Understanding Informational Privacy Through User Interfaces in Web Applications

By: Annalisa Spence and Mimmi Svensson

Supervisor: Arina Stoenescu
Examinator: Karl Bergström
Södertörn University | School of Natural Sciences, Technology and Environmental Studies
Bachelor's essay 15 credits
Media Technology C | 2 semester 2023

SÖDERTÖRNS HÖGSKOLA
sh.se | STOCKHOLM

Abstract

This paper critically examines users' perceptions of privacy and security in web applications, emphasizing interface design. Drawing on both quantitative and qualitative data grounded in CPM and PMT theories, our research addresses Internet users' concerns regarding online privacy and security. Employing triangulation analysis on survey responses and web-based observations, our findings reveal a strong association between users' trust in web applications and their visual elements. By providing visual examples of current design practices in our survey, we discover some important aspects of effective interface designs. Utilizing IUIPC theory, we identify how web application interfaces influence users' privacy management, impacting their trust and usage decisions. Notably, some users are subtly prompted to grant permissions or share personal information through deliberate exclusion of options in the design of certain web applications. The approach of this study encourages a critical perspective on privacy and integrity issues in online settings.

Keywords: Privacy, Security, Integrity, Interface Design, Web Applications, Communication Privacy Management, Protection Motivation Theory

Definitions

User

An individual that uses and interacts with a web application from a device, for example, a computer or a smartphone.

Interface

A device or program enabling a user to communicate with a computer. In the case of this study, we refer to interfaces as the front end of web applications. More specifically, the visual graphics which enable its users to interact with or through the application.

Security

Measures to protect and safeguard data from unauthorized access.

Privacy

The fundamental right of individuals to control information about themselves.

Big Data

Large and complex datasets which can be analyzed through computerization and identify patterns and trends about people, for example.

Informational privacy

Privacy regarding one's personal information, such as sensitive information regarding health, identity, or finance.

Integrity

In this paper, we refer to integrity as the protection of one's data from unauthorized access.

Cookies

Data about users or their devices collected and stored in web browsers.

SSL

Secure Sockets Layer (SSL) is standard for establishing an encrypted link between a server and a user. Most commonly encountered when talking about SSL-certificates for websites.

Table of Contents

1. Introduction

Information privacy and security is a growing concern among a large part of the public. Concerns lay in regards to what data is stored about them and how their data is being used. Previous research shows that privacy concerns are frequent among Internet users (Malhotra et al. 2004; Degirmenci, K. 2020; Milham, M. H. and Atkin, D. 2018), but the severity of the concerns varies greatly between different kinds of users. These concerns are mostly grounded in the perturbation of their information and data being exposed to non-authorized or outside sources, or for fraudulent activities (Internetstiftelsen, 2021). Previous studies identified differential privacy concerns regarding the type of platform used (Degirmenci, K. 2020; Balapour et al. 2020), online B2C relationships (Eastin et al. 2016), and various degrees of engagement and desire to keep their information private (Boerman et al. 2021). In this paper, we aim to build upon the identified concerns that Internet users may have regarding their informational privacy, without disputing these factors.

The internet has become a fundamental part of modern society and its structures, in the way of online services, digital work environments, and communication. It has led to the point that the internet and the social events that take place there can be considered integrated parts of peoples' everyday lives (Berg, 2015. p.19). Along with the surge of Big Data, there is an increasing need to properly address the concerns and issues that originate from large-scale data collection by companies or organizations. These kinds of concerns are arguably nothing new and are likely going to stay relevant as privacy is a fundamental part of individual rights (Swedish Authority For Privacy Protection, 2023). Not only because of recently established regulations such as GDPR (General Data Protection Regulation) but because the right to privacy is under the protection of other regulations as well (ibid.).

The quantity of research done on these particular privacy concerns is already of a significant amount and there are many well-established theories that researchers have adapted for research in digital environments. Much of previous research also provides a solid foundation of methods and tools that researchers can use to explore and analyze privacy concerns. However, we find that many of them do not provide practical implications to properly address these privacy concerns among Internet users. With that being said, this study tries to approach these concerns with a critical perspective on the design of current interfaces and systems in

modern web applications. Not to dispute earlier studies, which discuss the socio- or psychological motivations behind user actions (Boerman et al. 2021; Xu et al. 2011), this study tries to identify the structures and design choices that enable users to manage their information on web applications. In other words, as a continuation of previous research on this subject, we want to shift the focus from *why* to *how*.

1.1 Aim

The aim and purpose of this paper is to research how users understand and perceive their security and privacy on web applications through their respective interfaces. More specifically, we will examine user settings related to integrity, privacy, and security in terms of how the application collects, uses, and distributes personal data. This research adopts a critical approach to how these interfaces are designed. In this paper, we define design not only by aesthetic features, but also by functionality, and what kinds of configurations the individual is being given in these situations (e.g. affordances). Based on this, we further analyze users' motivations and privacy protection behaviors on web applications. This is to gain an understanding of *what* users do to protect their informational privacy, and *why* they want to protect it. With the help of the protection motivation theory (PMT) and communication privacy management (CPM), we hope to find insights into how users understand and perceive their security and privacy settings through the interface of a web application.

With this research, we further strive to open up a discussion about the importance of personal integrity online and further promote an understanding among users of what data is being collected, and why. By doing this, we aim to establish possible implications for design regarding user interfaces in web applications. These implications could contribute to the development of transparent and easily managed user settings when it comes to privacy or integrity settings. Furthermore, we hope to contribute insights regarding how a critical stance on privacy and integrity issues might help users approach these issues on the web.

1.2 Research questions

With the help of formulating research questions, our aim is to fulfill the purpose and goals of this study, along with contributing further insights to the topic.

- Is there a difference in how informational integrity, privacy, and security is perceived by its users on installed versus browser-based web applications?
- What role does the web application's interface have in allowing its users to configure their informational privacy settings?
- In what way do interface designs *nudge* users into accepting permissions or disclosing personal information?

2. Previous Research

For this study, we focused on finding and researching literature that discusses relevant theories to computer ethics, informational privacy, privacy management, and concerns regarding privacy or integrity on the internet. As it turned out, there has been a significant amount of research done on the subject of privacy concerns throughout the last two decades. It could be assumed that the increased amount of internet users has warranted higher efforts in researching the possible effects of our increased presence on the web. In this section, we will discuss some existing concepts which are commonly addressed in previous studies.

The Privacy Paradox (Eastin, et al. 2016; Taddicken, 2013) refers to the contradicting behaviors of some users. The paradox shines a light on the fact that most people highly value privacy and personal integrity online, yet they give away personal information in turn to receive certain benefits, which often include personalized ads or marketing offers (Eastin, et al. 2016, p.219). The interesting part of this paradox is the discussion about what the users are willing to offer in terms of personal information, and for what type of benefits they will receive in exchange. In this paper, we will not use this paradox as a theory or framework to ground our research, but it will contribute to the discussion later on. The paradox created many interesting questions in the early stages of our research which led us to examine other factors as to why users would compromise their privacy in exchange for perceived benefits.

Two factors that Eastin et al. bring up in their article regarding why some users are more willingly disclosing personal information are "inaccurate perceptions of vulnerability" or possibly "a lack of understanding about the real value of their [users] personal information" (2016, p.219). These statements are backed up by previous studies that suggest an awareness amongst users that their data is being collected by companies. However, they do not fully understand what purposes their data is being used for (ibid.). In the case of understanding

security or privacy settings in web applications, this becomes especially important. One might argue that it is not the responsibility of the application itself to educate its users about privacy management. Instead, the responsibility is shifted to the individual to comprehend and manage their information. This would make sense in many other day-to-day situations, such as crossing a road without looking out for incoming traffic, to give an example. We argue however in the scope of this study that there is a shared responsibility between all actors (in this case, users and applications). However, for this shared responsibility to become clear to everyone involved, they cannot just be assumed or function as unwritten rules. There needs to be a clear and established "zone" of context in which users can "limit or restrict others from accessing their personal information" (Himma & Tavani, 2008. p.144).

According to our current knowledge of the subject, the shared responsibility of privacy management and what it means can significantly vary by situation (Himma & Tavani, 2008. pp.159-160). First of all, transparency and permission requests regarding what data the company wants to collect and for what purpose, is as explained by Himma and Tavani (2008, p.143) required to respect the privacy of users. This implies a responsibility for the company to inform and prevent users from disclosing any information without consent. Secondly, since different web applications collect different types of data and record different types of activities, the user in question is expected to choose what information they want to disclose (Himma & Tavani, 2008. p.160). This requires a personal choice, which in turn suggests a personal responsibility in the matter of having to deal with any consequences of making that choice. While this is true to a certain extent, this situation would assume that all users can make an informed and conscious decision.

Thus, shared responsibility in this context implies that each actor involved has some degree of responsibility to ensure that the necessary information is being communicated and understood correctly (Himma & Tavani, 2008. p.160). This could arguably go both ways - as the application's privacy settings need to be clear and comprehensible, the user in turn needs to be honest and clear about what they want to consent to.

3. Theory

In this section, we will introduce and describe existing theories and theoretical frameworks which have been used in our analysis work of this study.

3.11 Important terms and concepts

The perspective from which we have approached this study is primarily from a Human–computer interaction (HCI) standpoint. With this perspective, we analyze the visual components of user interfaces as well as the technical functions that produce the configuration of settings provided to the user. Seeing as HCI is an interdisciplinary science, we have to consider what other perspectives might be important to acknowledge when analyzing our data and choosing relevant literature. Therefore, we have also chosen to approach this study from a socio-psychological standpoint in which we examine the user's privacy protection motivations, interpretations, and privacy concerns, to continue on previously established research conducted on these specific subjects. As we will explain further when presenting our theories, our chosen standpoint is closely linked to the theoretical foundation of this study.

3.12 Explanation of terms used in this paper

(a) Online and offline in this paper refers to the presence and absence of the user on examined web applications.
(b) Web applications in this particular study refer to *any web-based applications*. In this study, web applications will be examined in two formats: installed web applications on the device and web applications run through a web browser.
(c) When we refer to *users*, we refer to the users of examined web applications.

Another important note for this paper is the use of *security* and *integrity*. We want to note that we will use these two words interchangeably, mainly for two reasons:

1. These two concepts can have very similar meanings, depending on the context.
2. Although technical definitions exist for both, their differences are not as easily understood by the general public and are often used to express the same thing.

