LUND UNIVERSITY
School of Economics and Management

Department of Informatics

User Rules on Data Disclosure

The measures that users employ to protect their data on B2C e-commerce sites

Master thesis 15 HEC, course INFM10 in Information Systems
Presented in May, 2017

Authors: Chang Liu
Felix Conradson
Pritraj Singh Sehmi

Supervisor: Imad Bani-Hani

Examiners: Odd Steen
Styliani Zafeiropoulou

User Rules on Data Disclosure: The measures that users employ to protect their data on B2C e-commerce sites

Authors: Chang Liu, Felix Conradson and Pritraj Singh Sehmi

Publisher: Dept. of Informatics, Lund University School of Economics and Management.

Document: Master Thesis

Number of pages: 166

Keywords: data privacy, user awareness, information disclosure, B2C e-commerce, user rules and measures

Abstract:
The adoption of e-commerce has caused a shift in the way that businesses interact with their consumers. Business to consumer (B2C) e-commerce websites allow users the convenience of making purchases without having to physically go to the retailer's location. E-commerce practices involve the collection and use of user data for various purposes, from registration and transacting to providing suggested ads and recommendations. This collection and use of data brings up various privacy concerns for users, who may be unsure of how their data is being collected and used. Users may however have different awareness levels and tolerance for privacy risks. The current study examines the specific rules that users of B2C e-commerce websites have in place on information disclosure, and the measures that they take in order to minimize privacy risks on B2C e-commerce websites. The study applied Communication Privacy (CPM) Theory (Petronio, 2002) to e-commerce contexts and uses a qualitative research method in order to identify the rules and measures. The empirical evidence shows that while specific rules and measures vary for each individual user, there are a number of rules and measures that most users agree upon in the context of privacy on B2C e-commerce websites.

Content

Figures

Tables

1 Introduction

This chapter covers the background of the topic domain of the study, examines the problem area, and states the research question. It also states the purpose and the delimitations of the research study.

1.1 Background

The advent of e-commerce systems in business contexts has revolutionized the way that businesses and consumers interact in the modern business environment. The Internet has grown to become an essential platform for trading, selling and distributing products between organizations and customers (Corbitt, Thanasankit, & Yi, 2003). The traditional retailing model involving customers visiting retail outlets in order to browse products, compare prices and make purchases is being complemented by the use of online e-commerce platforms to carry out the same tasks from the customers' locations at their own convenience (Mittal, 2013). Some retailers do indeed retain this traditional model and complement it with the availability of online stores (for example H&M, ICA in Sweden), while other retailers opt for a fully online method of operation in terms of their retail stores (for example CDON.se in Sweden). Belanger, Hiller, and Smith (2002) adopt a definition of e-commerce that encompasses the consumer oriented interfaces, as well as back-end applications such as order processing and payment capabilities. As such, e-commerce can be thought of as an entire process that relies on exchanges of information between the customer and the selling entity in order to carry out the business transaction (Krishnan et al., 2017).

The rise of e-commerce in itself can be attributed to a number of factors. Mittal (2013) argues for the convenience that is provided by online shopping, in that the customer needs not leave their home or workplace and physically go to the shop in order to make purchases. In relation to this, it can also be arranged for products to be delivered, saving the customer the hassle of transportation. Srinivasan, Anderson, and Ponnavolu (2002) also argue about the ease in price comparison in the rise of e-commerce, whereby a consumer can look at various online stores and compare prices for a certain commodity, as compared to having to physically window shop and compare items that way. It is also easier to obtain detailed descriptions of products in a short period of time, and obtain reviews and recommendations from fellow consumers on e-commerce platforms that would help make the purchasing decision easier for a customer (Moon, 2004).

This immense shift in customers' transaction and purchasing habits brought about by the growth of e-commerce has led to the development of both business-to-consumer (B2C) and consumer-to-consumer (C2C) e-commerce platforms (Weltevreden & Rotem-Mindali, 2009). B2C platforms involve business to consumer transactions, featuring platforms for online retailing for independent stores on their own websites (Griffith & Palmer, 1999), as well as the availability of marketplaces such as Amazon for retailers to reach their customers and be able to sell to them over a third party website. C2C platforms, such as eBay, allow individuals to sell to other consumers over an internet marketplace (Wu & Bolivar, 2009). This allows indi-

vidual buyers and sellers to connect with each other and be able to transact, whereby the seller set prices for their goods, which can either be fixed, or open to bidding from interested customers. Our interest for this study focuses on the B2C side of e-commerce, with an organization selling directly to consumers either on their own independent site, or through a platform such as Amazon.

A key aspect of e-commerce operations is the collection of data from their users, which includes the personally identifiable information as well as payment details of the users, obtained through the details they volunteer when using the website (Moores & Dhillon, 2003). The data collected also includes the customer usage behavior, monitoring what pages they browse, what they search for, what they look at, and what they end up purchasing (Kohavi, 2001). This data becomes invaluable to the e-commerce organization, as it can be crucial for them in order to promote efficiency in their operations and assist their attempts to serve their customers better (Chen, Chiang, & Storey, 2012). E-commerce sites can use user data to provide personalized user experiences, customizing the website experience for a particular customer by recognizing the customer and providing a tailored selection of products, services and advertisements catering to their needs (Srinivasan, Anderson, & Ponnavolu, 2002). This promotes the use of recommendation systems in order to make suggestions to the user based upon their previous purchases and the items that they looked at (Sarwar et al., 2000). The contact information of users becomes important for advertisement and promotional purposes, as the e-commerce site can send out emails to their users to let them know of new products or deals that are currently available. The analytics aspect from user data also provides an organizational advantage in terms of market intelligence and efficient problem solving methods (Chen, Chiang, & Storey, 2012).

In light of this, it becomes evident that the e-commerce sites have an obligation towards their users in terms of ensuring that their privacy is maintained and data is kept secure. The protection of user privacy is an important aspect in the information society, and a key problem is the fact that people may be unaware of the privacy issues in electronic environments (Pötzsch, 2008). This in turn can lead to both immediate and future harms for users, causing severe problems for them due to privacy negligence or malicious intent (Mayer & Mitchell, 2012). Perreault (2015) discusses the importance of user privacy concerns in the context of e-commerce sites, talking about how information privacy concerns can influence the trust that the consumer places in the e-commerce site, which in turn influences whether or not they will be willing to make a transaction on the platform. Trust in e-commerce breeds confidence, which in turn leads to loyalty and repeat business (Gefen, 2000). Palvia (2009) also discussed the importance of trust, highlighting its fundamental importance in online exchange relationships, such as the relationship between e-commerce sites and their customer base. Organizations that lose their customers' trust through the persistence of blatant privacy concerns go on to experience a decline in transactions, therefore also end up losing their customers in the long term (Perreault, 2015).

1.2 Problem area

One of the main concerns involved with data collection on e-commerce sites is that there is a trade off involved in customization of the site experience for each user (Hann et al., 2002). The user may want to browse the site as anonymously as possible, while the e-commerce site administrators may at the same time strive to uniquely identify each site user in order to give

them a personalized experience and improve the suggestion recommendation system performance simultaneously, through the use of data collection procedures such as cookies (Srivastava et al., 2000). This gives rise to an ethical dilemma, especially in the case of third party cookies. Third party cookies differ from regular cookies in the sense that the cookies in this case are owned by a third-party company, and not the e-commerce site themselves. The third-party cookies, or persistent cookies, are able to track the user's browsing habits and create tailored ads and links for the user, depending on what they have searched for or looked at previously while the cookies were active and tracking their behaviour (Mayer & Mitchell, 2012). This brings up an issue of privacy and security, as the user may not be fully aware about what is being recorded about their internet activity, seeing as the third-party cookies operate through building a user profile and monitoring their activity across websites (Ramlakhan, 2011). The users may therefore need to resort to the use of measures for privacy protection in order to safeguard their personal data, in order to protect themselves from potential harms that could be caused through privacy and security breaches.

Awad and Krishnan (2006) discuss the problem of privacy invasion in e-commerce contexts as well, and discuss the trade-off between consumers wanting personalized and efficient service from online retailers while avoiding the problem of online profiling and use of their data for advertising purposes. Their findings showed that users may be willing to disclose their data for use in recommendation systems and efficient online service, but not so much in the use of their data for online profiling in terms of advertisements and unsolicited communication. This brings about a problem all of its own, since it is difficult to judge what the limits to information disclosure are for users of e-commerce sites, and what rules they have in place in order to ensure that they can get the personalized service that they value, while avoiding the spam advertisements that they perceive as annoying. There is also a gap in knowledge pertaining to what measures the users take once their data has already been collected in order to avoid the undesirable aspects of online profiling, such as excessive advertisements and unsolicited communication.

It can be argued that e-commerce websites do provide users with information regarding the data collected from them when they use the sites, using privacy agreement notices and ensuring that users agree to the terms of the user agreements (Earp et al., 2005). However, most of the time users may not take the time to read the entire text in the user agreements, and even when they do they may not completely understand the terms that they are agreeing to (Luzak, 2014). Pollach (2007) also argues that the user agreements often contains language choices that serve to highlight the positive aspects of the data collection that occurs the sites, while placing the potential privacy invasion and risk of compromise in the background. A key problem therefore arises when users agree to data collection terms that they may not understand completely, and potentially put themselves and their data at risk through use of e-commerce sites. Users may be tempted to just click "agree" without fully understanding what exactly they are agreeing to, due to either a lack of understanding of the syntax or a lack of time to read through the long user agreement statement text (Jensen & Potts, 2004). Once the users have already agreed to the terms of the user agreement, they may then be forced to take measures to protect the privacy of their data, since they have already agreed to surrender it to the site that they have chosen to use. In light of this, we argue that the topic domain of user rules on information disclosure, and measures taken by users to mitigate the threats posed by the lack of privacy of their data that is collected by e-commerce sites could be better covered in IS research, providing the motivation for choosing this subject area for our thesis study.

1.3 Research question

Based upon the outlined problem area, the focus of this research will be on the user perspective on data collection that occurs on e-commerce websites. The research aims to investigate the awareness of users on the safety and privacy of the data that they surrender to e-commerce site operators, and how the users attempt to keep their privacy and individual security intact in the light of potential threats to them in terms of privacy and security issues. It is key to establish the levels of awareness of users of B2C e-commerce sites about the privacy of their personal data and the particular potential threats of privacy breaches through our research. The establishment of the awareness of users about personal data privacy and their perspectives on potential threats posed by the collection of their personal data contributes to the basis of the research question derived for this study:

What measures and rules do users employ in order to mitigate data privacy concerns on B2C e-commerce sites?

