : The Case of a Higher Education Context. In *AMCIS 2020 : Proceedings of the 26th Americas Conference on Information Systems* (pp. 1-10) https://jyu.finna.fi/Record/jyx.123456789_74024

McKnight, D. H., Choudhury, V., Kacmar, C. 2002. "The Impact of Initial Consumer Trust on Intentions to Transact with a Website: A Trust Building Model." Journal of Strategic Information Systems 11 (3): 297–323. https://doi.org/10.1016/S0963-8687(02)00020-3

Meier, Y., Schäwel, J. & Krämer, N. C. (2020). The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making. *Media and communication (Lisboa), 8*(2), 291-301. https://doi.org/10.17645/mac.v8i2.2846

Milton, A. C. & Mullan, B. A. (2012). An Application of the Theory of Planned Behavior—A Randomized Controlled Food Safety Pilot Intervention for Young Adults. *Health Psychology*, 31(2), 250-259. https://doi.org/10.1037/a0025852

Moore, A. (2008). Defining Privacy. *Journal of Social Philosophy, 39*(3), 411-428. https://doi.org/10.1111/j.1467-9833.2008.00433.x

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, 140*(4), 32-48. https://jyu.finna.fi/PrimoRecord/pci.mitpress10.1162%2FDAED_a_00113

Nyoni, P. & Velempini, M. (2018). Privacy and user awareness on Facebook. *South African Journal of Science*, 114(5/6), 27. https://jyu.finna.fi/PrimoRecord/pci.gale_ofa590727583

Obar, J. A. & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, communication & society*, 23(1), pp. 128-147. doi:10.1080/1369118X.2018.1486870

Ofori, K. S., Fianu, E., Larbi-Siaw, O., Gladjah, R. E. & Boateng, E. O. Y. (2015). Factors Influencing the Continuance Use of Mobile Social Media: The Effect of Privacy Concerns. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/2245-1439.426

Oghuma, A. P., Libaque-Saenz, C. F., Wong, S. F. & Chang, Y. (2016). An expectation-confirmation model of continuance intention to use mobile instant messaging. Telematics and informatics, 33(1), pp. 34-47. doi:10.1016/j.tele.2015.05.006

Oliver, R. L. (1980). A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions. *Journal of Marketing Research, 17*(4), 460-469. https://doi.org/10.2307/3150499

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Pratt, J. & Conger, S. (2009). Without Permission: Privacy on the Line. *International Journal of Information Security and Privacy (IJISP), 3*(1), pp. 30-44. doi:10.4018/jisp.2009010103

Punch, K. (2003). *Survey research: The basics*. Sage Publications.

Qian, J., Qiu, F., Wu, F., Ruan, N., Chen, G. & Tang, S. (2017). Privacy-Preserving Selective Aggregation of Online User Behavior Data. *IEEE Transactions on Computers, 66*(2), 326-338

Quintal, V. A., Lee, J. A. & Soutar, G. N. (2010). Risk, uncertainty and the theory of planned behavior: A tourism example. *Tourism management* (1982), 31(6), 797-805. https://doi.org/10.1016/j.tourman.2009.08.006

Riesch, H. (2012) Levels of uncertainty. In: *Handbook of risk theory*. Amsterdam: Springer, 87–110. https://doi.org/10.1007/978-94-007-1433-5_4

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of psychology*, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rule, J. B. (2007). *Privacy in peril*. Oxford University Press. https://jyu.finna.fi/Record/jykdok.1173444

Salo, M.& Frank, L. (2017). User Behaviours After Critical Mobile Application Incidents: The Relationship with Situational Context. *Information Systems Journal*, 27(1), 5-30. https://jyu.finna.fi/Record/jyx.123456789_55944

Sigmund, T. (2021). Attention Paid to Privacy Policy Statements. *Information (Basel), 12*(144), 144. https://doi.org/10.3390/info12040144

Sijtsma, K. (2009). On the Use, the Misuse, and the Very Limited Usefulness of Cronbach's Alpha. Psychometrika, 74(1), 107–120. DOI: 10.1007/S11336-008-9101-0