We will provide an explanation of context when either definition is used, as they vary by situation. With that being said, the main context in which these definitions matter is *privacy* (and in the context of this specific paper, we refer to *informational privacy*).

3.2 Theories

From previous studies, we identified a couple of existing theories that would be appropriate for our research questions. In this section, we will introduce them one by one and explain their context of use or implementation.

3.21 Communication Privacy Management (CPM)

In the early stages of our research, we examined possible factors of why some users were more willing to compromise their informational privacy. As mentioned earlier, the privacy paradox explains that this occurs if there are perceived benefits or incentives that the user can receive in exchange. This explains the phenomenon to a certain extent, but we believe that this might be an oversimplified explanation. To identify possible factors, previous literature led us to the theory of CPM. This theory occurs frequently in similar and recent studies regarding security and privacy in mobile applications or e-commerce settings (Eastin et al. 2016.; Balapour et al. 2020.; Xu et al. 2011.). The CPM theory was initially used in interpersonal (face-to-face) relationships to examine and describe motivations or processes of thought when individuals make decisions to disclose information. However, as these recent studies suggest, the increasing amount of communicative technologies and their integration into our day-to-day lives makes CPM applicable to online contexts as well (Xu et al. 2011. p. 801). Additionally, as explained by Eastin et al (2016, p.216) the original classifications by Petronio (2002), who more or less founded this theory, are not sufficient to fully encompass the motivations behind a decision regarding online privacy. It is not a far stretch to assume that with new technologies come new possible factors that might affect an individual's perception of perceived risks or benefits. CPM theory relies heavily on identifying the boundaries individuals develop, which consist of privacy rules. These boundaries are not static, and they can behave differently depending on contexts (Eastin et al. 2016. p.216), which introduces us to an important but also interesting factor when conducting observations or surveys. The question is: how can we capture and truly examine these boundaries when examining an individual's behavior or how they respond to our questions? If we manage to identify these boundaries, we will be able to compare them and examine how they would change in a different situation. As such, examining users' behavior and thoughts with this theory could potentially lead to many qualitative insights regarding decisions of informational disclosure about demographics, environmental aspects, and possible psychological aspects. However, the scope of this study and the limited amount of resources would make it difficult

to capture all of these aspects and create any sort of productive conclusions. With that being said, we will mainly focus on CPM theory in our analysis, but it might not be utilized to its full potential.

3.22 Protection Motivation Theory (PMT)

Secondary to the CPM theory, we also want to include the Protection Motivation Theory (PMT). As Boerman et al. (2021, p.955) describe in their article, most previous research bases their theoretical foundation on the CPM theory, and these two theories utilize similar perspectives. While CPM theory focuses on the individual's management of their privacy through communication, PMT theory focuses on one particular aspect of individual behavior which we find is very important when discussing online privacy protection - the perceived threat and perceived efficacy of responses against said threat (Boerman et al. 2021, p.955).

Protection Motivation Theory draws on a similar notion as CPM theory, that the individual is exposed to some risks while using the internet. These risks can be perceived differently depending on the individual's values. PMT, as well as CPM, discusses to what extent individuals are motivated to protect their information regarding perceived risks. In contrast to CPM however, PMT discusses the individual's preventative measures and actions taken about how efficient they perceive their actions to be (Boerman et al, 2021. p.957). As such, PMT theory can help identify the reasoning for why some users engage in online protective behaviors and why some do not. PMT theory also adds dimension to this, in which it acknowledges that there might not be a perceived risk or threat at all (Boerman et al. 2021. p.957). We find the inclusion of the Protection Motivation Theory pertinent to our study, as it encompasses diverse factors influencing users' perceived control when interacting with specific interfaces. Our exploration of this theory within user interfaces aims to uncover affordances and signifiers that empower users and safeguard their online navigation experience.

3.23 Internet Users' Information Privacy Concerns (IUIPC)

Another theory used significantly in previous privacy research is Concerns for Information Privacy (CFIP). The theory utilizes a multi-dimensional scale which consists of 15 items to measure privacy concerns (Smith et al. 1996). Previous research shows that the theory has been accurate in finding statistically significant correlations between privacy concerns and behavior in (primarily) consumers (Smith et al. 1996; Degirmenci, K. 2020; Malhotra et al.

2004). However, the CFIP theoretical model was mainly created to approach offline consumer relationships and a traditional marketing setting (Malhotra et al. 2004. p.338). Therefore, previous researchers have created some alternative models to approach online settings more accurately. One alternative model we have decided to include for this study is the IUIPC theoretical model, which was suggested by Malhotra, Kim, and Agarwal (2004, p.338) to be used when researching online privacy concerns. In contrast to CFIP, IUIPC consists of three dimensions and 10 items. These items are useful in survey research, as they help to create relevant questions and topics for the survey itself and for analyzing the survey results (Malhotra et al. 2004. p345, p.351). The dimensions described in IUIPC are (1) *Collection,* (2) *Control,* and (3) *Awareness*. As for the items under each dimension, they vary depending on the intended context and research question, so we tailored the suggested items to our specific study. The items are listed below as follows:

Control:

(1) User online privacy is really a matter of users' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
(2) User control of personal information lies at the heart of user privacy.
(3) I believe that informational privacy is invaded when control is lost or unwillingly reduced as a result of my presence on the application.

Awareness (of Privacy Practices):

(1) Companies or organizations seeking information online should disclose the way the data are collected, processed, and used.
(2) A good online privacy policy should have a clear and conspicuous disclosure.
(3) It is very important to me that I am aware and knowledgeable about how my personal information will be used.

Collection:

(1) It bothers me when online companies ask me for personal information.
(2) When online companies ask me for personal information, I sometimes think twice before providing it.
(3) It bothers me to give personal information to an extended amount of online companies.
(4) I'm concerned that online companies are collecting too much personal information about me.

In summary, all three theories are applicable to our research questions and topics as they are suited for online settings, which include web-based applications. However, in the scope of this paper, we have limited our analysis to the CPM theory with PMT as a secondary theory to further discuss the implications of our findings. Additionally and lastly, the IUIPC theory has mainly been implemented in the creation of our survey, along with the presentation of the survey results. With this, we find that we have a solid theoretical foundation to base our research on. In the Analysis section, we will further demonstrate how these theories are relevant to our empirical findings.

4. Method

In our study, we adopt a comprehensive approach by using both quantitative and qualitative data collection methods. Quantitative data is collected with the help of online surveys. Qualitative data has been collected by conducting web-based observations using netnography as a base of methods. By combining these datasets, we aim to gain a valuable understanding of users by means of collecting and seeing correlations between measurable variables.

4.1 Surveys

The primary method we have used to gather data in this research is surveys. We have created the survey using the online tool Survey Monkey (www.surveymonkey.com). We sent out the survey on social channels like Facebook and Discord. We have also published the survey on Reddit, a larger platform where we hoped to gather a larger sample to quantify the data.

As for the motivation behind using surveys as the primary method, we chose this approach for several reasons. Firstly, respondents can answer the survey at any place and any time, making it both time-efficient for the respondents and the research project (Bryman, 2011. p.228). This is especially relevant in this study since we decided to use online surveys. The secondary reason is that it gives us more time to analyze the data in sequences. This means that we don't have to be present when the respondents answer the surveys (Bryman, 2018. p.286-288). This lack of presence brings us to our tertiary reason for choosing this method, which is to avoid bias such as the social-desirability bias (Bryman, 2011. p.229). This bias is mainly a concern when constructing interviews. While we acknowledge that this bias can manifest in survey responses as well, the risk is much more prominent in interviews as they do not offer the same anonymity as surveys. In interviews, we as interviewers would be able

to know who responded to what questions and how they responded. In contrast to our survey, we have no way of knowing who said what and so on. Lastly, using surveys instead of interviews also eliminates the risk of questions being asked differently in different interviews (Bryman, 2011. p.229). This, however, also creates a disadvantage where we can't explain the questions further if the respondents are unsure of how to answer the question (Bryman, 2018. p.288). Despite these challenges, we still believe that using surveys as our primary research method outweighs these limitations.

4.11 The design and content of the survey

As our sample could potentially include a large variety of people with varying backgrounds and experience, we created the survey through a couple of criteria and principles to make it as versatile as possible. To ensure that the questions in our survey resonate with all types of users, we have adjusted the questions so they stay both relatable and professional.

Conventional survey design principles mentioned in Bryman's book about methods (2011. pp.228-258) can mostly be applied to paper-form surveys, in which some aspects do not apply to the online web format. Therefore, we have adapted the principles we find appropriate for our web-based format. For example, in a paper survey, the respondent can skip pages and answer questions in any section of the survey (Bryman, 2011. p.230). This is not applicable in our survey as one page needs to be finished to continue with the next questions, which could be utilized as an advantage to maintain the relevance of the questions to the respondents. The first section of the survey includes lighter questions that are mostly closed, such as frequency and types of interaction on web applications. The following section contains visual examples with some open answers. These require the respondent to explicitly express their thoughts, opinions, or motivations. The visual examples comprise selected prompts, user settings, and cookie permissions from two different types of web applications: installed applications on a device, and applications run through the web browser.

In addition, we concluded that we couldn't feasibly fit every possible category of attitudes and behaviors in pre-determined answers. Therefore, we decided to leave the questions open to avoid limiting the respondents' choices (Bryman, 2011. p.246) and avoid the possibility of irritating the respondents with irrelevant categories (ibid.). To minimize survey fatigue, we chose to not place all open questions at the end of the section as that would require the respondent to answer all the weighty questions one after the other. In other words, the variety

of the current order is meant to provide a cognitive rest for the respondent. The visual example section of the survey includes some vignette-type questions (Bryman, 2011. pp.257-258), where we illustrate a specific scenario or situation that the user (e.g. respondent) might encounter while using web applications. We chose these types of questions to further increase the personal relevance of the questions to make them easier to understand (Bryman, 2011. p.258). Additionally, to form relevant questions for the survey we utilized the suggested items in the IUIPC model. These items are described in the Theory Section, and will also be further explained in our analysis.

4.12 Advantages of using online surveys

To keep the dropout at a minimum, we have as suggested by Bryman (2018, pp.290-291) included an introduction and explanation of the survey for the respondent to read. Along with this, we have also explained the anonymity and the right to erasure for the respondents. An advantage of using SurveyMonkey is that it provides accessible themes and layouts which creates a professional look for the survey. Not only to ensure as many respondents as possible complete the survey (ibid.) but also to save us time in the process of publishing the survey. Another benefit of using an online survey tool is the ability for us to divide the questions into different sections. This prevents tiring out the respondents with long and extensive pages, or the thicker variant of paper forms (Bryman, 2018. p.297).