In the context of this study, the rules that we are seeking to identify refer to the guidelines that users employ before agreeing to voluntarily disclose their information to a B2C e-commerce platform. The measures refer to the steps that users take in order to protect their privacy once their data has already been collected by the e-commerce site, either voluntarily (such as in the case of filling out fields with information) or involuntarily (such as collection of data through cookies).

1.4 Purpose

The purpose of this study is to identify the rules that users set for themselves when disclosing information on e-commerce platforms, and also identify the measures that users employ in order to govern the protection of personal information on e-commerce websites. In order to achieve this, it must firstly be established whether users are aware of privacy concerns on the e-commerce platforms. As users grow aware of these various concerns, they also become more careful about assessing the risks and benefits of information disclosure on e-commerce platforms as a result. As discussed in Metzger (2007), this then leads to the establishment of user rules in information disclosure in the context of privacy on e-commerce websites.

The study seeks to collect and analyze data regarding user perspectives on e-commerce platforms from people who have used these platforms before and have experiences of online shopping. Naturally this would entail a qualitative method of research that would allow us to obtain data through the use of interviews with users of e-commerce sites in order to obtain detailed empirical data. This establishes the level of user sensitivity to information disclosure and online privacy on e-commerce sites, and the reasons behind their sensitivity. The qualitative interviews will also give in depth insights into the practices of users when it comes to disclosing their information online. Ultimately, this allows us to show empirically how the users try to mitigate the threats of online privacy concerns using various measures, and what rules they employ in information disclosure online in order to minimize the risks of privacy breaches.

The study aims to contribute to the field by helping researchers and practitioners to understand how users respond and mitigate to the privacy concerns brought about by the practice of

their personal data being collected by e-commerce websites. We hope to obtain an understanding of the rules and measures that contribute to user practices on information disclosure and privacy, and by doing so also identify the motivations that users have for using the identified rules and measures. The user attitudes towards online privacy concerns play a critical role in avoiding ethical issues from organizational perspectives as well, which could influence e-commerce organizations to better structure their data collection activities and transparency in order to better facilitate user confidence and encourage disclosure of valuable data for business use. This would ultimately lead to a better customer experience on e-commerce websites, while simultaneously allowing the e-commerce retailers to obtain the trust of their users and provide protection for their data in order to provide optimum services to them.

1.5 Delimitation

This study is delimited to identify the user rules regarding information disclosure and measures of protecting personal information on e-commerce websites, more specifically focusing on B2C e-commerce platforms that involve interaction between a business and a consumer. However, the study does not take into account the privacy issues faced by users on C2C marketplaces, which involve interactions between individuals selling their own personal items to each other (for example, eBay). This is because C2C e-commerce websites may be perceived as having more anonymous interaction as compared to B2C websites (Weltevreden & Rotem-Mindali, 2009). B2C websites involve businesses as retailers, where the user in most cases knows the retailer that they are interacting with, or can find details about them as a registered organization. In contrast, the anonymity of individual sellers on C2C platforms could lead users to undertake a completely different set of measures or privacy rules in order to keep themselves safe, which could be a separate study on its own.

In addition, this study focuses on user perspectives on data collection, and does therefore not discuss the ethical aspects involved in data collection and usage from organizational perspectives. The study does not analyze the mechanisms of data mining and data transmission, since these fall outside the scope of our research. It is key to note that the empirical data collected in the qualitative research conducted may not necessarily represent the views of the entire community of B2C e-commerce website users. This is due to the smaller sample size for empirical data collection making the findings limited to their insights, which may not necessarily represent the insights of the entire B2C e-commerce site user population. The sample was limited to users within our immediate environment who had experience with shopping on B2C e-commerce sites. This affects the generalizability of our research, as the entire population of online shoppers may not share the same rules and employ the same measures that are consistent with the empirical findings of our research.

2 Literature review

This chapter explores the concepts discussed in the existing academic literature in the domain of our study, in order to understand the findings obtained by previous researchers, analyze gaps and questions in their research, and gain perspective on the methodologies and theories that they used and proposed in their studies.

2.1 What is online privacy

In order to understand the meaning of online privacy in the scope of e-commerce and online transacting, we must first understand what exactly the user's privacy means. Online privacy as a concept may be difficult to rationalize (Iachello & Hong, 2007), as there may be a difference between the privacy preferences and user behavior across platforms depending on cultural and contextual backgrounds. Li and Karahanna (2015) discuss the role of privacy concerns in terms of whether or not users will choose to share personal information for a personalized experience on the websites, as compared to not sharing information and forfeiting a personalized website experience. An example of a factor that could influence the level of privacy awareness and concern from the user perspective is the personality difference between different users; extroverts could feel more comfortable than introverts when sharing information about themselves (Lee, Ahn, & Bang, 2011). Similarly, the level of concern differs from person to person depending on whether or not they have a more independent personality (Peslak, 2006). Encio (2014) explored whether or not the professional background of individuals has an impact on their perception of online privacy and security, and found that consumers from an IT or technical background show more concerns about privacy issues as compared to consumers from industries from non IT backgrounds, such as fashion, manufacturing etc.

Privacy in the context of our study can be defined as the protection of personal data from unauthorized access, use, distribution and manipulation. Personal data can furthermore be broken down into the data that can be linked to specific individuals, including, but not limited to, names, physical addresses, email addresses, phone numbers, social security numbers, credit card and bank details, and other identification numbers (Frackman, Martin, & Ray, 2002).

Turner and Dasgupta (2003) outline three key elements for information privacy; separateness, restricted access, and beneficial use; whereby separateness refers to the ability to describe the boundaries and ownership of the data, restricted access refers to the protection of the data that has been collected by only allowing authorized entities to access it, and beneficial access means that only the data owners, or parties that have been authorized to collect the data, are able to benefit from its use. By taking these three elements into account, it can be implied that the privacy of the user's personal data is upheld as long as the key conditions for information security are satisfied. Firstly, there should be a clear definition of who owns the data, and to what extent the data belongs to the collecting party or to the user; secondly, there should be no unauthorized accessing or sharing of the data that has been collected from the user, and thirdly, only the user and the collecting party that has been authorized to use the data should

be allowed to benefit from the data, and no external entity should benefit from the user's personal data.

However, it becomes a problem when these elements are not always upheld in terms of collection of user data, since it compromises the privacy of the collected data. In some cases these elements can be quite unclear, for example, it can be unclear as to who actually owns the data that is being produced and collected (Perreault, 2015). Basing his argument in the context of today's widespread smartphone use, the author uses the example of location settings on users' smartphones while they browse online. The location of the user can therefore be pinpointed and collected through the location services on their phones. Does an e-commerce site have the right to collect and use this information then, considering that it may be unconsciously surrendered to them by the user when they browse the site using their smartphones? Similarly, the use of persistent or third party cookies on browsers could be considered to have the effect of unauthorized sharing of the users' data across the websites that they browse through, as well as provide benefit to unauthorized parties by allowing them access to the user's data.

2.1.1 Online privacy concerns

One of the key concerns from the user perspective on e-commerce sites is informational privacy (Belanger, Hiller, & Smith, 2002; Paine et al., 2007). Users are concerned about the data that is collected from them while they are using the e-commerce sites, how the data is stored, and who has access to the data. For example, users could be concerned about how their usage of the website is being tracked, and how the data that they are surrendering in such a situation is being used. There is also cause for concern in terms of data storage, since users cannot be sure that their data is being stored in a secure manner free from leakage to unauthorized parties. This in turn leads to the problem of data access, whereby users may be concerned as well about who exactly can access the data that has been collected from them, and whether or not the data is safe with these entities that are allowed access to it.

To build onto the outlined issue of information privacy, the main concern for users on e-commerce sites in terms of privacy is the use of their data for a different purpose as compared to the purpose that was specified when it was collected, causing the issue of secondary usage of user information (Turner & Dasgupta, 2003). The concept of secondary use of information as a concern for users also encompasses the collection and access of user data by third parties other than the e-commerce sites (Belanger, Hiller, & Smith, 2002; Pollach, 2007). Third party data collection and use can occur due to methods such as third party banners on e-commerce sites that attract the unsuspecting users to click on them, allowing the third parties access to the user's browsing information. The users' personal information can also be collected through the use of persistent third party cookies, and as the users may be unaware that these are active or exist, or how they work, it can be considered that this is also a form of secondary data use that could be a cause for concern for users.

Mayer and Mitchell (2012) categorize the harms that can be caused as a result of privacy and security issues on the internet as threefold, economic, physical, and psychological harm. The authors further emphasize the role of actors who may find themselves with access to user data, and take an action to cause harm using the compromised data. For example, the actor could be a hacker, who accesses the data through nefarious means by hacking into a database. The hacker can then use the data to commit fraud, causing economic harm to the user who gave up their data for collection. Another instance of harm could be caused by a malicious employee

of the organization as the actor, accessing the data using their position at the company, and leaking sensitive information about a particular user on a public platform with the intent to cause psychological harm. This gives users the impetus to employ measures to protect themselves in terms of privacy, in order to ensure that the data they give up is not used in a way that could harm them.

Turner and Dasgupta (2003) illustrate this point further by discussing the modern day dynamics of online business activities, highlighting the practices of third party information access through monitoring usage behavior, sharing arrangements in terms of data, or acquisition and purchases of data. The authors further discuss the role of sophisticated modern day data mining tools that are in use in e-commerce organizations, which are able to match and aggregate data sources, allowing organizations to build more accurate user profiles and uncover minute details about the users of the e-commerce websites. This kind of detailed mining and analysis of user data could be considered to be an invasion of privacy, as this process may allow the e-commerce organizations are able to find out information about the users which is deeply personal and beyond what the user might have been willing to provide to the organization.

Another key privacy concern from a user perspective involves the misuse of contact information such as emails and phone numbers for unsolicited marketing communication from e-commerce organizations (Pollach, 2007). The unsolicited contact could be through phone calls, or through junk mail sent as spam to a large number of users (Belanger, Hiller, & Smith, 2002; Paine et al., 2007; Udo, 2001). This kind of communication could feel like a misuse of user data from the e-commerce organization, using part of the user's personal information in form of their contact details to cause annoyance to them. Yazdanifard et al. (2011) also discuss the problem of online purchase fraud as a privacy concern, whereby user data in the form of credit card and bank information is intercepted by hackers or scammers in order to cause economic harm to the users by carrying out financial fraud and stealing their funds. Such instances may occur on e-commerce sites that may not have sufficient security policies and procedures in place in order to provide protection for users against such hackers and scammers.