Singleton, R. A. & Straits, B. C. (2018). Approaches to Social Research (6th ed.). Oxford: Oxford University Press. ISBN 978-0195372984

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477. https://doi.org/10.2307/40041279

Soumelidou, A. & Tsohou, A. (2020). Effects of privacy policy visualization on users' information privacy awareness level. *Information Technology & People, 33*(2), 502-534. https://doi.org/10.1108/ITP-08-2017-0241

Susanto, A., Chang, Y. & Ha, Y. (2016). Determinants of continuance intention to use the smartphone banking services: An extension to the expectation-confirmation model. *Industrial management + data systems, 116*(3), 508-525. https://doi.org/10.1108/IMDS-05-2015-0195

Tavakol, M. & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education, 2*, 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

Tuttle, H. (2018). Facebook Scandal Raises Data Privacy Concerns. *Risk Management*, 65(5), 6-9. https://jyu.finna.fi/PrimoRecord/pci.proquest2101229017

Vatanasombut, B., Igbaria, M., Stylianou, A. C., & Rodgers, W. (2008). Information systems continuance intention of web-based applications customers: The case of online banking. *Information & Management*, 45, 419–428. doi:10.1016/j.im.2008.03.005

Vehkalahti, K. (2019). *Kyselytutkimuksen mittarit ja menetelmät*. Helsinki: Helsingin yliopisto.

Vilkka, H. (2007). *Tutki ja mittaa: määrällisen tutkimuksen perusteet*. Helsinki: Tammi.

Vishwanath, A., Xu, W. & Ngoh, Z. (2018). How people protect their privacy on facebook: A cost - benefit view. *Journal of the Association for Information Science and Technology*, 69(5), 700-709.

Wacks, R. (2010). *Privacy: A very short introduction*. Oxford University Press. https://jyu.finna.fi/Record/jykdok.1794203

Wang, Y., Asaad, Y. & Filieri, R. (2020). What Makes Hosts Trust Airbnb? Antecedents of Hosts' Trust toward Airbnb and Its Impact on Continuance Intention. *Journal of travel research*, 59(4), pp. 686-703. doi:10.1177/0047287519855135

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum

Wieringa, J., Kannan, P., Ma, X., Reutterer, T., Risselada, H. & Skiera, B. (2021). Data analytics in a privacy-concerned world. *Journal of business research, 122*, 915-925. https://doi.org/10.1016/j.jbusres.2019.05.005

Wu, K., Huang, S. Y., Yen, D. C. & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior, 28*(3), 889-897.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's information privacy concerns: Toward an integrative view. Proc. 29th Annual Internet Conf. Inform. Systems (ICIS 2008), Paris, France (AIS, Atlanta).

Xu, H., Dinev, T., Smith, J. & Hart, P. (2011). "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances." *Journal of the Association for Information Systems,* 12 (12): 798–824.

Xu, F., Michael, K. & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research*, 13(2), 151-168. doi: http://dx.doi.org.ezproxy.jyu.fi/10.1007/s10660-013-9111-6

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *Cyberpsychology & Behavior*, 11, 615–616. doi:10.1089/cpb.2007.0208.

Yousafzai, S. Y., Foxall, G. R., & Pallister, J. G. (2010). Explaining Internet banking behavior: Theory of reasoned action, theory of planned behavior, or technology acceptance model? *Journal of Applied Social Psychology*, 40, 1172–1202. doi:10.1111/j.1559-1816.2010.00615.x