Perhaps the most useful advantage of using SurveyMonkey is the data visualization it provides after responses have been collected, in which the tool automatically creates different charts. Through these, the collected data and its variables are sectioned and, to some extent, coded automatically which helps us in our analysis work. By using this tool, the risk of misinterpreting the collected data can be minimized as it is computerized, which requires less personal interpretation (Bryman, 2018. p.297). However, since we have many open questions there are some limits to this automatic coding and as such, requires us to manually code and categorize the data. For this, we have utilized PMT and CPM theory as a foundation to categorize the data into relevant codes.

4.13 Using SurveyMonkey in a physical location

SurveyMonkey can provide a stationary variation of the surveys you create. This means that you can set up a computer, tablet, or another device to act as a survey station. This was something we wanted to try to gain more responses, as well as test its usability in research

contexts. We set up a station near the entrance at Södertörn University, which consisted of a tablet and keyboard, as well as a written sign and QR code for the survey's web link. Additionally, we edited some of the survey questions and options to better suit the context (e.g. less open answers) without changing the question's purpose. We intended to be able to provide support for those answering the survey, in case any questions or confusion would arise. This survey station was up for about 4 hours, in which we only gathered two responses. With that being said, it is unclear if this method is suited for this type of research project. Further, the use and testing of this method would be required to imply the applicability of the stationary mode.

4.14 Survey sample

In this study, we have made use of minor convenience samples. This means that we have sent the survey to a range of people in our vicinity. This method of sampling has a high response rate, however, it is arguable if this type of sampling can be generalized or representative for a specific demographic group (Bryman, 2018. p.243-244). We mainly published the survey on several social platforms, such as Facebook and Reddit. This was to reach a wider audience and possibly collect interesting insights from respondents with substantially different backgrounds and experiences on the Internet. Furthermore, we have also distributed the survey link through personal contacts. The final demographics will be presented in the Results section of this paper.

4.2 Netnography

Netnography is a methodological approach to how we can analyze the ethnography of the internet. It was first established by Robert V. Kozinets in 1997 as an adaptation of ethnography for the internet and how we can implement web-based research. As netnography can be used to analyze, interpret and understand behaviors and interactions among users online (Berg, 2015. p.10-11), we believed this method to be suitable for our research questions.

The internet must be understood as a complex and changing environment with a set of different technologies (Berg, 2015. p.25). In this case, we have used netnography to conduct observations and collect data online about users' privacy protective behavior, and their privacy concerns. As explained by Kozinets (2011), there already exists information and

public data on the web, specifically in different online forums by users, that can be used in netnographic research (p.83).

In order to use netnography in our research, a theoretical standpoint and perspective should be used in conjunction with the method to gain a better insight and understanding of the collected data (Berg, 2015. p.66). As such, our main theoretical models for this method were drawn from CPM and PMT theory. Subsequently, the empirical data collected in accordance with our theoretical frameworks creates a more coherent analysis and makes sure it stays in line with our research question and perspectives (Berg, 2015. p.66). Throughout our research, we have attempted to interpret the qualitative results in an iterative process, so that we can present the results with transparency and minimized bias (Kozinets, 2011. p.91).

We have used Kozinets' four categorizations of online users when conducting netnographical research (2011, p.52): (1) *newbies*, (2) *minglers*, (3) *devotees*, and (4) *insiders*. We believe these categorizations to be of value in our analysis work, as our research requires us to examine different types of users. This is to determine if experience and engagement is a contributing factor to privacy concerns.

(1) *Newbies* can be identified based on their low effort to contribute to the community as they don't have strong ties to the group itself and don't post publicly very often.
(2) *Minglers* spend more time conversing and contributing to the online community compared to newbies. They do participate in the community and engage in discussion with other users but are not deeply committed or invested in its cause. This is due to not having a deep connection to the majority of other users. They rather contribute for the purpose of having company.
(3) Compared to the minglers' characteristics, *devotees* are much more committed and engaged in the community. They tend to contribute regularly and show great enthusiasm for the group. In addition, they tend to have a great understanding of the group in the community, its users, and its culture (Kozinets, 2011. p.52-53). It could be perceived that these types of users hold some sort of leadership in their communities, like moderators. As such, they are usually respected in their communities as they are very knowledgeable and contribute a lot.
(4) *Insiders*, along with devotees, are also very knowledgeable. They have been a fundamental part of the community for an extended period and are considered long-term members. Insiders possess a deep understanding of the communities' rules, history, and

dynamics. As they have been a part of the community for a long time, they also have a strong personal identity connected to it (Kozinets, 2011. p.53).

4.21 Observations

By using netnography as a methodological approach, we have conducted observations on public online forums to gather data about users' behavior, actions, and thoughts about privacy and security online. We have decided to perform covert observations to observe the natural circumstances and activities and interactions that occur on the web among users.. Our observations have been documented with the help of an observational coding scheme (See Appendix 1). As suggested by Kozinets, we have followed steps to help us determine which platforms would be best suited for our research (2011, p.127). This is based on aspects such as relevance to our topic, website features, and activity and interactions by users (ibid.). As explained above, we have documented the type of users in our observational coding scheme according to the four categories.

4.22 Observation sample

As for the observations conducted through our netnographical methods, the sample is still intended to be a variety of Internet users with different backgrounds. As such, the main platforms we decided to examine were forums such as Reddit. We will introduce the specific websites in the Results section. It is worth noting that it proved to be challenging to find specific forums where subjects like data and informational privacy are of focus as they can appear as a topic on any kind of platform. As such, the platforms that we examined also contain topics that are not relevant to this study. This was acknowledged early on and should be considered by any researchers who want to use this method in future netnographical studies.

4.3 Analytical method

The methods we are using for analyzing our dataset is a triangulation of correlation tables and bivariate analysis, chi-square tests, and coding. Correlation tables have been used in similar studies (Malhotra, Kim & Agarwal., 2004; Boerman et al., 2018; Balapour et al., 2020) and so we believed it to be a relevant method to use. The coding techniques we will be using for our analysis are mainly based on the IUIPC items and dimensions. Secondly, we also have CPM and PMT theory in which different privacy concerns are described. Each of these

methods serves its own purpose, and we have chosen to make use of these specific methods based on the type of data we want to collect. We will explain further how these methods are used in our research in the Analysis section of this paper.

5. Results

Our research methods resulted in a total of 64 survey respondents, as well as seven separate observations. To present our findings we will summarize the results from each method in separate sections.

5.1 Survey Results

In the following section, we will present the survey results answered by respondents. This includes both the online survey and the stationary survey we held at our university.

5.11 Overview

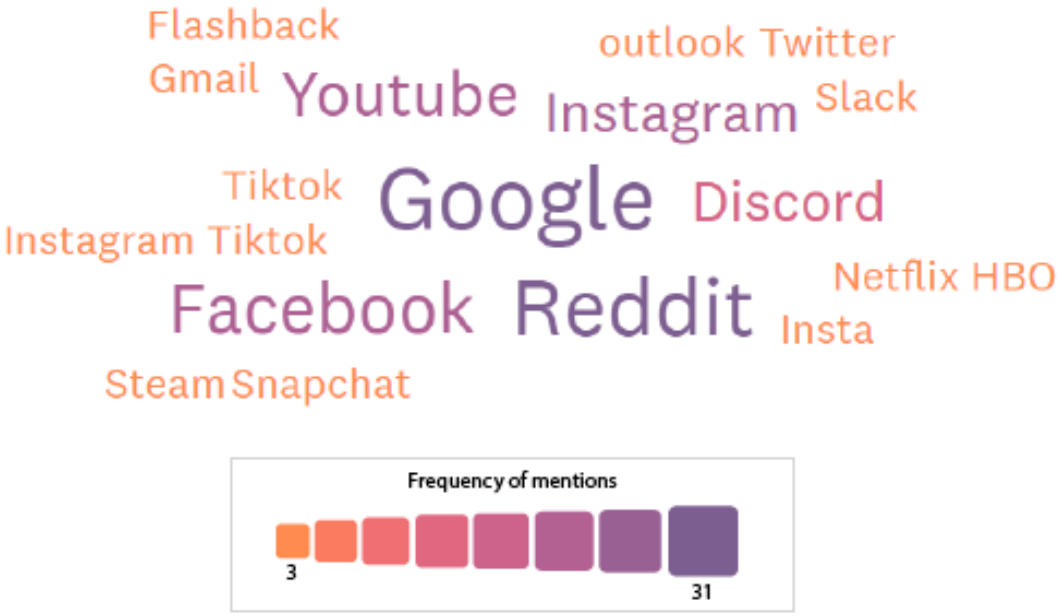
Generally, throughout the surveys, there were some common comprehensions and explanations given by the respondents. Recurring themes were identified, which suggests a discernible trend regarding what the respondents perceive as important in terms of informational privacy. Additionally, the results also suggest trends in terms of how a user interface is interpreted and understood by the user (respondent) as well as how this affects their activity on the web application.

Despite the many open-answer questions, we did not have a large portion of dropouts in relation to those who completed the survey. For example, in the online survey, there were 62 respondents in total. 100% of these respondents answered the first page of the survey which included demographic and activity questions. After the first page, there is a significant dropout (17 respondents). The cause of this is unknown. However, out of those who completed the survey (45 respondents) the completion rate of the second page with the most open answers was 100%. Only on the final page with optional questions did we find that some open-answered questions were skipped, which leaves us with a completion rate of between 64-82% and 91% for the closed question.

5.12 Demographic and Activity

Table 1. Respondent demographics		
Demographic Variables	Category	Frequency (Percent)
Age	18-24 25-30 **31-40** 41-50 51-60 61-70 71+	12 (19.35%) 15 (24.19%) **18 (29.03%)** 8 (12.90%) 7 (11.29%) 1 (1.61%) 1 (1.61%)
Education	Grade school High School **University** Vocational Education Other	1 (1.61%) 18 (29.03%) **30 (48.39%)** 10 (16.12%) 3 (4.84%)
Devices to access the web (multiple choices permitted)	**Smartphone** Computer Tablet	**58 (93.55%)** 52 (83.87%) 4 (6.45%)
Frequency of accessing the web	**Multiple times per day** Once per day	**60 (96.77%)** 2 (3.23%)
Purpose for accessing the web	**Entertainment** Education Work Shopping Communication Finance services Health services Other	**59 (95.16%)** 41 (66.13%) 32 (51.61%) 29 (46.77%) 28 (45.16%) 12 (19.35%) 8 (12.90%) 4 (6.45%)

below FIGURE 5.1



The most common platforms on which the respondents spend the majority of their time are shown in the word cloud above (figure 5.1). The largest names in the cloud are mentioned with a high frequency among the respondents, while the smaller names are less frequent.