There could also be instances of false websites that mirror the layout of trusted e-commerce sites, luring in victims by appearing legitimate and reliable. Criminals may use these sites to offer deals that may seem too good to be true, using cheap prices and fake consumer reviews in order to gain the users' trust and coax them into providing their personal data and use it for malicious purposes such as fraudulent or criminal activities (Abbasi et al., 2010; Zahedi, Abbasi, & Chen, 2015). Paine et al. (2007) also discuss the possibility of viruses and malware being used in order to invade user privacy by intercepting their data not only from the e-commerce sites but from their devices as well. These threats can be used to compromise user data by taking advantage of lax security infrastructure on e-commerce platforms in order to piggyback on the transactional functionality of the e-commerce sites and intercept user data, which can then be used by malicious parties to cause harm to the users.

2.2 User awareness about data collection

The level of user awareness about data collection and the control that the users have over the data that they surrender to e-commerce sites are key players in determining the actual information privacy concerns (Perreault, 2015). In order for the users to have concerns about privacy, it is imperative that they first have the knowledge or awareness that there is actually

something to be concerned about. They must understand that online transactions on e-commerce site involve the sharing of personal data, and have a level of understanding about the risks involved with this sharing that causes privacy concerns to exist. We could therefore define user awareness on e-commerce sites in the context of this IS research as the level of knowledge that the users of e-commerce sites have in regards to the situation pertaining to the tracking, collection, analysis and use of their personal information, that could be surrendered to the site either voluntarily via data collection forms or through behavior monitoring tools such as cookies.

Different users may have different levels of awareness, which could as well be dependent on their risk tolerance that they have for their personal privacy (Perreault, 2015). Users who have lower risk tolerance characteristics may have a higher level of awareness about privacy concerns on e-commerce sites, while on the other hand the users with higher risk tolerance levels may not bother themselves as much with privacy concerns. In a scenario for instance where a user has a lower risk tolerance, they may take it upon themselves to do some research about data collection on e-commerce sites, and in that way understand properly what information is being taken from them. They may then choose to take measures in order to protect their information privacy, after gaining the awareness of the situation on the sites that they use.

In light of this, one of the key aspects that must be taken into account when discussing the concept of user awareness is that some users may not completely understand that e-commerce websites have the ability to incorporate operational systems that actively search for, obtain and store personal and system data during the user's online session on the site (Whitman, Perez, & Beise, 2001). This could especially be true when taking into account novice computer users, who may not be as tech savvy as more experienced computer users, and as such may not fully understand the nature of data collection procedures and activities on e-commerce platforms. For example, an elderly person who may not have grown up surrounded by e-commerce technology may not understand and have the same level of awareness regarding user privacy as a young person who has been making online purchases from a young age.

Similarly, Chen, Beaudoin, and Hong (2017) discuss the importance of experience as a teacher in terms of awareness of online privacy issues, using the example of people that may have been the victims of online privacy hacks and suffered economic harm as a result being more likely to have a higher level of awareness of the severity of the consequences of online privacy breaches. As a result, victims of online privacy breaches are likely to be more careful with analyzing what is collected from them on e-commerce sites. They may also be more cautious when disclosing their personal data when online and browsing an e-commerce site, and take measures to protect themselves from unauthorized collection of their information so as not to suffer from another breach of privacy.

Encio (2014) found that consumer negligence in terms of awareness plays a key role in privacy breaches on e-commerce platforms. The author elaborates on the idea that while e-commerce sites may have their vulnerabilities in terms of opportunities for unauthorized parties to gain access to user data, majority of the time security breaches are caused by a lack of awareness causing negligence on the part of the user. Unaware users as a result are more susceptible to threats such as fraudulent banner ads leading to imposter sites, despite the security measures that may already have been put in place on the e-commerce site. On the other hand, Perreault (2015) discusses the idea that consumers are willing to disclose personal information despite the threat of privacy issues, if there is sufficient benefit involved for them as a result of disclosing the information.

This idea is explored by Stanton and Stam (2002) as well, whose work with information boundary theory proposes that users' willingness to share and disclose their personal data is dependent on user perception of their relationship with the organization that collects the data, as well as the expected use of the data, and the expected benefit to the user as a result of sharing the data. As such, the user may be well aware of the data collection that is ongoing, but could choose to share their data due to the perception of the collecting organization as being reliable and well reputable, and having set out a clear objective in terms of the use of the data and the benefits that the consumer gets through sharing their data. Similarly, if a user's data privacy concerns outweigh the benefits of disclosing their data to the e-commerce site, then they are likely to disengage from using that particular e-commerce platform due to the increased perception of risk to the privacy of their data (Li, Sarathy, & Xu, 2010; Perreault, 2015).

2.2.1 Use of cookies

Cookies are an inherent part of web applications today, and are used to track users and their behaviour. However, the use of cookies spawns implications related to user online privacy, as the main goals of online advertisers and data brokerage firms are to collect as much information as possible about users in order to supply them with specialized and targeted ads towards the users in question (Cahn et al., 2016). The concerns of privacy and cookies have been discussed in research literature and popular press for many years, which has led to a multitude of different tools that handle cookie management and removal (Cahn et al., 2016). Passwords, page visits, and the dates for which when sites were visited are all things that can be tracked through the use of cookies (Cahn et al., 2016).

The methods of data collection via cookies used by e-commerce sites may include server level, client level and proxy level collection techniques (Srivastava et al., 2000). The data could be collected using log files that automatically track and record user behavior on the e-commerce sites, or through embedded JavaScript code on each of the web pages themselves, that sends user activity to the e-commerce site operator from the client side computer or device (Murdock, 2006). The JavaScript method involves the use of cookies, which are small data packets that store user information on the user's browser. Each time the user opens the URL again, the cookies send the user's stored information from their computer to the web server, allowing sites to access the user's information from the previous times they may have visited the site (Panda Security Mediacenter, 2014).

The majority of cookies are active until the user exits the web browser; however, persistent cookies that have a preset expiration date remain on the user's hard drive until the preset expiration date is reached (Whitman, Perez, & Beise, 2001). The web browser returns a persistent cookie to a server upon following visits, which allows the browser to identify the user as a foregoing visitor (Whitman, Perez, & Beise, 2001). The use of persistent cookies give rise to even more significant privacy issues than that of regular cookies, since storage of navigational streams and login information can be used for monitoring and tracking user browser behaviour and linking to any provided personal information (Turner & Dasgupta, 2003).

2.2.2 Reasons for not using measures to protect personal privacy

According to a study conducted by Paine et al. (2007) regarding online privacy, internet experience was the most significant indicator if users take action to protect their privacy online or not. The study also concluded that the more time spent online, the more likely it is to take actions in protecting one's privacy, and the more Internet experience, the more the users will have knowledge about possible privacy threats, and will know what can be done in order to protect them from these threats.

In the same study by Paine et al. (2007) it was also noted that the participants approach privacy issues in the context of their own practices, stemming from their own experiences and concerns. In their study, 73% of the respondents stated that they took measures in protecting their privacy online. Firewalls, hiding of IP addresses and anonymizing services are some examples of measures they found that users take in order to protect privacy. However, there were a proportion of the respondents that did not take any measures in protecting their privacy. Reasons for not taking any action in protecting online privacy were examined, and the most dominant reason was indifference, meaning that the respondents simply did not care about privacy. Another big factor was that the respondents in their study did not know in what ways their privacy could be protected. Many of the respondents in their study also stated that there was no need to protect their privacy, since they felt that they were safe enough.

2.3 User agreements and privacy policies

The user agreement is an integral part of the e-commerce site and a primary facilitator to their operation. It is the key link to user relationships, as this agreement is what contains and specifies the terms, conditions, regulations, policies and relevant laws under which the operation and transactions on the website occur. It acts as a guideline for what the user and the organization are liable for, and serves as a service contract outlining the terms of engagement between the involved parties. With the modern online business environment raising plenty of privacy issues for consideration, organizations that conduct business on their internet platforms in the e-commerce environment are providing privacy policies as part of the user agreements for using the websites, in an attempt to assuage user fears about privacy issues while they transact. (Whitman, Perez, & Beise, 2001)

However, a key problem with these policies in user agreements manifests when organizations attempt to sugar-coat the data collection and handling procedures by highlighting the positive aspects and beneficial reasons for user data collection within their policies, and push the potential issues for security breaches and privacy invasion to the background, increasing the user perception of legitimacy in terms of data collection and safety of data (Pan & Zinkhan, 2006; Pollach, 2007). A company could for example illustrate that user data is collected in order to create a tailored and personalized experience for the user, which is a beneficial aspect of data collection from the user perspective. Meanwhile, the company may at the same time downplay the methods that they use for promotional purposes owing to use of third party persistent cookies, by ensuring that tailor made sponsored ads appear on the other websites that are also used by the same user such as their social media sites.

One of the key issues regarding user agreements actually comes from the users' side of the coin - since majority of online platform users fail to read through the agreement at all, or skim

through it quickly and fail to read it in depth and try to fully understand the terms and policies presented within the agreement. Hillman (2006) attempts to explain this phenomenon by suggesting that the online transaction environment is not usually the best for reading lengthy pieces of text that encompass user agreements. The author tries to justify this claim by suggesting that online shopping on e-commerce sites, by its design, is meant to be convenient and quick, and therefore users of the e-commerce sites are often more hurried and impulsive in nature while using these sites. As such, they may not have the time or patience to sit down and scrutinize through the clauses and policies specified in the user agreement as, for example, they might have done with a physical hard copy document that they would actually have to sign.

While users continue to list the secondary use of data as a key concern in terms of personal data privacy, one of the things that they fail to realize when they neglect reading the entirety of the user agreement is that the terms of user agreements may contain policies that specify exactly how the data is used, and the technological remedies that may be available for users who do not wish to share their data (Turner & Dasgupta, 2003). In such instances, the users may have nobody to blame but themselves in the event of an invasion of what they may perceive as their private data, since they agreed to the terms outlined in the user agreement. Pollach (2007) suggests that one of the reasons for users failing to read through the entirety of user agreements, or skipping through them entirely and accepting the terms without reading through, is that the syntax used in the texts for the user agreements may be difficult to understand. In such instances, it may be that the words and terms used in the user agreement are technical and industry specific jargon, which may not be easily understood by laymen who may not have a very technical background. This could lead then to users accepting the terms of the user agreements without actually knowing what they mean (Weltevreden & Rotem-Mindali, 2009), just so that they as users can benefit from the e-commerce service, browse products, make purchases, carry out transactions and make payments.