APPENDIX 1 – PILOT SURVEY ITEMS

Variable	Measurement item	Reference
Use Continuance Intention	I might stop using the service in the future if the service had experienced a privacy incident	Oghuma et al. (2016)
	I will likely continue using the service in the future despite a privacy incident occurring	Oghuma et al. (2016)
	I will likely continue using the service for the next six (6) months despite potential privacy incidents	Oghuma et al. (2016)
	I will continue using the service as regularly as I do now	Wang, Asaad & Filieri (2020)
	I intent continue using the service in the future	Oghuma et al. (2016)
Trust	I believe that the service provider acts in my best interest	McKnight et al. (2002)
	I trust that the service provider provides enough safeguards for me to be safe using the service	McKnight et al. (2002)
	Service provider has informed me of all matters that affect my privacy	McKnight et al. (2002)
Satisfaction	I feel satisfied with the service	Oghuma et al. (2016)
	I feel content with the service	Oghuma et al. (2016)
	The service is pleasant to use	Oghuma et al. (2016)
	I am very pleased by the service experience	Oghuma et al. (2016)
Confirmation	The trade-off between cost and benefit of service use is fair	Based on Oghuma et al. (2016)
	The cost of service use is as I expected it to be	Based on Oghuma et al. (2016)
	I have received the benefit I expected to gain from the use of the service	Based on Oghuma et al. (2016)
Perceived cost of use	I disclose personal information to the service provider in exchange for use	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	The privacy risks associated with use are acceptable	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	There would be severe consequences if my personal information was compromised	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	There would be severe consequences if my account were breached	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
Perceived benefit of use	I gain benefit from using the service	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	The service allows me to pass time easily and entertain myself	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	The service allows me to effectively and conveniently interact with others	Adapted from findings by Vishwanath, Xu & Ngoh (2018) and Oghuma et al. (2016)
	The service allows me to easily find information about friends, activities, events, companies etc.	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	I enjoy using the service	Oghuma et al. (2016)
	I feel I can reveal personal information in social networking services	Adapted from findings by Dowding (2011), Child,

Attitude towards use		Haridakis and Petronio (2012), (Dienlin & Trepte, (2015), Ajzen (1991), Xu, Michael & Chen (2013) and Hong, Kim and Lee (2008)
	Revealing personal information on social networking services should be carefully considered	Adapted from findings by Dowding (2011), Child, Haridakis and Petronio (2012), (Dienlin & Trepte, (2015), Ajzen (1991), Xu, Michael & Chen (2013) and Hong, Kim and Lee (2008)
	I should only reveal the required personal information to set up a profile	Adapted from findings by Dowding (2011), Child, Haridakis and Petronio (2012), (Dienlin & Trepte, (2015), Ajzen (1991), Xu, Michael & Chen (2013), and Hong, Kim and Lee (2008)
	To me, it is most important to maintain privacy online	Xu et al. (2008)
Use orientation	I mainly use the service to entertain myself (videos, memes, etc.)	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	I mainly use the service to perform specific tasks (set up meetings, staying in touch with others, etc.)	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	The way I use the service varies between entertainment and performing tasks	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
Affected dimension of privacy	It is a serious problem if the privacy policy limits my ability to control my personal level of solitude in the service	Adapted from Buckner & Knowles (2012)
	It is a serious problem if the privacy policy limits my ability to control my personal level of intimacy in the service	Adapted from Buckner & Knowles (2012)
	It is a serious problem if the privacy policy limits my ability to control my personal level of reserve in the service	Adapted from Buckner & Knowles (2012)
	It is a serious problem if the privacy policy limits my ability to control my personal level of anonymity in the service	Adapted from Buckner & Knowles (2012)
Social influences	Members of my social group convinced me to join the service	Based on findings of Custers, Van Der Hof and Schermer (2014)
	I joined the service as many of the members of my social group were already members or going to be.	Based on findings of Custers, Van Der Hof and Schermer (2014)
	Disclosing personal information in SNSs is common among members of my social group	Based on findings of Custers, Van Der Hof and Schermer (2014)
Awareness	I'm aware of the privacy issues related to Social Networking Services	Xu et al. (2008)

	I read news and other articles regarding privacy when come by them	Xu et al. (2008)
	I have read the privacy policy of the service I use	Based on Wu et al. (2012), Bechmann (2014), Obar & Oeldorf-Hirsch (2020), Custers, Van Der Hof and Schermer (2014) and Acquisti & Gross (2006)