5.13 Privacy concerns in web application users

Many of the privacy concerns we mentioned in our survey were confirmed to be of relevance by the respondents throughout their responses. These privacy concerns were:

- Collection of personal data (33%)
- Unauthorized use of personal data (24%)
- Sold personal data (71%)
- Unauthorized access to data (44%)
- Ambiguous or unclear options in privacy settings (62%)

(The percentages shown are non accumulative as one respondent could express concerns regarding more than one type.)

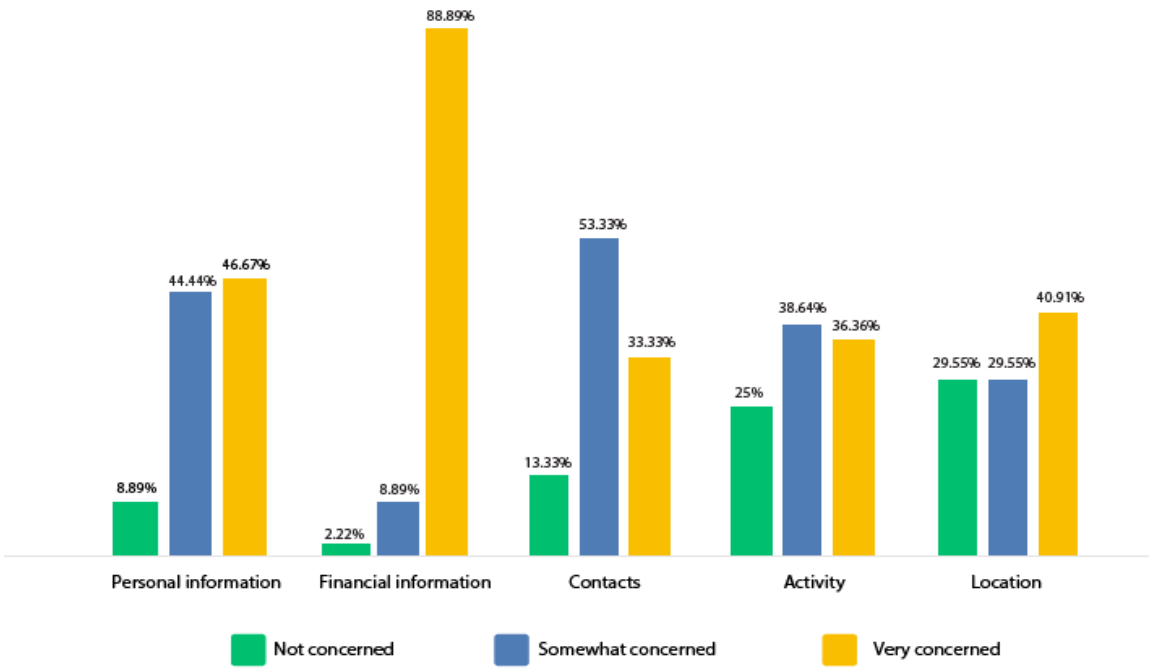


FIGURE 5.2

In terms of privacy concerns, respondents were asked to rate what kind of information they were the least or the most concerned about if it were to be accessed by an unauthorized party. The results are shown above in figure 5.2.

We also discovered some additional concerns mentioned by respondents in the open-answer questions.

- Surveillance (user activity)
- Lack of control or choice regarding informational privacy
- Fear of intentional malicious design practices to manipulate user actions

The last point of concern provides one answer to the question of how interface designs possibly nudge users into disclosing personal information on the application. While this concern was less commonly mentioned, it is an interesting find in terms of our research. In our survey, we made no direct mention of nudging or manipulative design practices. Despite this, mentions of nudging and manipulative designs occurred on several questions throughout the survey.

5.14 Privacy Concerns in relation to the application's user interface

An application's user interface is composed of varying elements, some applications might require more options than others depending on the functionality and purpose of the application. In this study we chose to incorporate examples from two different types of web applications - (1) installed applications, and (2) applications accessed through a web browser. Some of the examples in the survey were Spotify (browser version), Adobe Behance, Duolingo, and a blog website. According to our results, these were the interface elements mentioned that affected the respondents' level of trust in some way:

In installed applications, the most commonly mentioned elements were:

- Insufficient or irrelevant settings (84%)
- Vague or unclear definitions of options (24%)
- Lack of information about data collection or usage (40%)

(The percentages shown are non accumulative as one respondent could express concerns regarding more than one type.)

In applications accessed through a web browser, there were significantly more types of concerns mentioned, and as such, a larger variety of elements:

- Icons in the web browser indicating security, protection, or encryption, such as a key or a padlock.
- Large pop-up windows or prompts regarding cookies or privacy settings

- The name or address of the web application as an identifier
- Warnings issued by the browser itself when visiting an unsecure website

Other factors mentioned which helped the respondents assess their level of security on web applications were:

- The social status or hierarchy of the web application's owner, like a governmental authority or a well-established platform. (17%)
- Social input, and reviews from other people on third-party websites like TrustPilot. (8%)
- Transparency about data collection and purposes of use. (15%)
- The activity of the web application, such as spam or intrusive prompts. (11%)
- Website certificates such as SSL, or other methods of encryption. (22%)

5.2 Observation results

We conducted observations on two different platforms which are public discussion-forum websites: Reddit and Familjeliv. We have documented our observations with the help of a coding scheme (see Appendix 1). The threads we observed were initially posted between 2017 to 2023. The discussions on these threads are as of now inactive but remain open for the public to read, with some still being open for users to add comments and replies to. We have conducted seven observations in total. The final results are summarized in the table below.

5.21 Internet Users Information Privacy Concerns - An overview **FIGURE 5.3**

DIMS	**Items**	**Frequency**	**Strength***	**Concern**	**Solutions**
Control:	(1) ACC	0.71	2.5	User autonomy	Non-disclosure privacy measures
	(2) CTRL	1.0	2.42	Difficulty interpreting privacy settings	External help from other users
	(3) INV	0.86	2.83	Monitored presence on applications	Configure visibility through privacy settings
Awareness:	(4) DISC	0.28	3	Insecurity towards company's privacy practices	Refraining from using the application, or use in isolated environments
	(5) POP	0.28	3	Risk of Surveillance	Faking personal information
	(6) AWAR	0.43	3	Access of personal	Prevent tracking through

				information	several security measures
Collection:	(7) COMP	0.43	2	Involuntary usage of application	Finding alternative applications
	(8) CRIT	0.57	2.75	Seeking advice or help with settings	External help from other users
	(9) EXTN	0.14	3	Removing accounts as security measure	Disable activity status, avoiding disclosure
	(10) CONC	0.57	2.25	Inexperience, involuntary usage	Avoid platform, use general precautions for the web

ACC = access and distribution of user information, CTRL = user control of personal information, INV = invasion of informational privacy when control is lost, DISC = disclosures of data collection by companies, POP = online privacy policies should be clear, AWAR = awareness of how information is or will be used, COMP = companies asking for personal information is bothersome, CRIT = critical thinking towards disclosing personal information, EXTN = providing personal information to multiple companies is bothersome, CONC = concerns of extensive collection of personal information

**calculated by the mean average, on a scale of 1-3. 1 being the least concerned, 3 being the most concerned*

5.22 Findings regarding privacy concerns and privacy management

In total, five observations were conducted on the social platform Reddit which currently exists both as a website and as an installed application on mobile devices. Additionally, we conducted two observations on the platform Familjeliv. When conducting these observations, we were mainly examining privacy concerns in different users. Additionally, we wanted to explore possible solutions or methods these users utilized to either prevent or confront these concerns. As such, our findings suggest these methods of privacy protection:

Control	Awareness	Collection
Not disclosing private information	Request data packages	Configure data collection settings
Two-factor authentication	Avoid using the application	Never using their real personal information
Disable marketing and ad settings	Open application in isolated environments	Disable cookies and remove browser history
Request erasure of data	Ask other users about application	Deleting account

The observations' discussions extended to Instagram and Discord, with users discussing privacy and safety on respective platforms.

Instagram:

- The thread on Instagram focused on using the platform safely in terms of privacy.
- Contributors included a devotee, a newbie, and minglers, each providing unique insights on privacy-related practices.

Discord Privacy Concerns:

- Discussed on Reddit, Discord raised concerns about safety settings and potential tracking.
- Advice was sought on the best safety settings for account creation, specifically expressing worry about being tracked and unauthorized reading of private messages.
- Minglers, predominantly, provided generic solutions while conveying a serious attitude toward the topic, highlighting the importance users placed on safeguarding their privacy on Discord.

6. Analysis

In this section, we will first introduce the analysis methods we have made use of to analyze and gain a deeper and more nuanced understanding of the results. We will thereafter present our analysis of the results.

6.1 Analysis methods

As previously stated in our methods of this research, we have made use of a triangulated set of methods. These include chi-square tests, correlation tables, and bivariate analysis to analyze the results from the surveys and observations. By triangulating methods, we hope to be able to increase the reliability and validity of our findings. Conducting chi-square tests in our analysis will help us determine if there is a significance in the associations between two categorized variables (Bryman, 2011. p.335). This statistical test will help us determine if variables are independent of each other, or if there is a significant relationship between the categorized data (Bryman, 2011. p.355). Additionally, correlation tables can offer a bivariate analysis to gain further insight into if there are any relations between two, or more, variables through a statistical connection and relation (Bryman, 2011. p.326). This approach enables us to assess the strength and direction of a linear relationship between two continuous variables (Bryman, 2018. p.149; p.416-417).

These methods will also be used for datasets of a more qualitative nature, to provide a comprehensive understanding of the research (Lofland et al. 2006. p.200-201). To do so, we have utilized SPSS's automatic recode as well as manually coded the data into numerical values.