Perreault (2015) also argues that in some instances, customers may just sign up for a basic service and volunteer their basic information primarily for subscription purposes, but due to a lack of understanding or awareness caused by failure to read the user agreement, may end up surrendering a lot more information through the tracking of their usage and presence of persistent cookies. Clearly stated privacy policies and information disclosure procedures that increase the awareness of the user regarding what is collected from them and how it is used play a key role in legitimacy of the e-commerce platform in the user's perspective (Pan & Zinkhan, 2006). Perreault (2015) further explored the expectations of users of websites in terms of data collection and the purposes behind this phenomenon. The author discussed the idea that once users provide their data, they will have expectations of the uses of their data by the business, for the intended purposes specified prior to collection. In the event that the business organization uses this data to collect further data, or for a different purpose than what is expected by the user, then this could be a cause for concern for the user's privacy. This idea draws inspiration from the social contract theory (Dunfee, Smith, & Ross Jr, 1999), since the user's agreement with the organization to provide data to the business can be seen as an implied social contract (Culnan, 1995; Milne, 1997; Pan & Zinkhan, 2006; Perreault, 2015).

In light of this, the organization that collects the data from the users immediately has a responsibility to safeguard that data and ensure that the users' privacy in turn is maintained, that they are safe from harms that could occur from privacy breaches and data leaks, and that their expectations are fulfilled in terms of data use and purpose. This idea proposes that user agreements are guided by social contracts based upon moral rationale between the organiza-

tion and the users, by which the e-commerce organization takes responsibility for the wellbeing of its stakeholders, in this case its users (Li, Sarathy, & Xu, 2010). As such, the authors further suggest that the social contract may be considered violated in the event that the e-commerce organization collects information that the user does not explicitly understand the purpose of, or is not completely aware of, as well as if the organization fails to provide the user with an option to opt out of the extra data collection that may be surplus to the basic information that they may have already provided.

2.4 Information disclosure

During transactions online between consumers and organizations, consumers may be asked to disclose information of varying nature, such as their demographic profile, credit card numbers, email addresses, financial information, medical records and other kinds of personal information. Consumers may be careful of the disclosure of identifying, sensitive and personal information, and is related to their willingness of disclosing such information. Studies have found that consumers possess higher concerns when it comes to disclosing sensitive information such as financial, health and medicine data, as well as social security information. Concerns regarding online information privacy surface for consumers when their personally identifiable information is collected without their consent or that their information is misused, and therefore, a consumer's online privacy concerns are reflected by the potential vulnerability of the personal information disclosed to an organization. (Gupta, Iyer, & Weisskirch, 2010)

In a study conducted by Olivero and Lunt (2004) examining information disclosure by consumers of e-commerce, it was noted that consumers don't disclose information as a way to establish intimacy as is done in interpersonal relationships, but that the benefits associated with information disclosure are evaluated in relation to the potential for increased information, improved services and financial reward. The interviewees of their study revealed that the willingness to disclose information increased when the perceived benefits could warrant costs such as time consumption and vulnerability risks. The study also revealed that if information on one hand can be disclosed due to financial reasons, on the other hand the trade of information strengthens the perception of risk, causing a need for protection that may garner a lack of trust. The participants of the study also claimed the need of being in control of the ownership of the personal data, as a way to avoid undesirable intrusions of privacy and also to safeguard their interests, and being treated as informed partners where their information is being traded as a commodity.

Another aspect related to information disclosure in an e-commerce setting is that of reputation (Olivero & Lunt, 2004). Whether customers decide to take part in electronic transactions is highly dependent on the brand image that the organization possesses. Regarding information disclosure this also seems to be the case, as the results of the study by Olivero and Lunt (2004), also indicate that there is a higher willingness to disclose information if the consumer believes that the organization is well known and has an image to preserve. Furthermore, another aspect of users providing personal information to online vendors is the users' context-related experiences. When personal information is given to a vendor, the user may feel that a psychological contract is formed, that works as an assurance that the vendor will handle their personal information with responsibility, and if the user feels as if their privacy has been in-

vaded, the user may feel that this contract has been violated as a result (Bansal, Zahedi, & Gefen, 2016).

In previous research, it has been stated that a prior positive experience with a certain website is connected to increased trust level towards that website (Bansal, Zahedi, & Gefen, 2016). Positive experiences and familiarity in a website increase behavioural intentions related to trust, while negative experiences with a website lower the trust. (Bansal, Zahedi, & Gefen, 2016) further argue that a previous positive experience with a website should decrease the inhibitions for consumers to provide personal information on the web.

2.5 Trustworthiness of e-commerce platforms

In order to identify the measures of ensuring individual privacy on e-commerce sites, it is important to understand the role of trust in online behaviours of consumers. Generally, various definitions of trust exist, which can be characterized by three primary elements: uncertainty, vulnerability, and dependence (Corbitt, Thanasankit, & Yi, 2003). Trust can be reflected in different perspectives such as psychology, sociology as well as buyer-seller relationships. According to Mukherjee and Nath (2007), there are five main antecedents to trust: shared values, communication, opportunistic behaviour, privacy and security. For this research, the focus is on the buyer-seller relationship through consumer trust in e-commerce websites. Trust does not only bring about the guarantee of business brand benefits, but also determines the amount of consumers, since customers may seek the safety offered by transacting with recognizable brands that are considered safe (Rust, Zeithaml, & Lemon, 2004). The knowledge of online retailers' reputation and recognizability could as such determine the degree of trust by customers. For example, under the condition of uncertainty, the popular online retailers are easier to gain trust. The brands that are trusted by customers would provide a perception of safety in terms of engaging in online activities. Also, buying from a popular brand could contribute to the customer's social needs in terms of acceptance from peers who shop from the same retailers (Rust, Zeithaml, & Lemon, 2004).

Trust issues are critical to both interpersonal and commercial relationships (McKnight, Choudhury, & Kacmar, 2002). Belanger, Hiller, and Smith (2002) highlighted two concerns of consumer trust in online purchasing behaviours: the lack of commonly accepted definition of online consumer trust and the lack of empirical attention to perceived trustworthiness. Previous research has defined trust as a willingness to believe on various attributes of the other parties, such as fairness, goodness, strength, and ability (McKnight, Choudhury, & Kacmar, 2002). Consumers make purchasing decisions based on their level of trust in the online retailers, and customers with different levels of trust use various performance measures such as speed, reliability, availability, navigability, order fulfillment, and customization (Mukherjee & Nath, 2007). Parallel to this, online purchasing behaviours do not only consider the relationship between the online retailer and the consumer, but also the relationship between the consumer and the computer system (Belanger, Hiller, & Smith, 2002).

Based on the above insights, it can be argued that trustworthiness has become a major consideration that needs to be addressed. For this reason, several strategies have been applied by online marketers to make effect on perceptions of trustworthiness such as the TRUSTe symbol and the CPA webtrust (Belanger, Hiller, & Smith, 2002). These strategies would apply to different situations depending on the industry characteristics and product features. It's neces-

sary to balance the relationships between trustworthiness, privacy, security, and purchase intentions (Belanger, Hiller, & Smith, 2002). According to Büttner and Göritz (2008), trustworthiness promotes both intention to buy and financial risk taking, and as such, trustworthiness mediates the influence of perceived risk on intention to buy. The consumers, as the initiators of the shopping activities, make their decisions after evaluating the need for the purchase, integrating previous experiences, the credibility of the retailers as well as the recognition of the retailer (Li & Zhang, 2002).

It can be considered then that trust-related behaviors in e-commerce include sharing personal information, making a purchase, and acting on information provided by a website (McKnight, Choudhury, & Kacmar, 2002). Webb and Sheeran (2006) discuss a correlation between behavioral intentions and actual behaviour. Trusting intentions of consumers would mean that the consumer is securely willing to depend on the online retailers. Trustworthiness, as a subjective probability of depending, would take into account the probability that consumer would share information with the other parties. According to McKnight, Choudhury, and Kacmar (2002), consumer subjective probability of depending involves the projected intention to engage in three specific risky behaviors: provide the vendor personal information, engage in a purchase transaction, and act on vendor information.

2.6 Measures to protect data in literature

2.6.1 Improving password security

The protection of personal data at its core requires a good authorization mechanism that ensures that only authorized users can access the information, and a common method for ensuring this in electronic data contexts involves authenticating users with the use of username–password combinations (Vu et al., 2007). Sometimes, users may create passwords that are easy to remember (Gaw & Felten, 2006). This in turn means that these passwords are easy to crack by malicious individuals, through password guessing or the use of computer programs (Bishop & Klein, 1995). Research has shown that passwords that are easy to remember always contain some biographical information such as birth date, names, and their favorite items (Vu et al., 2007). These simple characters are easy to gain via the aforementioned users' social media profiles or through simple searches on search engines that could bring up results from tax or civil registries. For instance, Leyden (2003) found that three most common types of passwords would include a user's own name, favorite football team, and date of birth. If the person who attempts to gain access to information knows much about the target user's life details, this greatly increases the risk of personal data being stolen via the compromised password. Proactive password checking could be helpful in order to improve the security of user-generated passwords (Proctor et al., 2002).

Another problem with password based authentication for accounts that could be of concern in terms of privacy breaches is that users tend to use the same password for multiple accounts (Ives, Walsh, & Schneider, 2004). If the password for one account is compromised, then the security of all the other accounts may also be at risk. In the context of e-commerce for this study, consumers conduct various online transactions over the e-commerce website which involves their personal information, including online payment activities, personal details and addresses, as well as transaction histories. These details could be accessed by anybody who

may be unauthorized but have access to the user account of the target user on the e-commerce platform, by way of a compromised password. For the two issues discussed above, first of all, consumers on e-commerce site need to adjust their password generation strategy in order to improve password strength (Russharvey Consulting, 2017). It is necessary to minimize the use of passwords created using aspects of their own biographical information, and instead use combinations of uppercase and lowercase letters, numbers and special characters in order to form stronger passwords (Vu et al., 2007). In addition, it is recommended that consumers should create separate password for each account in order to minimize the risk of compromising several accounts in case one of them is hacked into (Vu et al., 2007).