APPENDIX 2 – MAIN SURVEY ITEMS

Construct	Measurement item	Suomeksi	Reference
Intention of Use Continuance (UseCont)	I might stop using the service in the future if the service had experienced a privacy incident	Saatan lopettaa palvelun käytön tulevaisuudessa, jos palvelussa ilmenee yksityisyysongelma	Oghuma et al. (2016)
	I will likely continue using the service in the future despite a privacy incident occurring	Tulen todennäköisesti jatkamaan palvelun käyttöä tulevaisuudessa huolimatta ilmenevästä yksityisyysongelmasta	Oghuma et al. (2016)
	I will likely continue using the service for the next six (6) months despite potential privacy incidents	Tulen todennäköisesti käyttämään palvelua seuraavan puolen vuoden ajan huolimatta mahdollisista yksityisyysongelmista	Oghuma et al. (2016)
	I will continue using the service as regularly as I do now	Tulen käyttämään palvelua jatkossa yhtä säännöllisesti kuin tähän asti	Wang, Asaad & Filieri (2020)
	I intent continue using the service in the future	Aion jatkaa palvelun käyttämistä tulevaisuudessa	Oghuma et al. (2016)
Trust (Trust)	I believe that the service provider acts in my best interest	Uskon palveluntarjoajan toimivan minun etuni mukaisesti	McKnight et al. (2002)
	I trust that the service provider provides enough safeguards for me to be safe using the service	Uskon palveluntarjoajan tarjoavan riittävästi suojatoimenpiteitä, jotta palvelun käyttäminen on minulle turvallista	McKnight et al. (2002)
	Service provider has informed me of all matters that affect my privacy	Palveluntarjoaja on kertonut minulle kaikista yksityisyyttäni koskevista asioista	McKnight et al. (2002)
Satisfaction (Sati)	I feel satisfied with the service	Olen tyytyväinen palveluun	Oghuma et al. (2016)
	I feel content with the service	Palvelu on riittävän hyvä	Oghuma et al. (2016)
	The service is pleasant to use	Palvelua on miellyttävä käyttää	Oghuma et al. (2016)
	I am very pleased by the service experience	Olen erittäin tyytyväinen palvelukokemukseen	Oghuma et al. (2016)
Confirmation (Conf)	The trade-off between cost and	Palvelun käytön hyöty-kustannussuhde on hyvä	Oghuma et al. (2016)

	benefit of service use is fair		
	The cost of service use is as I expected it to be	Palvelun käytön kustannukset ovat odotuksieni mukaiset	Oghuma et al. (2016)
	I have received the benefit I expected to gain from the use of the service	Olen saanut palvelusta odottamani hyödyn	Oghuma et al. (2016)
Perceived cost of use (PercCost)	I disclose personal information to the service provider in exchange for use	Paljastan henkilökohtaista tietoa palveluntarjoajalle vastineeksi palvelun käytöstä	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	The privacy risks associated with use are acceptable	Palvelun käytön yksityisyysriskit ovat hyväksyttävät	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	There would be severe consequences if my personal information was compromised	Henkilökohtaisten tietojeni paljastumisella olisi vakavia seuraamuksia	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
	There would be severe consequences if my account were breached	Jos tililleni murtauduttaisiin, sillä olisi vakavia seurauksia	Adapted from findings by Vishwanath, Xu & Ngoh (2018)
Perceived benefit of use (PercBen)	I gain benefit from using the service	Palvelun käyttö on minulle hyödyllistä	Adapted from Vishwanath, Xu & Ngoh (2018)
	The service allows me to pass time easily and entertain myself	Palvelun avulla pystyn kuluttamaan aikaa helposti ja viihdyttämään itseäni	Adapted from Vishwanath, Xu & Ngoh (2018)
	The service allows me to effectively and conveniently interact with others	Palvelu mahdollistaa tehokkaan ja kätevän vuorovaikuttamisen toisten kanssa	Adapted from Vishwanath, Xu & Ngoh (2018) and Oghuma et al. (2016)
	I enjoy using the service	Nautin palvelun käyttämisestä	Oghuma et al. (2016)
Attitude towards use (Att)	I feel I can reveal personal information in social networking services	Tunnen voivani paljastaa henkilökohtaista tietoa sosiaalisissa verkostoitumispalveluissa	Adapted from findings by Dowding (2011), Child, Haridakis and Petronio (2012), (Dienlin & Trepte, (2015), Ajzen (1991), Xu, Michael & Chen (2013) and Hong, Kim and Lee (2008)
	Revealing personal information on social networking services should be carefully considered	Henkilökohtaisten tietojen paljastamista sosiaalisissa verkostoitumispalveluissa tulisi harkita huolellisesti	Adapted from findings by Dowding (2011), Child, Haridakis and Petronio (2012), (Dienlin & Trepte, (2015), Ajzen (1991), Xu, Michael & Chen (2013) and Hong, Kim and Lee (2008)