6.2 User coding and user-related factors

To better understand the context in which privacy concerns take place, user-related factors are coded into *Concern* and *Comprehension*. These codes are primarily based on discussions around CPM theory. More specifically: Balapours et al. (2020. p.9) discussion regarding how different amounts of experience and understanding in users significantly affect their perceived security on mobile applications. As such, each factor has a positive and negative variant: (1) *Concerned User* and *Unconcerned* User, (2) *Comprehends* and *Does Not Comprehend*. These factors will be used for our chi-square tests.

6.3 Chi-square tests

The following contingency tables are the results from the survey. Each hypothesis is supported by our research questions, however worded differently.
The Significance Level (α) is set to 0.05 for this analysis.

H1 - There is a correlation between those who express significant levels of privacy concerns and understanding privacy settings.

	Comprehends	Does not comprehend	Total
HIGH	33	1	34
LOW	3	8	11
Total	36	9	45

HIGH = high level of concern, LOW = low level of concern **FIGURE 6.31**

(df) = 1 **$x^2 = 25.28$**

H2 - There is a difference in how users perceive their informational privacy and how it is managed on different types of web applications.

	Able to manage settings	Not able to manage settings	Total
INSTALLED	21	24	45
BROWSER	36	9	45
Total	57	33	90

INSTALLED = installed web application (both desktop and mobile), BROWSER = web applications run through a web browser **FIGURE 6.32**

(df) = 1 **$x^2 = 10.74$**

H3 - Users who do not value their informational privacy as much are less likely to understand privacy policies and settings.

	Comprehends	Does not comprehend	Total
UNCO	19	5	24
CONC	12	9	21
Total	31	14	45

UNCO =unconcerned users, CONC = concerned users **FIGURE 6.33**

(df) = 1 **$x^2 = 2.523$**

From our chi-square tests, only H1 and H2 rejected the true null hypothesis. The significance level (α) was set to 0.05, and all tables contained a *(df)* of 1. In accordance with the chi-square distribution table (see Appendix 3), this leaves us with a critical value of 3.841. To suggest that there is a correlation between the variables stated in the tables, our chi-square statistic (x^2) needed to be above the critical value. Therefore, according to our analysis result, we can confirm:

H1 - A correlation between those who express significant levels of privacy concerns and understanding privacy settings.

H2 - There is a difference in how users perceive their informational privacy and how it is managed on different types of web applications.

Lastly, H3 did not reject the true null hypothesis so we cannot confirm that H3 is correct.

6.4 Correlations - survey

To find relevant or significant correlations or patterns in our collected survey data, we utilized Pearson correlations to visualize related variables (Bryman, 2011. pp.326-327). As such, a bivariate analysis was used to create the tables. The dependent variables were *experience, comprehension,* and *levels of concern*. The final table is shown in Figure 6.41. A more extensive table can be found in Appendix 4, which explains the comprehension levels of each question in the survey.

Correlations

Variables		Level of Concern	Experience	Comprehension
Level of Concern	Pearson Correlation	1	,011	,127
	Sig. (2-tailed)		,943	,404
	N	45	45	45
Experience	Pearson Correlation	,011	1	,492**
	Sig. (2-tailed)	,943		<,001
	N	45	45	45
Comprehension	Pearson Correlation	,127	,492**	1
	Sig. (2-tailed)	,404	<,001	
	N	45	45	45

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

FIGURE 6.41

The correlation between "Level of Concern" and "Experience" is very low ($r = 0.011$), and the p-value is not significant ($p = 0.943$). Therefore, there is no statistically significant correlation between these two variables.
The correlation between "Level of Concern" and "Comprehension" is again low ($r = 0.127$), and the p-value is not significant ($p = 0.404$). There is no statistically significant correlation between these two variables either.

The correlation between "Experience" and "Comprehension" is moderate to strong ($r = 0.492$), and the p-value is highly significant ($p < 0.001$). This suggests a statistically significant positive correlation between these two variables. The correlation coefficient of 0.492 suggests a positive linear relationship: as one variable increases, the other tends to increase.

6.5 Correlations - observations

In terms of how different types of users handle these discussions, we thought to examine if there was a pattern between the level of privacy concerns expressed and their level of engagement on the web application. User types were categorized according to the types of online users, as described earlier in this paper (Kozinets, 2011, p.52).

Correlations

		User Type	Non consensual collection and use	Lack of control	Excessive collection
User Type	Pearson Correlation	1	-,487	-,786	-,680
	Sig. (1-tailed)		,257	,107	,160
	Sum of Squares and Cross-products	5,000	-8,000	-19,000	-9,000
	Covariance	1,667	-2,667	-6,333	-3,000
	N	4	4	4	4
Non consensual collection and use	Pearson Correlation	-,487	1	,906*	,966*
	Sig. (1-tailed)	,257		,047	,017
	Sum of Squares and Cross-products	-8,000	54,000	72,000	42,000
	Covariance	-2,667	18,000	24,000	14,000
	N	4	4	4	4
Lack of control	Pearson Correlation	-,786	,906*	1	,984**
	Sig. (1-tailed)	,107	,047		,008
	Sum of Squares and Cross-products	-19,000	72,000	117,000	63,000
	Covariance	-6,333	24,000	39,000	21,000
	N	4	4	4	4
Excessive collection	Pearson Correlation	-,680	,966*	,984**	1
	Sig. (1-tailed)	,160	,017	,008	
	Sum of Squares and Cross-products	-9,000	42,000	63,000	35,000
	Covariance	-3,000	14,000	21,000	11,667
	N	4	4	4	4

*. Correlation is significant at the 0.05 level (1-tailed).

**. Correlation is significant at the 0.01 level (1-tailed).

FIGURE 6.51

Our findings could not prove any correlation between user type and different types of privacy concerns.

User Type ←→ Non consensual collection and use is negative: ($r = -0.487$), but the p-value is not significant ($p = 0.257$). Therefore, no correlation exists.

User Type ←→ Lack of control is negative ($r = -0.786$), but the p-value is not significant ($p = 0.107$). No correlation exists here either.

User Type ←→ Excessive collection is negative ($r = -0.680$), but the p-value is not significant ($p = 0.160$). No correlation was found between these two variables.

6.6 Identified patterns and trends

There are several interesting occurrences and trends that we identified through our analysis of the survey results. However, they could not prove to be statistically significant through our analysis. With that being said, these trends could be of interest for further research as our sample is too small to accurately describe their significance.

(a) Out of the 45 respondents who completed the entire survey, none preferred the cookie permission “accept all, or customize”. The majority (approx. 60%) wanted both options of accepting or rejecting all cookies.

(b) A high level of expressed concern regarding leaked personal information can be found in all age groups.

  (i) Those who expressed these concerns also expressed high levels of concern for leaked financial information.

  (ii) Approximately 80% of this group has a higher level of comprehension of settings and privacy risks.

(c) The most common response to what makes a web application secure, is “You can never be sure”.

7. Discussion

As stated earlier in this paper, security, and integrity can be seen as two different topics due to their different definitional meanings. The further we analyze different aspects of privacy concerns on web applications, the more intertwined these topics seem to become. As our findings suggest, some privacy concerns are not solely based on the web application itself and its management of personal information. Concerns regarding external parties could arguably be outside of our scope in this particular study, but it’s a factor nonetheless that needs to be included when discussing privacy concerns in these contexts.

For example, an external influence on privacy concerns could be a cyber attack. Cyber attacks are related to cyber security, because in order to analyze how the attack happened, we need to look at the infrastructure of the system and how it was breached. The other side of the analysis is *why* the attack happened. Was it to gather information or to sabotage the system itself? In these cases, information would either be accessed without permission, or the information could be damaged or corrupt. Nonconsensual access to personal information is a part of personal integrity, because of the individual values that keep us from disclosing

private information (Boerman et al, 2018. p.955). For example, cloud storage is one potential target in cyber attacks. As we could store our personal pictures, notes, or contacts in the cloud, we are arguably always at risk for these items being accessed. If a cyber attack then resulted in these items being destroyed or "lost", this would still be considered a concern regarding informational integrity as it's connected to *who* has access to our data - not necessarily what the data is being used for. As such, whether or not such a case is a security concern, privacy concern, or integrity concern is not so easily answered.

The IUIPC theory was instrumental in revealing the frequency and severity of privacy concerns. Notably, under the dimension of control, *user control of personal information* emerged as the most frequent concern in our table. Users experienced difficulties with interpreting privacy settings and often sought external help. Despite being the most frequent, this concern was not the most severe (2.42). The second most frequent concern, the *invasion of informational privacy when control is lost* implied a strength of 2.83. This concern was described as a monitored presence on applications, and addressing this concern implies a user's responsibility to configure visibility and disclosed information through privacy settings. As discussed earlier, communication requires a shared responsibility between the application and the user. This finding highlights the importance of creating accessible options in user settings.

Comparisons between Familjeliv and Reddit uncovered nuanced differences but highlighted shared frustrations about online privacy and safety. Minglers and newbies, with a few devotees, expressed varying trust levels in platforms. As such, our observations can confirm that privacy concerns related to privacy settings are of importance on these web applications. It could also be suggested, along with our survey results, that mixed degrees of understanding can occur on any web application. However, it is difficult to point out exactly why one user does not find something in their settings, or why they might not understand what it means. Unless stated otherwise, we do not know if the user has any sort of visual or cognitive impairment, or if they are using a device that may affect their perception. Furthermore, we cannot confirm whether or not the users in these observations are referring to the installed application of Facebook, or if it is accessed within a browser.

7.1 Ethical aspects

Challenges related to ethical aspects of using netnography in research should be regarded. One aspect that is suggested to reflect upon is the user's participation in the research. It is important to make sure that the user's voluntary participation is stated, and that they are informed about their consent. Along with this, we also need to make sure that their confidentiality is guaranteed. Another aspect that goes hand in hand with the user's participation is our presence whilst observing (Berg, 2015. p.126-127). As we can not fully guarantee knowledge of our presence whilst observing online, we have made sure to retain all personal information about users and only stick to observing open, and public, communications on the web. It is suggested that an entrée and introduction from us as researchers are done to further observe users in web-based research using netnography. This is to announce our presence whilst conducting the observations on the chosen platform to its users. However, Kozinets (2011) explains that this type of research can also be done in a way that is not announced to the users being observed and is therefore not intrusive (p.83). As we do not strive to contribute or be a part of the observations whilst the interactions are taking place online in different forums for example, we are instead observing interactions and communication that has already taken place online.