2.6.2 EU data privacy legislation

The data protection laws in the EU are based upon the EU Data Protection Directive adopted in 1995 which served to set a security standard for the processing, transmission and storage of personal data within the European Union (Electronic Privacy Information Center, 2017). The new revised regulation, the General Data Protection Regulation (GDPR) is set to be implemented in May 2018 and improves upon the previously set directive by introducing stricter accountability obligations, stronger rights and restrictions on flows of data internationally (Ashford, 2016). One of the key issues tackled by the regulation is consent to collection and use of data. Under the new regulation, sensitive personal data can only be gathered with full explicit permission, for a legitimate purpose (Allen & Overy, 2017). In addition to this, in the event that data is processed with the intent of direct marketing, the user will have the right to object and this right must be explicitly brought to their attention (Allen & Overy, 2017). In the scope of our study, this would mean that e-commerce organizations that use targeted advertisements would have to explicitly inform their customers about their rights to object to this form of unsolicited marketing communication.

Furthermore, persons or organizations that collect and manage personal information must protect it from misuse and must respect the rights of the data owners which are guaranteed by the regulation (European Commission, 2017). The regulation also provides users with the right to withdraw consent to the collection and processing of their data just as easily as they can give it, without suffering any negative consequences as a result (Allen & Overy, 2017). In addition to this, the regulation provides users with the rights to access the data that has been collected from them, and restrict the use of the data for certain processing if they see fit (Allen & Overy, 2017). It is also interesting to note that the regulation allows for the right of erasure, or the right to be forgotten, which means that the users can request that their data be erased from the collecting organization if they wish (Allen & Overy, 2017).

3 Theoretical model – CPM Theory

This chapter explores the concepts and elements of the theoretical model upon which we are basing our research, and how the concepts of the theory can be applied to our research and facilitate a deeper understanding of our empirical findings.

Communication Privacy Management (CPM) is a theory that deals with the tension between privacy and disclosure, by examining why and how individuals decide to disclose or withhold their private information across different relational contexts (Metzger, 2007; Petronio, 2004). ‘‘In this theory, privacy is defined as the feeling that one has the right to own private information, either personally or collectively; consequently, boundaries mark ownership lines for individuals’’ (Petronio, 2002, p. 6). Metzger (2007) elaborates on this further, discussing that CPM is a theory based on rules, and suggests that people form rules in order to make better decisions regarding the process of revealing or concealing private information, and thereby trying to protect their privacy in the most efficient way. The rules are developed as a way to help individuals maximize the benefits, while at the same time trying to minimize the risks following information disclosure. These rules can be stabilized over time through continued use, but are also situational and can thus be changed to better fit new or evolving conditions and situations (Metzger, 2007).

CPM also stipulates that there are three different processes of boundary management (Metzger, 2007). The first one, “boundary rule information” states that people form rules to regulate at what times and at what circumstances information is to be revealed rather than to be withheld. Secondly, “boundary coordination” deals with the process of mediating privacy rules between different partners, for example if information that has been disclosed is allowed to be revealed to others, outside the relationship in question. Part of this process is also to define rules to control boundary linkages, boundary ownership rights and boundary permeability. The third process, “boundary turbulence”, is the result from differences in privacy rules used by people, deficient boundary coordination or privacy rule violations (Metzger, 2007).

3.1 The privacy boundary structure

The privacy boundary structure, as the theoretical basis of CPM theory, defines the elements of information presentation, and as displayed in Figure 3.1, there are three main elements that form the the system of CPM theory: privacy ownership, privacy control and privacy turbulence (Petronio, 2013). Petronio (2013) further discusses that these three elements are interrelated, explaining the understanding of privacy issues, the behaviours, decisions as well as changes that are important in managing private information.

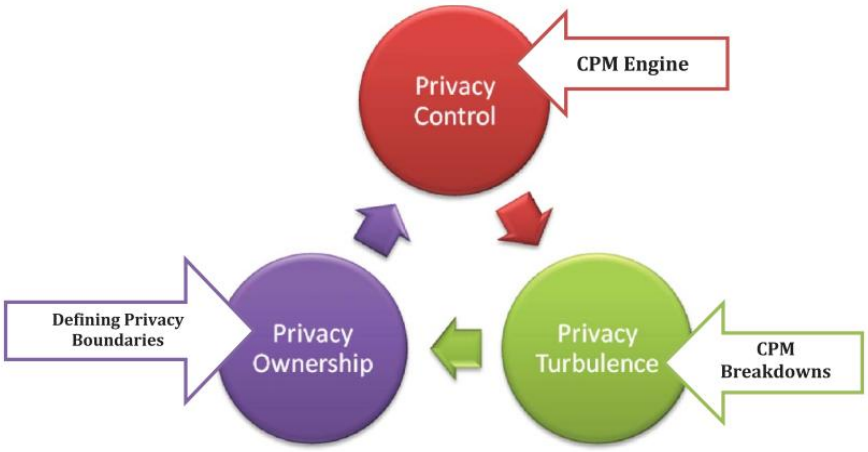

Figure 3.1: Communication Privacy Management Elements (Petronio, 2013)

3.1.1 Privacy ownership

Petronio (2013) elaborates that CPM theory could be used to predict how people consider privacy ownership. People want to integrate their ownership issues as well as rights of sharing privacy information. The research also indicates that privacy ownership can be restricted or shared with others, and Petronio (2013) further explains how granting access to information authorizes the parties that are granted this access to co-ownership of the data. These parties then become perceived by the original owner to be responsible for the data in the same way as the original owner would be. Because co-ownership plays a critical role in maintaining the original owner's private information, there is increasing attention paid to the recipient serving in a co-ownership role (Petronio & Reierson, 2009). Petronio (2013) further elaborates that there can be multiple co-owners, and the length of ownership obligations may last a long or short period of time in the context of privacy ownership. As disclosers share information with new recipients, they in turn become co-owners, or shareholders, of the aforementioned data. (Petronio, 2004). This can be applied in e-commerce contexts, as users share their data with retailers, allowing them to become co-owners of the data and therefore expected to exercise the same level of responsibility as they would if they were the original owners of the user data.

3.1.2 Privacy control

Privacy control is the second element in the boundary structure, as people believe they have the right to the privacy of their information, and as such feel that they should exercise control over it. As such, Petronio (2013) discusses that individuals choose to control the flow of private information through the development and use of privacy rules. These rules could be influenced by factors such as previous experiences, cultural values, and situational needs. The privacy rules for third party disclosures are negotiated between the original owners and co-owners of the data each time the data is shared (Petronio, 2004).

3.1.3 Privacy turbulence

Privacy turbulence refers to situations that arise from a lack of coordination between the parties privy to information as per the privacy boundary structure, for example situations whereby there are violations of privacy rules, privacy dilemmas, and unclear boundaries to privacy of data (Petronio, 2004). The issue with CPM theory is that in the real world, sometimes individuals or organizations may not strictly follow the privacy rules set in place, due to various factors. This leads to a lack of coordination as the shareholders of information fail to understand or implement the privacy rules as intended by the original owner of the information. As Petronio (2013) discusses, privacy regulation can be unpredictable in nature and leads to turbulence, which may take the form of disruptions in the management systems of privacy or in some cases total breakdowns in the privacy boundary structure. These kinds of issues cause problems not just for the original owner of the data, but also for the authorized co-owners who have been entrusted with the privacy of the data by the original owner.

Privacy turbulence could be caused by errors or mistakes, or on purpose by individuals or entities with malicious intent that cause a violation of privacy (Petronio, 2004). For example, an intentional breach of data privacy may be caused by a disgruntled employee looking for payback against an organization that collects or stores data, or by a simple mistake by another employee who works in the organization that collects or stores the data. Frampton and Child (2013) discuss the issue of privacy turbulence and the role it plays in formulating measures to accommodate the risk of turbulence. Metzger (2007) also explores the issue of privacy turbulence and the role that past experiences with turbulence in privacy could play in information disclosure. Metzger (2007) further proposes that experiences with privacy turbulence could play a greater role in future disclosure decisions.

3.2 Application of CPM theory for user rules in e-commerce contexts

As discussed previously, CPM is a rule based theory that focuses on the disclosure or concealing of private information. Petronio (2013) discusses how CPM has been applied to family communication contexts, relationship contexts, and health and social media behavior. However, we are more interested in Metzger (2007) and the focus on CPM from consumer perspectives in e-commerce contexts. According to Petronio (2004), people move from personal privacy boundary to a collective privacy boundary by disclosing information to others, which in our study would be highlighted by consumers sharing their information to e-commerce sites within a collective boundary. The author further describes the importance of privacy rules in order to control the data flowing in and out of the established boundary, in order to mitigate and counter the effects of privacy turbulence.

Since privacy turbulence occurs in situations where privacy rules are violated, unclear, or uncoordinated between the actors within the collective boundary (Petronio, 2004), it is necessary to incorporate privacy rules in order to be prepared for the chance of turbulence (Frampton & Child, 2013). In the case of this study, it can be considered that users of e-commerce need to establish privacy rules that they undertake in disclosure, as well as measures in order to protect their data within the collective privacy boundary encapsulated within information disclosure and collection by e-commerce sites. Privacy turbulence on e-commerce sites could be caused through the misuse of data that has already been given up, such as usage data through

cookies, and contact information, establishing the need to expand the scope of CPM theory to cover measures for avoiding privacy turbulence in addition to the rules on information disclosure from user perspectives.

Metzger (2007) applied the CPM theory to e-commerce contexts, and explored the factors that would contribute to the behavior of users in terms of disclosure. The following arguments are based on the same work, as Metzger discussed the motivation behind seeking how the user data will be used, with users utilizing privacy policies in order to get an understanding of what will be done with their data and therefore evaluating the risks against the benefits to them. In addition, the author also discussed experiences as a factor in information disclosure in e-commerce contexts, finding that the level of deception was greater in users with more e-commerce experience, meaning that they may have experienced some boundary turbulence in the past to make this happen. Metzger's conclusive remarks suggested that consumers regulate access to their data by erecting boundaries around them dependant on the perceived risk of sharing information that may be considered sensitive, and as consumers make these decisions about whether or not to conceal or reveal information, they end up forming rules and taking measures in order to apply to their dealings with e-commerce organizations. This study seeks to dive into and explore these particular measures in more detail, and analyze the rules that users of online shopping platforms put into place in order to mitigate the threat posed by sharing their data and minimize potential privacy breaches on e-commerce platforms.