	I should only reveal the required personal information to set up a profile	Minun tulisi paljastaa ainoastaan tilin luomiseen tarvittavat henkilökohtaiset tiedot	Adapted from findings by Dowding (2011), Child, Haridakis and Petronio (2012), (Dienlin & Trepte, (2015), Ajzen (1991), Xu, Michael & Chen (2013), and Hong, Kim and Lee (2008)
	To me, it is most important to maintain privacy online	Minulle on tärkeintä säilyttää yksityisyys verkossa	Xu et al. (2008)
Dimension of Privacy Perceptions (Dimensions)	It is a serious problem if the privacy policy limits my ability to control my personal level of solitude in the service	On vakava ongelma, jos yksityisyyskäytännöt rajoittaisivat kykyäni vapaasti hallita eristyneisyyttäni palvelussa	Adapted from Buckner & Knowles (2012)
	It is a serious problem if the privacy policy limits my ability to control my personal level of intimacy in the service	On vakava ongelma, jos yksityisyyskäytännöt rajoittaisivat kykyäni vapaasti hallita osoittamaani läheisyyttä palvelussa	Adapted from Buckner & Knowles (2012)
	It is a serious problem if the privacy policy limits my ability to control my personal level of reserve in the service	On vakava ongelma, jos yksityisyyskäytännöt rajoittaisivat kykyäni vapaasti hallita varautuneisuuttani palvelussa	Adapted from Buckner & Knowles (2012)
	It is a serious problem if the privacy policy limits my ability to control my personal level of anonymity in the service	On vakava ongelma, jos tietosuojakäytäntö rajoittaa kykyäni hallita anonymiteettiäni palvelussa	Adapted from Buckner & Knowles (2012)
Social influences (SocInf)	Members of my social group convinced me to join the service	Sosiaalisen verkostoni jäsenet saivat minut liittymään palvelun käyttäjäksi	Based on findings of Custers, Van Der Hof and Schermer (2014)
	I joined the service as many of the members of my social group were already members or going to be.	Liityin palveluun koska monet sosiaalisessa verkostossani olivat jo liittyneet tai aikoivat liittyä	Based on findings of Custers, Van Der Hof and Schermer (2014)
	Disclosing personal information in SNSs is common among members of my social group	Sosiaalisen verkostoni jäsenille on tavanomaista paljastaa henkilökohtaista tietoa yhteisöpalvelussa	Based on findings of Custers, Van Der Hof and Schermer (2014)
	I'm aware of the privacy issues related	Olen tietoinen sosiaalisiin verkostoitumispalveluihin	Xu et al. (2008)

Awareness (Awa)	to Social Networking Services	liittyvistä yksityisyysongelmista	
	I read news and other articles regarding privacy when I come by them	Luen yksityisyyteen liittyviä uutisia ja artikkeleita löytäessäni niitä	Xu et al. (2008)
	I am aware that the service has a privacy policy	Olen tietoinen, että käyttämässäni palvelussa on yksityisyyskäytäntö	Awareness is an issue regarding privacy policies based on Wu et al. (2012), Bechmann (2014), Obar & Oeldorf-Hirsch (2020), Custers, Van Der Hof and Schermer (2014) and Acquisti & Gross (2006)
Use Orientation (UseO)	What type of purpose do you use the service for?	Millaista tarkoitusta varten käytät palvelua?	Adapted from Kari, Salo & Frank (2020)
	What type of use do you see as the purpose of this service?	Millaisen käytön näet tämän palvelun tarkoituksena?	Adapted from Kari, Salo & Frank (2020)
	For what type of purpose did you start using the service?	Millaista tarkoitusta varten aloitit palvelun käytön?	Adapted from Kari, Salo & Frank (2020)