As web-based research can intend sensitive and personal information about users, it is important that ethical considerations, and possible challenges, are taken into account. In Scandinavia and other regions in Europe, there are legal standards that need to be kept where fundamental rights related to one's “dignity, freedom, autonomy, solidarity, equality, democracy and trust” are considered high values. These values are kept at a high standard as they are also heavily connected and regulated by GDPR laws (General Data Protection Regulation) (AoIR, 2019. p.5).

7.2 Validity and statistical relevance

Ecological validity can be up for discussion when it comes to collecting data that can not be guaranteed to be generalizable or representative by using surveys as a means of collecting data. Bryman argues that one should question if the results of a study can be adapted and placeable to people's everyday social environments and settings (2018, p.74). The data we collected could technically be correct in regards to the people that have been included in our research, but not necessarily adaptable to the rest of the population. Especially since all

survey participants were from Sweden, and no data was collected to measure ethnic participation. In regards to the ecological validity of our research, the unnatural setting of answering questions in a survey could therefore perhaps limit the validity of our collected data (ibid.). We do acknowledge however that a larger set of respondents would also prevent certain limitations, but for the scope and time frame of this paper, a larger dataset would not be manageable.

8. Conclusions

In this study, we aimed to gain insights into how users understand and perceive their privacy and security on web applications. We have focused on how the design of interfaces on web applications affects users' ability to make individual choices in regard to their informational privacy. By utilizing surveys and netnographical observations, we have analyzed our results through quantitative analysis methods such as bivariate analysis, correlation tables, and chi-square tests.

8.1 Main findings

As suggested by our correlation tables containing the survey data, there is no significant correlation between the level of concern and experience or comprehension. This point proves that individuals may experience significant privacy concerns irrespective of their internet proficiency or understanding of privacy settings.
We did however discover a significant positive correlation between users' experience of using web applications and their comprehension levels of privacy settings. This would suggest that the more experience a user has, the better they understand privacy settings or privacy policies.

The observations we conducted also provided us with some insight into what protective or preventative measures were taken by users who were concerned about their information being collected. As our findings confirmed through our analysis, there was no correlation between user types and the type of privacy concerns they encounter. However, we did find some interesting viewpoints and perspectives from online users through our observations. In summary, users on Reddit engage in discussions about privacy and safety. The diversity of contributors, including devotees, newbies, and minglers, suggests a broad user base with varying levels of expertise and experiences in addressing privacy concerns on different

platforms. These observations underscore the universal importance placed on privacy across various online platforms.

We can also conclude that users on platforms like Reddit and Familjeliv express a collective desire to enhance their online privacy settings, with shared frustrations regarding the navigational complexities of Facebook and Google. This suggests a universal need for user-friendly interfaces and increased transparency in platform settings. Another notable trend for potential exploration in future research is the recurrence of specific web applications. The platforms that surfaced most frequently in the word cloud from our survey findings align with those commonly raised in our observations regarding privacy concerns.

- Is there a difference in how informational integrity, privacy, and security is perceived by its users on installed versus browser-based web applications?

Our survey and observational results indicate a noteworthy correlation between users' perceptions of their informational privacy and the design of web application interfaces. Respondents, when asked about what defines a secure web application, commonly expressed skepticism about achieving complete safety on the internet, particularly on websites. This suggests a perceived lack of control over maintaining informational integrity, possibly attributed to issues like transparency and security breaches. Moreover, privacy concerns expressed in this study seem to stem from external influences rather than users' actions.

Due to this fact, we cannot say for certain whether or not this concern would differ between web applications as the threat is not directly related to the application itself. What we can conclude from our study, however, is that there is an appreciation for transparency and non-ambiguous settings regardless of the type of web application. Any indications of encrypted connections or data signaled through visual representations, are an indication of reduced concerns regarding informational privacy. To further research users' privacy concerns and protective measures, it will be essential to analyze the risks and factors that elevate the risk of external interference or unauthorized access to information. That is to say, if websites were more vulnerable to cyber attacks or data leaks, that would signify increased concerns regarding web applications in browsers. The findings of this study could not prove this theory, however.

- What role does the web application’s interface have in allowing its users to configure their informational privacy settings?

The web application's interface is posited as the source of affordances for users to manage their information and privacy. Control over informational privacy is constrained by the interface's design, despite the potential for more extensive technical functionality. The ensuing consequences of limited control vary; users may seek assistance from the application's support team or other users, take an uncertain approach, or, as highlighted in our survey, resort to more drastic measures. If users perceive a lack of control over their informational privacy, they might opt to cease using the application altogether or provide false information, thereby populating the application's database with inaccurate data. However, when presented with clear permission requests and comprehensive privacy settings, respondents demonstrated a willingness to adopt privacy protective measures.

- In what way do interface designs *nudge* users into accepting permissions or disclosing personal information?

Our survey findings support the notion that certain aspects of an application's interface design influence users to grant permissions or divulge personal information. One specific design practice highlighted by a respondent pertains to the presentation of cookie permissions. The deliberate inclusion of an "accept all cookies" option with a single click, alongside a "customize" option that requires more time to read through permissions, was noted. According to our results, this design choice is deemed inconvenient by a majority of web application users, leading them to opt for the quickest option to make the prompt disappear. This inconvenience should not be utilized by companies seeking to collect more user data, as the practice is arguably dishonest.

8.2 Implications for design

As a conclusion of our findings in terms of how user interfaces can be designed more responsibly in web applications: there are certain elements that users look for in web applications to determine if the website is reliable security-wise. These elements are as previously described:

1. Popular or high-end, professional websites
2. The address contains HTTPS
3. Lock Pad or key icons

Other elements we found which affected the comprehension levels of users positively were:

(a) A singular privacy setting isn't sufficient, yet a longer, detailed list may overwhelm users. Our research suggests the importance of maintaining a balance - offering an adequate number of privacy settings while ensuring transparency about the intentions and purposes behind data collection.

(b) None of the respondents wanted to be offered the option of “accept all cookies” without an option to “reject all cookies”. This is perhaps the most important finding in terms of “nudging” as it points to a nonconsensual disclosure of private information. Interface designs should therefore not exclude options from the user as to deliberately influence their choices.

8.3 Final reflection

Throughout this research project, we have managed to gather a large set of empirical data through our chosen methods. We managed to answer our research questions and hopefully managed to contribute with new knowledge on the topic of informational privacy.

While our chosen methods proved valuable for our specific research objectives, a reflective analysis acknowledges limitations within the scope and timeframe of this study. Future research might enhance empirical data collection by prioritizing surveys for broader data samples. This approach could enhance both ecological and representative validity. It's important to note that this doesn't diminish the suitability of netnography for our research questions; rather, qualitative methods like observations demand more time and analysis than we hoped to afford.

With that being said, the topic of privacy and privacy management, as well as security and integrity, will presumably continue to be of high importance. The purpose and aim of this study still hold as a continuation of previous research and do not disprove earlier conclusions regarding privacy concerns. We, as researchers, hope to contribute to the discussion with this paper and possibly new knowledge to be used in future design projects.

References

AoIR, 2019. *Internet Research: Ethical Guidelines 3.0 Association of Internet Researchers.* https://aoir.org/reports/ethics3.pdf. 2023-11-05.

Balapour, A., Nikkah, H. R. and Sabherwal, R. 2020. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management.* 52. 102063.

Berg, M. 2015. *Netnografi: Att forska om och med internet*. Lund: Studentlitteratur.

Boerman, S. C., Kruikemeier, S., and Zuiderveen Borgesius, F. J. 2021. Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research.* 48(7). pp.953-977.

Bowler Jr., G. M. 2010. Netnography: A Method Specifically Designed to Study Cultures and Communities Online. Book Review in *The Qualitative Report*. 15(5). pp.1270-1275.

Bryman, A. 2011. *Samhällsvetenskapliga metoder*. Stockholm: Liber

Bryman, A. 2018. *Samhällsvetenskapliga metoder*. Stockholm: Liber

Eastin, M. S., Brinson, N. H., Doorey, A. and Wilcox, G. 2016. Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior.* 58. pp.214-220.

Himma, K. E. and Tavani, H. T. 2008. *The Handbook of Information and Computer Ethics.* New Jersey: John Wiley & Sons Inc.

Internetstiftelsen, 2021. *Svenskarnas oro kring den personliga integriteten på nätet*. https://internetstiftelsen.se/om-oss/press/pressmeddelanden/svenskarnas-oro-kring-den-personliga-integriteten-pa-natet/. (Accessed 2023-11-17).

Kozinets, V. R. 2011. *Netnografi*. Lund: Studentlitteratur.

Lofland, J., Snow, D., Anderson, L. and Lofland, H.L. 2006. *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis*. Waveland Press: Illinois.

Malhotra, N. K., Kim, S. S. and Agarwal, J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research.* 15(4). pp.336-355.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*. 20(2) pp.167-196.

Swedish Authority for Privacy Protection, 2023. *Processing of personal data – for researchers.*https://www.imy.se/en/organisations/data-protection/processing-of-personal-data--for-researchers/ 2023-11-30.

Taddicken, M. 2013. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication.* 19. pp.248–273.

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

Pictures

[Photography on title page]
Pexels, 2016. Unknown Title [Online] Tags: Apple, Desktop, Laptop, Notebook. Available at: https://www.pexels.com/sv-se/foto/anteckningsbok-apple-arbete-barbar-dator-39284/ (Accessed 2023-12-15)

Appendixes

1. Observation scheme

Online Social Network Observation Schedule: Privacy, Integrity, and Digital Security Discussions

Objective: To analyze netizens' attitudes, behaviors, relationships, intentions, and discourse regarding privacy, integrity, and digital security on online social networks.