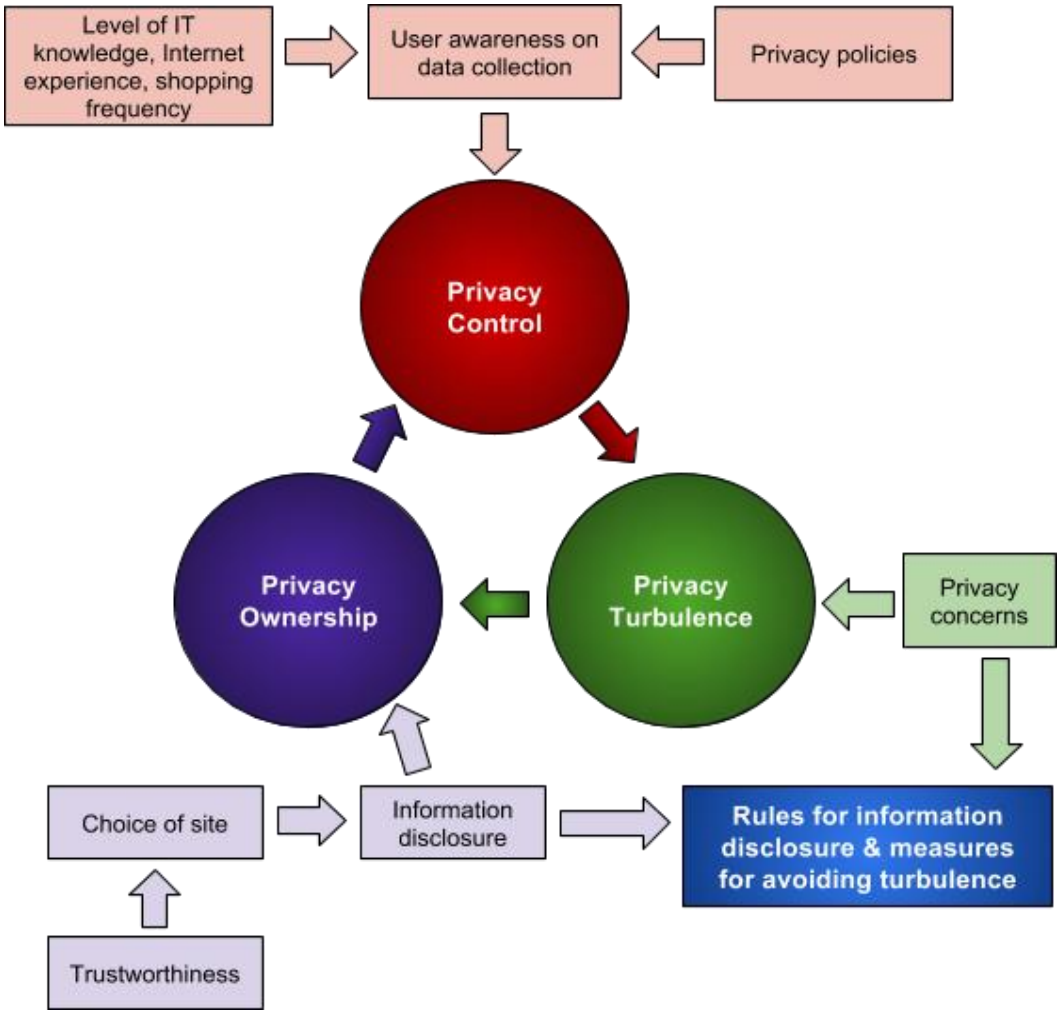

Figure 3.2: Adapting Communication Privacy Management Elements (Petronio, 2013) for our study

The adapted model (Figure 3.2) of the Communication Privacy Management Elements model introduced by Petronio (2013) seeks to expound on the elements involved in CPM, and apply these to the context of users of e-commerce platforms. In the adapted model, it is key to investigate the user awareness on data collection through various methods in the e-commerce contexts, their views on the usage of data, and how this affects user perception of privacy control as explored in CPM. In order to explore user awareness, the study looks at the role played by privacy policies in order to establish whether users make use of the information afforded to them about data collection, and also define the role of previous experiences and knowledge about data collection. User awareness in this study seeks to incorporate the level of knowledge about IT in general, awareness about legal protection of user data, as well as the level of investment in terms of time and money made on e-commerce platforms by the user.

In terms of privacy ownership, this study explores user perspectives on information disclosure, that allow them to share their information with e-commerce sites and accept the sites as co-owners of their data, allowing them into the privacy boundary for that particular data. In order to understand this it is important to understand the drivers that contribute to selection of shopping sites, and establish the role of trustworthiness in disclosure of information that contributes to privacy ownership, as well as find out what website features build trust from user perspectives. The study therefore examines the limits to what information users are willing to share with the e-commerce sites so as to allow them into the privacy boundary and share ownership of user data. As for privacy turbulence, the study seeks to explore the actual privacy concerns may that occur on e-commerce sites from user perspectives, and as such seek out the measures that users employ to minimize the potential breaches of privacy. The combination of these measures to combat privacy concerns, as well as the rules put in place by users for their initial information disclosure defines the specific area of our investigation in the adapted CPM model.

4 Research methodology

This chapter details the description of how this study was carried out, and the steps taken in order to conduct the research. We also motivate the choices made in terms of research methods and discuss the efforts taken to ensure validity and reliability of our findings.

4.1 Research strategy

Our research focus was to attempt to identify the rules that users employ in order to protect their data on e-commerce sites, in line with the CPM theory that proposes that users impose rules in order to coordinate data boundaries and avoid turbulence in privacy. The first step for us in this research was to take into account the existing literature concerning privacy issues on the internet, and this literature was found using available resources such as Google Scholar, the Lund University library, and relevant IS libraries such as the AIS Electronic Library. We narrowed down our searches for relevant literature on these platforms by making use of relevant keywords, such as "privacy concerns", "information disclosure", "user awareness" and more of the same. This thorough search for existing academic work is important as it helped us to acquire in depth knowledge about this particular subject domain, suitable theories and frameworks that have been employed and developed and also an understanding of previous research methods that have been employed by previous researchers in the field (Recker, 2013; Webster & Watson, 2002).

It was important next to take into account the privacy policies and user agreement terms that are stated on e-commerce platforms. These policies were studied in order to identify what they state as the data that is being collected from the users, identify the potential privacy threats involved with each of them, and through the empirical findings identify the rules that users employ in order to ensure their safety from the harms posed by the possible privacy concerns. In addition to this, the nature of our thesis work demanded that empirical data must be obtained from users of e-commerce websites in order to determine their opinions on the privacy concerns that exist on the shopping platforms, and to find out the rules that they have in place in order to protect themselves and their data from the harms that are prevalent in case of privacy breaches.

4.2 Methods of data collection

4.2.1 Qualitative research method

For the empirical data collection in the study, we decided to employ a qualitative research method for collecting empirical data, which will be done by conducting interviews with users of online shopping. The motivation for applying qualitative research was that we could use

interviews, which have the advantages of being targeted, meaning that focus can be directed at the topic of the research and that they can garner causal inferences from our respondents as they perceive them, thus giving us insightful answers to our questions as a step in trying to answer our research question (Recker, 2013). These characteristics of interviews correspond well with the nature and scope of our research question, as we are identifying the rules and measures that consumers of e-commerce take in order to protect their privacy.

As we are researching what measures and rules users of e-commerce sites employ in order to protect their privacy, a qualitative study is more relevant, since as mentioned before, interviews would give us insightful answers that are needed in order to be able to answer our research question. Therefore, taking a quantitative approach would not be as suitable for us in relation to our research question, as it would be difficult to fully extract the sentiments of the respondents using a quantitative method (Smith, 1983). Using semi-structured interviews also gives us the opportunity to ask follow-up questions whenever we see fit, which would be hard to execute using an online questionnaire for instance.

Another motivation for not using quantitative research for our study is that we are not interested in measuring the state of certain variables, which quantitative research focuses heavily on, since it has a strong emphasis on numerical data (Recker, 2013). Granted, we do have some questions that are of a measurement nature in our interview guide, but it is not the main focus of our research. Furthermore, questionnaire-based surveys may cause a problem in the event that respondents may need further clarifications regarding the questions, and therefore cannot contribute relevant data (Bhattacherjee, 2012). If the respondents have difficulties in understanding a certain question in interview based qualitative research, we as researchers can step in and explain the question for the respondent, something that could not be done to the same extent when using survey questionnaires. In addition, Bhattacherjee (2012) discusses low response rates as one of the challenges of survey based quantitative research, which was an issue that we may have faced in the event that we had chosen to use a quantitative research method for this study.

This empirical data was as mentioned obtained through interviews, providing us with qualitative data from users of e-commerce sites detailing their experiences and expectations in regards to the privacy of their data online. It is of utmost importance to take into account that the qualitative data obtained from interviews is open to interpretation, and the findings from this sort of data will be open to our analysis and understanding in order to make sense of the data from the interviewee transcripts. Interpretive research becomes key for us to be able to build a deeper understanding of the phenomena that we are studying (Gummesson, 2003), allowing us to gain insightful perspectives from real world events and experiences from users of e-commerce sites. It is key as well to understand that interpretive research may be subjective in nature (Recker, 2013), meaning that we as researchers must take into account the social and historical context in order to better understand our findings.

4.2.2 Analysis of privacy policies to identify potential data privacy issues

As part of our research strategy, and in order to identify potential issues that could jeopardize the privacy and personal information of consumers of e-commerce, we analyzed the privacy policies of 15 e-commerce sites. Before deciding which sites in particular to analyze, we decided that we wanted to analyze well visited sites, and thereafter did some online research with the goal of finding the most used e-commerce sites. The result of this research can be

seen in Table 4.1, where each site is listed along with a description of the sites' core business. The idea of analyzing the privacy policy of each website was to find any clauses that may invoke privacy concerns for the users of e-commerce, and that may be prevented by the consumers applying protection measures.