The online space			
Platform:			
Keywords or hashtags commonly used:			
Open/Private:		Active/Inactive:	
User profiles			
Access	**Public profile**	**Private profile**	
Frequency of posts or interactions			
Type of user			
Ages (if applicable)			

Interactions			
Attitudes and opinions			
	Date	By User	Description
Expressions of concern			
Expressions of indifference			
Mention of recent event or related incident			
Behaviors and User interactions			

Sharing personal info			
Use of privacy settings			
Overall engagement			
Agreement/Disagreements			
Responses to others' posts			
Sharing of tips/advice on maintaining digital security			
Any stories or anecdotes related to privacy breaches			
Language and tone			
Tone of discussion			
Terminology, use of specific language?			
Relation to the platform			
Level of trust in the current platforms privacy features			
Complaints or praises towards the platform's handling of user data			
Intentions and actions			
Any initiatives towards enhancing digital security practices			
Participation in any campaign or movement related to privacy			
Perceived Threats			
Identification of specific threats to privacy			
Discussions about			

evolving online threats			
Use of Multimedia			
Are images, videos or infographics used in discussions?			
Other content shared related to privacy and digital security			
Emerging Trends			
New topics or concerns gaining traction			
Any significant shifts in sentiment or public opinion			
Awareness, critical thinking and ethical considerations			
Use of trust-worthy sources in sharing of information			
Use of questionable sources without credibility			
Ethical implications discussed of online actions			
Platform's responsibility in ensuring user privacy			
Perceived personal responsibility in their own actions regarding privacy			

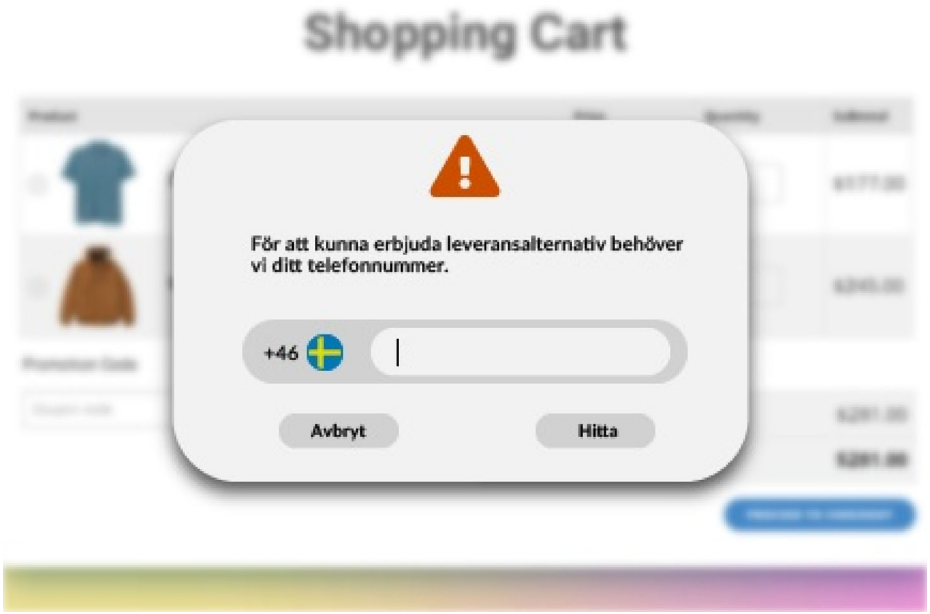
Key findings and observations:

Any identified patterns, trends, areas of particular interest for further exploration

2. Visual Examples Survey

* 10. Du är inne på en shoppingsajt, och har precis gått till kundvagnen för att betala för dina varor. Du får upp den här rutan när du börjar fylla i dina uppgifter.

Du har redan skrivit in din adress. Är det nödvändigt för sidan att be om telefonnummer i detta fall?



- ◯ Ja
- ◯ Nej
- ◯ Jag vet inte

* 11. Du registrerar dig på ett forum för katt-entusiaster. I slutet av registreringen ombeds du att även fylla i ditt telefonnummer utan angiven orsak. Vad väljer du att göra?

- ◯ Jag skriver in mitt telefonnummer och fortsätter registreringen.
- ◯ Jag avbryter registreringen och letar efter något som förklarar varför forumet vill ha mitt telefonnummer. Beroende på anledning kanske jag registrerar mig ändå.
- ◯ Jag avbryter registreringen och letar efter andra forum istället.
- ◯ Annat (ge exempel):

  _____

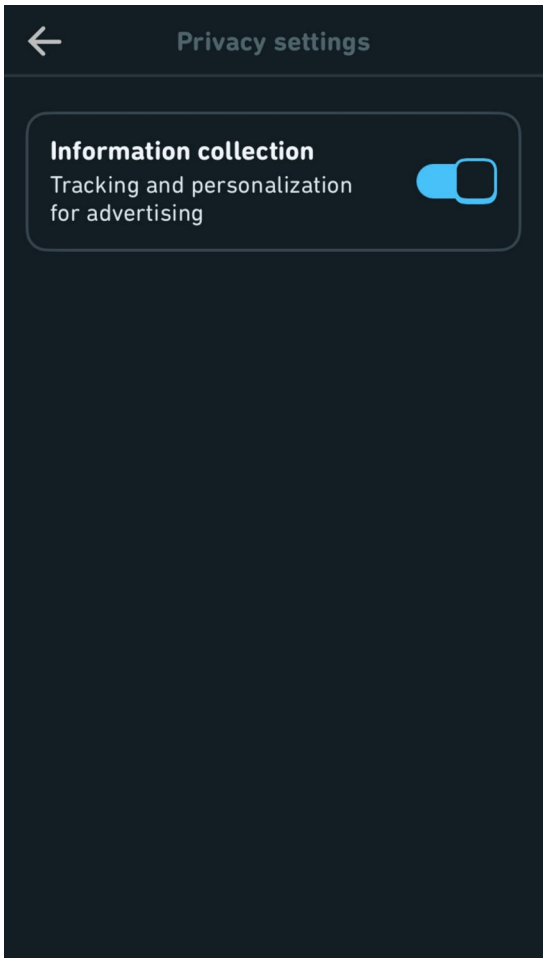
- ◯ Inget av ovanstående alternativ

* 12. Du går in på en webbsida för streaming och ska börja söka efter någon rolig video att titta på. Du får upp den här rutan:

Accepterar du?

- ◯ Ja
- ◯ Nej
- ◯ Vet inte

* 13. Upplever du att det är lätt att förstå vad denna integritetsinställning innebär? Förklara varför/varför inte.

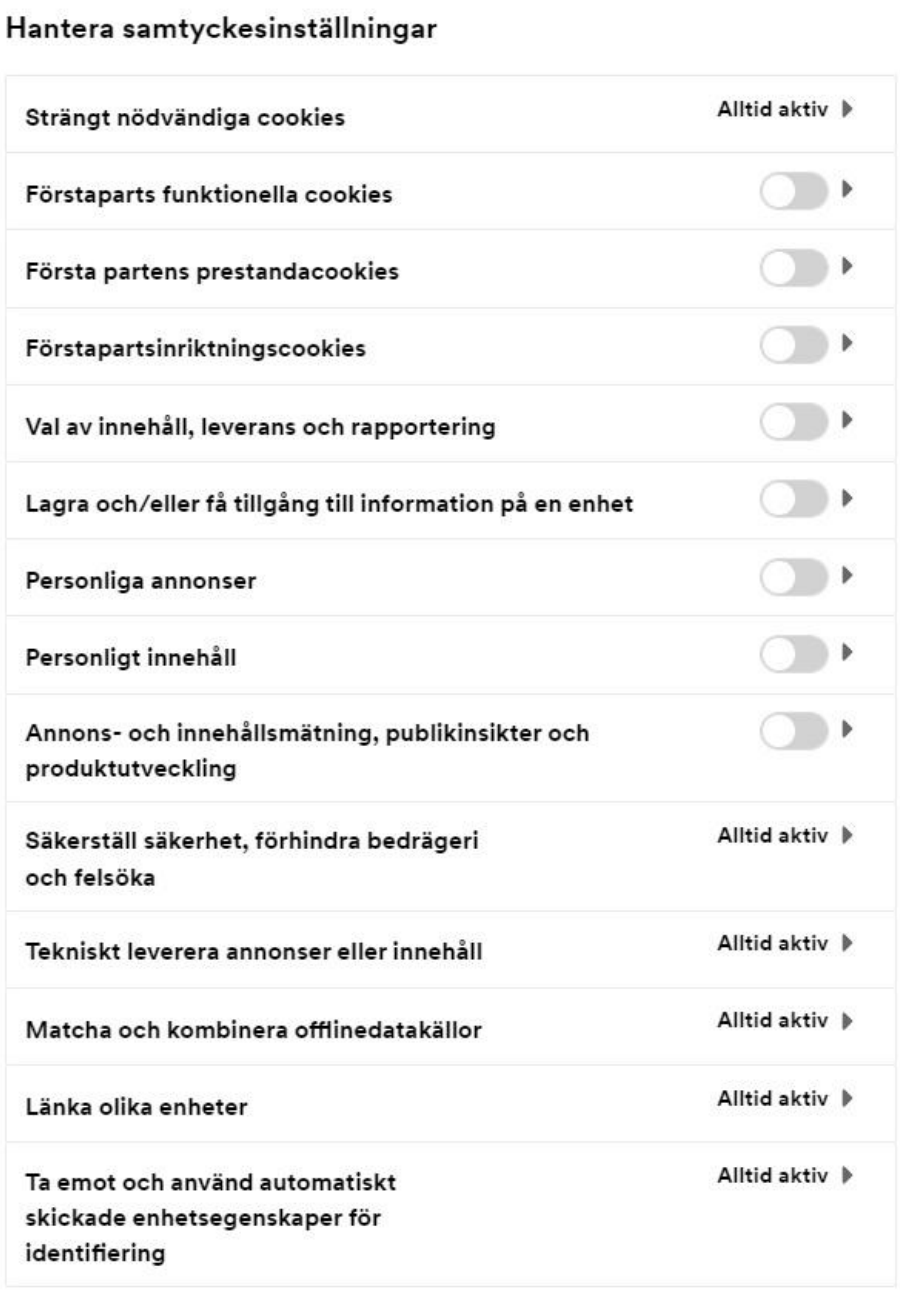


Översättning:

Informationsinsamling

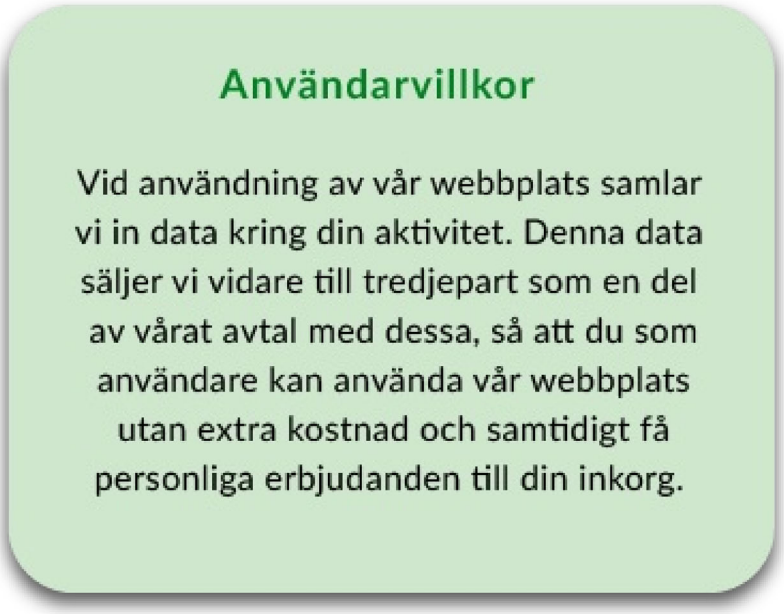
Spårning och personlig anpassning för reklamerbjudanden

* 14. Upplever du att du förstår vad dessa samtyckesinställningar innebär?



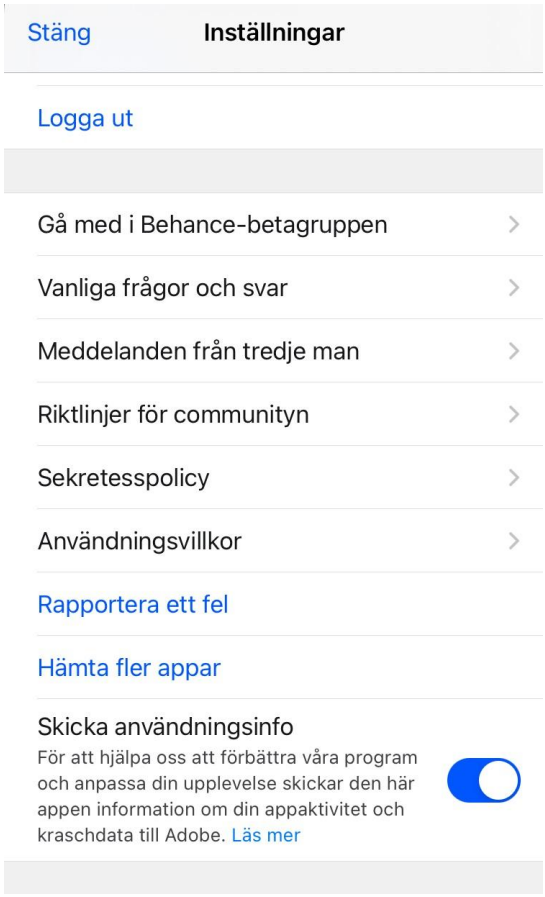
* 15. Utifrån de två föregående exemplen, är mängden alternativ rimlig för dig som användare?

* 16. Skulle detta få dig att vilja använda webbplatsen om detta stod i användarvillkoren?



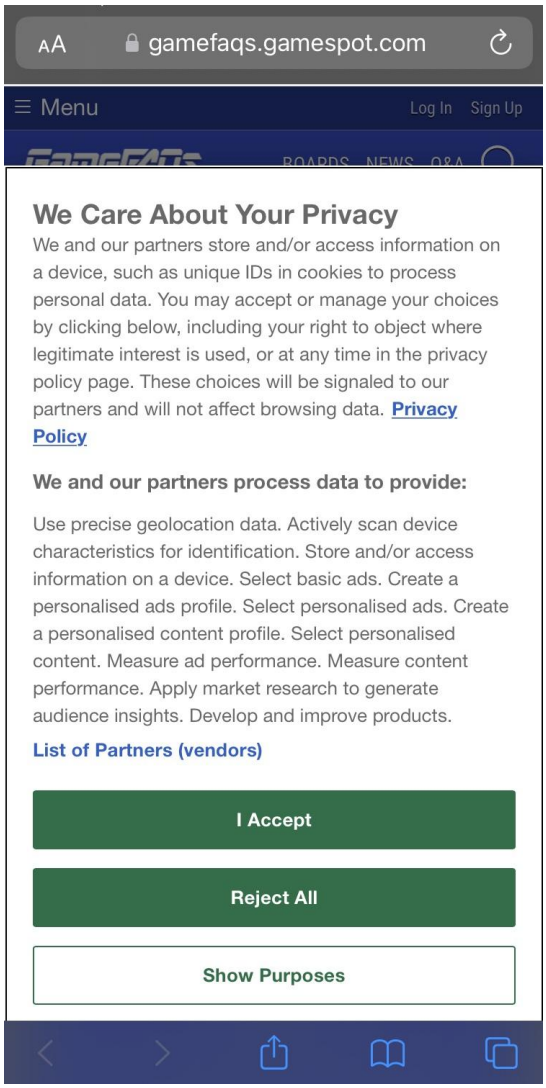
- ◯ Ja, jag har inget emot detta.
- ◯ Nej, jag vill inte att de säljer vidare min data.
- ◯ Nej, de har inte specifikt bett om mitt samtycke. Mitt användande av webbplatsen ska inte vara skäl nog.
- ◯ Det spelar ingen roll för mig.
- ◯ Annat

* 17. Du vill ändra dina integritetsinställningar i den här appen. Var klickar du?



* 18. Hur upplever du att dessa typer av rutor fungerar?
Är det bra att de täcker skärmen så du måste ta ställning innan du fortsätter på sidan? Är det ett störande moment?

Förklara gärna hur du resonerar!



* 19. Vilka alternativ vill du kunna välja mellan när du får upp en sådan ruta?

○ 

○ 

○ 

○ Inget av ovanstående alternativ

Säkerhet och integritet på webben

Avslutning

Avslutningsvis vill vi ställa ett fåtal frågor kring säkerhet och integritet och hur du resonerar eller tänker kring dessa.

Dessa är inte obligatoriska. Vill du inte svara på nedan frågor kan du avsluta enkäten genom att trycka på **Klar**.

3. Chi square distribution table

	P										
DF	0.995	0.975	0.2	0.1	0.05	0.025	0.02	0.01	0.005	0.002	0.001
1	.0004	.00016	1.642	2.706	3.841	5.024	5.412	6.635	7.879	9.55	10.828
2	0.01	0.0506	3.219	4.605	5.991	7.378	7.824	9.21	10.597	12.429	13.816
3	0.0717	0.216	4.642	6.251	7.815	9.348	9.837	11.345	12.838	14.796	16.266
4	0.207	0.484	5.989	7.779	9.488	11.143	11.668	13.277	14.86	16.924	18.467
5	0.412	0.831	7.289	9.236	11.07	12.833	13.388	15.086	16.75	18.907	20.515
6	0.676	1.237	8.558	10.645	12.592	14.449	15.033	16.812	18.548	20.791	22.458
7	0.989	1.69	9.803	12.017	14.067	16.013	16.622	18.475	20.278	22.601	24.322
8	1.344	2.18	11.03	13.362	15.507	17.535	18.168	20.09	21.955	24.352	26.124
9	1.735	2.7	12.242	14.684	16.919	19.023	19.679	21.666	23.589	26.056	27.877
10	2.156	3.247	13.442	15.987	18.307	20.483	21.161	23.209	25.188	27.722	29.588
11	2.603	3.816	14.631	17.275	19.675	21.92	22.618	24.725	26.757	29.354	31.264
12	3.074	4.404	15.812	18.549	21.026	23.337	24.054	26.217	28.3	30.957	32.909
13	3.565	5.009	16.985	19.812	22.362	24.736	25.472	27.688	29.819	32.535	34.528
14	4.075	5.629	18.151	21.064	23.685	26.119	26.873	29.141	31.319	34.091	36.123
15	4.601	6.262	19.311	22.307	24.996	27.488	28.259	30.578	32.801	35.628	37.697
16	5.142	6.908	20.465	23.542	26.296	28.845	29.633	32	34.267	37.146	39.252
17	5.697	7.564	21.615	24.769	27.587	30.191	30.995	33.409	35.718	38.648	40.79
18	6.265	8.231	22.76	25.989	28.869	31.526	32.346	34.805	37.156	40.136	42.312
19	6.844	8.907	23.9	27.204	30.144	32.852	33.687	36.191	38.582	41.61	43.82
20	7.434	9.591	25.038	28.412	31.41	34.17	35.02	37.566	39.997	43.072	45.315

4. Correlation table: Concern-Experience-Comprehension

Correlations

		LevelofConcern	Experienced	Understands Definition	UnderstandsContext ForDisclosure	Understands PrivacyRisk	Understands OneOption	UnderstandsExcessive Options	UnderstandsLa ckingOptions
LevelofConcern	Pearson Correlation	1	,011	-,082	-,025	-,025	,130	-,028	,291
	Sig. (2-tailed)		,943	,591	,868	,872	,395	,854	,053
	N	45	45	45	45	45	45	45	45
Experienced	Pearson Correlation	,011	1	,401	,321*	,282	,084	,285	,151
	Sig. (2-tailed)	,943		,006	,031	,061	,583	,057	,322
	N	45	45	45	45	45	45	45	45
Comprehension	Pearson Correlation	,127	,492	,514	,294	,394	,430	,623	,545
	Sig. (2-tailed)	,404	<,001	<,001	,050	,007	,003	<,001	<,001
	N	45	45	45	45	45	45	45	45
UnderstandsDefiniti on	Pearson Correlation	-,082	,401	1	-,177	,302*	,247	,023	,118
	Sig. (2-tailed)	,591	,006		,245	,044	,101	,880	,441
	N	45	45	45	45	45	45	45	45
UnderstandsContex tForDisclosure	Pearson Correlation	-,025	,321*	-,177	1	-,053	-,016	,263	-,050
	Sig. (2-tailed)	,868	,031	,245		,728	,917	,081	,744
	N	45	45	45	45	45	45	45	45
UnderstandsPrivacy Risk	Pearson Correlation	-,025	,282	,302*	-,053	1	,176	,112	,107
	Sig. (2-tailed)	,872	,061	,044	,728		,247	,464	,486
	N	45	45	45	45	45	45	45	45
UnderstandsOneOp tion	Pearson Correlation	,130	,084	,247	-,016	,176	1	-,117	-,159
	Sig. (2-tailed)	,395	,583	,101	,917	,247		,444	,297
	N	45	45	45	45	45	45	45	45
UnderstandsExces siveOptions	Pearson Correlation	-,028	,285	,023	,263	,112	-,117	1	,361*
	Sig. (2-tailed)	,854	,057	,880	,081	,464	,444		,015
	N	45	45	45	45	45	45	45	45
UnderstandsLackin gOptions	Pearson Correlation	,291	,151	,118	-,050	,107	-,159	,361*	1
	Sig. (2-tailed)	,053	,322	,441	,744	,486	,297	,015	
	N	45	45	45	45	45	45	45	45

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