Table 4.1: Selection of e-commerce sites

Name of retailer	Privacy policy link	Core business
Adidas	https://www.jdsports.se/customer-service/privacy/	Sportswear and accessories
Aliexpress	http://rule.alibaba.com/rule/detail/2034.htm	Retailer market place
Amazon	https://www.amazon.de/gp/help/customer/display?nodeId=3312401	Retailer market place
Apple	https://www.apple.com/legal/privacy/en-ww/	Electronics, accessories, software, online services
Asos	http://www.asos.com/privacy-policy/	Clothing/Fashion
Biltema	http://www.biltema.se/sv/Kundservice/Kakor/	Tools, car supplies, leisure products
CDON	http://cdon.eu/customer_service/security_policy/	Home electronics, video games, books, clothing
Elgiganten	https://www.elgiganten.se/cms/integritetspolicy/integritetskyddspolicy-for-elgiganten-ab/	Home electronics
HM	https://www.hm.com/se/customer-service/legal-and-privacy/privacy-policy	Clothing/Fashion
IKEA	http://www.ikea.com/ms/sv_SE/privacy_policy/privacy_policy.html	Furniture, home accessories
Nelly	https://nelly.com/se/privacy-policy/	Clothing/Fashion
Netonnet	https://www.netonnet.se/Content/CustomerInformation/PersonalInformation	Home electronics
Nike	http://www.nike.com/us/en_us/c/help/privacy-policy	Sportswear and accessories
Norwegian	https://www.norwegian.com/en/booking/booking-information/legal/privacy-policy/	Airline
Telia	https://www.telia.se/privat/om/integritetspolicy	Telecommunication and related products

The findings from the analysis would then be used as a basis for the interview questions, along with the findings from the literature study. The most common issues that we found re-

late to the use of cookies, information sharing and unsolicited communication of information. We quickly realized that many of the privacy policies dealt with the same recurring themes, but there were however important potential issues that were only found on a particular site, and that were not found on the other sites. The result of our analysis can be found in Table 4.2, where we divided the different themes into categories of concerns, and listed what kind of information that is gathered from the consumer related to that concern. Apart from this, we also stated the potential outcome of each privacy concern, in case of a breach of privacy for that particular concern.

Table 4.2: Potential privacy concerns and outcomes from privacy policy analysis

POTENTIAL CONCERN CATEGORY	PRIVATE INFORMATION COLLECTED	POTENTIAL OUTCOME OF PRIVACY CONCERN
Cookies	User identification data	Unauthorized access to data, Information disclosure, May invoke feelings of being monitored
	Usage logs	
	Tracking of user movements on the site	
	Browsing habits (how often they are on the site, what they look at, what they purchase)	
	Traffic data and positioning data	
	Interests in product	
Information sharing with collaborators/third parties	User identification data	Unauthorized distribution of data, Unauthorized access to data
	Browsing habits (how often they are on the site, what they look at, what they purchase)	
	Name, mailing address, phone number, email address, contact preferences, and credit card information.	
	IP address	
	Information from social media account, if account is linked to the e-commerce store	
Trustworthiness	Name, mailing address, phone number, email address, contact preferences, and credit card information.	Sense of insecurity when giving out personal data
Unsolicited communication	Email addresses, phone numbers, postal address	Unauthorized use of data

Due to the fact that fifteen e-commerce sites' privacy policies were analyzed, and that the privacy policies across these different sites were relatively similar in most cases, it can be argued that the analysis has captured the main themes of most e-commerce sites' privacy policies.

4.3 Data collection techniques

In order to carry out our empirical investigation we made use of interviews to carry out the qualitative research. Interviews are a common data collection procedure in qualitative research, and enabled us to collect personal comments and opinions aimed at contributing to answering our research question directly from the respondents (Bhattacherjee, 2012). We opted for a semi structured approach with our interview format, and the reason behind this was that it would allow us more flexibility through the conversational form of communication involved in semi structured interview procedures (Recker, 2013). This then gave us the opportunity to ask follow-up questions in case we had to obtain further insights. Answering questions related to privacy may be regarded as sensitive for some respondents, and when being interviewed in a personal and conversational manner rather than a more structured way respondents may find it easier to discuss sensitive issues (Recker, 2013), which is another reason we opted for a semi-structured method of interviewing.

4.3.1 Formulating the interview questions

In order to come up with a good interview guide and gain further insights on how to formulate proper interview questions, we read relevant literature on interview design. According to Bhattacherjee (2012), the design of the interview is a process of continuous modification. Using the themes obtained from CPM theory, combined with knowledge from the provided literature review, the first draft of the interview questions was formulated.

In order to ensure that each interview question was appropriate for the study and to establish whether there was a need for any potential changes to the interview questions, we decided to conduct a pilot study. This was done to test our interview questions and assess which ones would fit our purpose, and to find out if there were any problems or unclear questions. Pilot studies have the advantage of giving advanced warnings about where research could fail, and whether proposed instruments are appropriate or over complicated, and identify potential practical issues in the research process (Van Teijlingen & Hundley, 2002). The major purpose of the pilot study as such was to get a general opinion of the interview in relation to the actual research question we have through testing the validity of the interview questions.

Bhattacherjee (2012) discusses how pilot testing allows researchers the possibility to detect potential problems within the research design. The findings from our pilot study mainly showed us that we had to modify some of the questions in order to make them easier to understand. We also had to re-evaluate the categories of the questions in the interview in order to make them consistent with the findings from our investigative reading through of the privacy policies on e-commerce websites as outlined in Section 4.2.2. The initial interview questions were a bit difficult to understand for the pilot interviewees who first came into contact with our study. Based on the first pilot study (see Table 4.3), we decided to reflect the information from existing privacy policies and come up with some questions around that. For instance, we

would investigate the opinions on formats of privacy policies such as layout and language. After completing the second pilot interview, the five categories of our interview questions were decided: general information, factors that influence online shopping choice and information disclosure, privacy policies, the use of cookies and tracking, thoughts about giving up information, privacy concerns and controls. A summary of the resulting changes from our two pilot interviews is displayed in Table 4.3 below.

Table 4.3: Summary of pilot study results

Name	Gender	Age	Interview time	IT knowledge	Resulting change
A	Male	24	16 min	Intermediate	Integrate the information from privacy policies in e-commerce sites
B	Male	25	14 min	Intermediate	Categorize the interview questions

After the modifications to the interview guide, we had a total of fourteen questions. As stated previously, we carried out semi-structured interviews in order to gain a deeper first hand understanding of rules on information disclosure, online data privacy issues and the measures used to counter them. The interview questions and the related motivations behind each question are summarized in Table 4.4 as follows.

Table 4.4: Justification of interview questions

Questions	Motivation
1. What is the main driver for you when deciding what website to use when shopping online? (Price, recognition of retailer, delivery time, trustworthiness, convenience, security etc.)	Choice of sites
2. Do you do any type of research about an e-commerce site when using it for the first time? (Read reviews, find out from friends' experiences).	Choice of sites
3. Do you normally read through the privacy policies of the e-commerce websites that you have used? Why/ why not?	User awareness/Privacy concerns
4. Are you satisfied with the existing formats (language, clarity) of privacy policies on the e-commerce websites you use? please give some reasons for your answer	User awareness /Trustworthiness
5. Do you know what the purpose of cookies on e-commerce websites is?	User awareness
6. What is your opinion on cookies, are they beneficial or a nuisance? How do you deal with them?	Privacy concerns
7. Are you willing to provide personal information to web sites so that online advertisements can be targeted to your tastes and interests? Why?	Privacy concerns/Privacy boundary
8. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?	Information disclosure
9. If you do provide personal information to web sites, do you sometimes provide false/different information? (use separate email, bank card, nickname for online shopping use)	Information disclosure
10. How do you protect your information when making online payments with credit cards? Have you used an alternative payment method online that you might prefer?	Information disclosure/Privacy concerns
11. Do you log in to an e-commerce site using your social media account (Facebook/Google+)? What are the reasons for your answer?	Information disclosure
12. Do you actively check for "secure labels" or website security features (eg https) when visiting e-commerce sites? If so, why?	Privacy concerns /Trustworthiness
13. Do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?	User awareness
14. Are there any other measures that you take to keep your information safe when using e-commerce websites?	Privacy concerns/Other measures

4.3.2 Selection of informants

Since this study focused on collecting insights from a user perspective, anyone with online shopping experiences could be selected as a respondent for the interview. The target respondents didn't necessarily need a particular set of professional skills or experience, as long as they had participated in online shopping beforehand. This was because the interview questions were designed to gain insights on data issues regarding the most common online shopping scenarios and elements, such as browsing products and online payments. As such, there was no need to look for respondents with a special set of characteristics, skills or technical experience in order to take part in this study. In order to find participants for our interview, we started contacting the people in our social networks and in our immediate academic and domestic environment, and asked them about their online shopping activities in order to gain an understanding of whether we can obtain respondents from our immediate environments.

A total of 20 respondents who have had online shopping experience, and are currently living in Sweden, Kenya or China agreed to participate in our interviews. We considered that having these respondents from different geographical locations and backgrounds, and not focusing on a particular professional or technical group, could unearth more about unique online shopping experiences, thereby helping to ensure the reliability of our data by obtaining different perspectives. Table 4.5 below shows the profiles of the respondents, including their age group, gender, interview duration and type of interview. Our respondents were aged between 20 and 61, which tried to guarantee the reliability of this research by obtaining empirical information from respondents across these age groups. The interviews were all recorded, and the respondents were informed of this at the beginning of the interview as well. The interview recording was done in order to allow the interviewer and interviewee to engage in extensive dialogue without the interviewer having to worry about written documentation of the interviewee's responses. This ensured that nothing was missed and all the responses were properly recorded, allowing us to transcribe the interviews properly after the interview. Table 4.5 below presents the respondent profiles and characteristics of the interviews.

Table 4.5: Respondent profiles and interview characteristics

Respondent	Gender	Age group	Interview Time	Interview type
RA	Female	26-35	15 min	Face-to-face
RB	Male	18-25	28 min	Face-to-face
RC	Male	18-25	16 min	Face-to-face
RD	Female	18-25	14 min	Face-to-face
RE	Male	26-35	20 min	Face-to-face
RF	Female	18-25	17 min	Face-to-face
RG	Male	18-25	14 min	Skype
RH	Male	26-35	13 min	Skype
RI	Female	26-35	14 min	Skype
RJ	Male	18-25	17 min	Skype
RK	Male	18-25	16 min	Skype
RL	Male	26-35	15 min	Face-to-face
RM	Female	18-25	30 min	Face-to-face
RN	Female	18-25	15 min	Face-to-face
RO	Female	56-65	15 min	Face-to-face
RP	Female	18-25	13 min	Face-to-face
RQ	Male	56-65	14 min	Face-to-face
RR	Male	18-25	15 min	Face-to-face
RS	Male	18-25	14 min	Face-to-face
RT	Male	18-25	18 min	Face-to-face

4.3.3 Conducting the interviews

In order to ensure that the interviews were conducted in a peaceful environment, we mostly interviewed the respondents face-to-face in quiet locations, mainly within the premises of Lund University School of Economics and Management. Five of the conducted interviews were however done over Skype, as these respondents had difficulties meeting us in person.

Before each interview, we would ask the respondent's permission to record the interview. "Smart Record", which is a mobile app, was selected as the record tool for the face-to-face interviews, and "MP3 Skype Recorder" was used for the Skype interviews that were all conducted on PC's. After each interview, we would manually transcribe the recorded audio. All the interview transcriptions are available in the Appendix at the end of this document (see **Appendix II - XXI**). Before we started asking the actual interview questions, some general questions about the respondents were asked such as educational level, how much IT knowledge they considered themselves to have, how many online purchases they had made in the last three months, as well as asking how much money they had spent during those months. Then, we gave them a brief overview of our research area and interview questions. After this, we went into the interview itself. Some of the interview questions were asked with the opportunity for follow up questions, in order to follow the respondent's line of thought to gain deeper understanding about the phenomenon discussed in that particular section of the interview. After each interview, we thanked the participant for their time and contribution to our research.

4.4 Data analysis methods

The first step after conducting all the interviews was to transcribe the audio recordings into text formats. Kvale and Brinkmann (2009) discuss the transcribing process as being a process that involves the translating of oral language into a written format. We opted to have our transcripts take a more naturalized format that eliminates some of the features of oral speech, such as pauses, transition expressions such as "ums" and "ers", and adding relevant punctuation and paragraphing in order to make the transcripts easier to understand and read through (Bucholtz, 2000; Davidson, 2009). These transcripts of interview data provided us with a large amount of raw text data, from which we then needed to extract useful data out of in order to gain empirical insights to help us with our research. In order to do this, the transcriptions were then coded in order to find relevant data from the responses that make up the entire raw data.

4.4.1 Coding the data

Recker (2013) described coding as a method of reducing chunks of empirical data into meaningful information, which was key for us to do in order to make sense of the large amount of text data that we obtained as a result of our interviews and transcription process. Coding allows us as researchers to condense the large amount of text based data in order to understand the phenomena of interest and formulate a better comprehension of the empirical evidence (Basit, 2003). We needed to obtain data relevant to the investigation that we were carrying out, leading to the development of codes that were relevant to the categories of the interview questions. As such, the codes and their sub codes were also relevant to our research on priva-

cy concern awareness, and the user rules and measures to mitigate the effects of these concerns.

As our research is carried out with focus on the CPM theory, we created a table to show all codes and subcodes that we used in our coding process (see Table 4.6), and how they relate to CPM. The fully coded results of the empirical data from the interviews have been consolidated into one table, and can be found in the Appendix of this document (**Appendix I**). The coding was done manually as opposed to using software for the same purpose. The reason for this was that while it may be faster to code electronically and generate results (Basit, 2003), it also may take a long time to get acquainted with a software for coding (Miles, Huberman, & Saldana, 2013). Since none of us were very experienced with any software for coding, it was beneficial for us to do it manually rather than spend time acclimatizing to a new software which we may not even understand how to use to its maximum potential.

Table 4.6: Codes and their relationship to CPM

Main Code	Subcodes	Relation to CPM
1-Choice of site	1a-Drivers 1b-Research	Privacy Ownership
2-Privacy Policies	2a-Formats	Privacy Control
3-Cookies & Tracking	3a-Targeted ads	Privacy Control, Privacy Ownership
4-Information Disclosure	4a-Limits 4b-False / different information	Privacy Ownership
5-Payment info	5a-Card security protection 5b-Alternative payment methods	Privacy Turbulence, Privacy Ownership
6-Social Media Login	-	Privacy Ownership
7-Security Controls	7a-Security features 7b-Laws	Privacy Ownership, Privacy Control, Privacy Turbulence
8-Other measures	-	Privacy Control, Privacy Turbulence

4.4.2 Interpretive analysis of qualitative data

Since we are working with qualitative data collected from interviews, it is key to take note of the role of the hermeneutic process in the analysis phase of the empirical data collected for our research. Hermeneutics in information science research could be considered to be an interpretive method of analysis that seeks to examine the interpretation of meaning (Butler, 1998; Myers & Avison, 2002). It can be considered for this research that the findings from

interview transcriptions are open to us as researchers to interpret and extract meaning from in ways that are relevant for our needs in this study. This leads us to an interpretive method of analysis of data, whereby the responses we have collected from our interviews have been analyzed and coded as per our needs, and this is done in a way that involves the interpretation of interviewee responses by us as the researchers. Orlikowski and Baroudi (1991) emphasized the role of interpretive research in enabling researchers to derive constructs and relationships from their findings, through finding meaning in interview data and making sense of the raw data in the transcripts. This method of analysis of empirical data is important for us in this research considering that the data collected from the interviews focuses on the thoughts and opinions of our respondents, which means that in order to find useful data from the transcripts, we must interpret their responses and make sense of the data in the context of our data.

4.4.3 Triangulation of data

Triangulation of data refers to the perusing and relating of multiple sources of evidence regarding a particular phenomenon in order to obtain a more in depth picture of the situation (Recker, 2013). Triangulation in our research helps us to boost the validity and clarity of our findings. This was achieved through the comparison of our empirical findings from the coded interviews, and comparing them to the potential privacy concerns that we found on the privacy policies on the e-commerce sites that were analyzed as part of the study. This attempts to make our findings more reliable as well since they take into account multiple data sources, thus could be considered to be less biased and more robust, by allowing us to obtain a more complete, holistic and contextual portrayal of the study phenomenon (Jick, 1979). Shenton (2004) discusses the role of triangulation in providing more credibility in research practice, with the use of different data sources and multiple informants helping to provide diversity in the data used in research. As our arguments are strengthened by relating empirical evidence to the data found from actual privacy policies, we argue that our research may be considered more credible due to undertaking the triangulation of data in the study.

4.5 Research quality and ethics

One of the key things that we must take into account in order to maintain a partial view of the research findings and avoid bias is to be objective with our research. (Recker, 2013) identifies four principles that ensure a maximum amount of objectivity in research, namely replicability, independence, precision and falsification. We seek to enhance objectivity in our research by undertaking the study in a way that is free from bias, and careful precision and adherence to the research procedure in order to ensure that our research can be replicated by a future study that may wish to do so.

It is important for us as well to take into account the principle of contextualization in research in order to ensure that our findings are valid and of proper quality. Knowledge about the reality of a situation within a subject domain and topic area through interpretive research is formulated through understanding social constructs (Klein & Myers, 1999), which must be taken into account in order to gain proper perspectives regarding our empirical findings. It is important to understand the social and historical context of the actors involved in the data collection process, in order to obtain a clearer picture of the real world situation (Bhattacherjee,

2012). In order to achieve contextual accuracy in our research, we chose to analyze the user policies from a variety of e-commerce websites with a range of core businesses in order to grasp whether or not there are stark differences or similarities between the policies, and identify the common aspects, which in turn led us to the common data privacy issues faced by users of the websites. In addition, contextualization helps us to understand the concern levels of users that may have experienced privacy security breaches and how they react to online threats due to data collection on e-commerce sites, as well as helping us to understand how the level of IT knowledge and internet experience impacts the users' rules and measures in terms of data collection and privacy on their internet shopping activities.

In terms of our interviews, it is key that we take into account the ethical power dynamics that may come into play. Brinkmann and Kvale (2005) discussed these dynamics in detail, describing the dangers of attempting to guide the interviews in a particular direction and forming biased responses as a result. We have attempted to mitigate this by using interview questions that are open and focus on the opinions of the respondents. These authors also discussed the importance of ensuring that the respondents are comfortable during the interview, and at the same time obtaining the maximum amount of information without making the respondent feel uncomfortable with the questions. The key to do this in our research is to ensure that the interviews are conducted in a respectful and professional manner, making sure that the environment for the interview is relaxed and open, so that the respondent is comfortable with talking to us and disclosing the relevant information for our research.

Bhattacherjee (2012) proposed that four key principles are essential guidelines for ethical interview research: voluntary participation and harmlessness, anonymity and confidentiality, analysis and reporting, and disclosure. We applied these principles for our research, by ensuring the anonymity of the respondents was preserved, and participation in the interviews is voluntary. The participants were not harmed in any way, physical or psychological. In terms of disclosure and reporting of findings, we have incorporated all of the data that we collected through our empirical research into our findings, without manipulating our collection, interpretation and analysis procedures in a way that would contradict the industry specific practices and principles of scientific research.

5 Empirical findings

*This chapter highlights the results of our qualitative research by examining the interviewee characteristics and explaining the responses from our interviews in the relevant subsections of our study. References are made to the coded results of the interviews **(Appendix I)** attached together at the end of the manuscript.*

5.1 Interviewee characteristics

We interviewed twenty respondents, and in order to protect the respondents' privacy, we named them RA to RT in this study. After finishing the summary, we created Table 5.1 as follows, which reflects the general information of each interviewee in terms of IT knowledge, number of hours spent daily on the internet, number of online purchases in the last three months, and their average approximate amount spent online per month in Swedish krona (SEK). It can be seen from this table that fourteen out of twenty interviewees have intermediate and high level of IT knowledge. The time spent online for personal browsing by our respondents ranged from one hour to twelve hours, with the average time being just over seven hours. It is interesting to note that in the case of RK, their daily online time for personal endeavors is only two to three hours but as they work in the IT field, RK spends majority of their day online for work related reasons as a result.

As stated in the methodology section, the basis of our selection of informants was that the respondents have accepted and utilized platforms of online shopping. Table 5.1 below shows the IT knowledge of the respondents, the amount of time they spend online per day, the average approximate number of online purchases they made in the last three months, and the approximate amount spent on online shopping per month. As can be seen in Table 5.1, there are three respondents that said they made no online purchases in the last three months. This is due to the fact that those three respondents are international students who are currently studying in Sweden, and therefore, for various reasons, they haven't engaged in online shopping in Sweden so far during their study period. In response to this situation, we asked them about their general online shopping habits as they were when living in their home countries. As we discovered, they did actually engage in online shopping in their home countries, and as this was the key prerequisite in order to contribute to our investigation, we could thus include them in our study and use their insights as part of our empirical data.

Table 5.1: Respondents' online habits

Respondent	IT knowledge	Hours spent online (per day)	Number of online purchases in last 3 months	Average approximate amount spent online per month (in SEK)
RA	Intermediate	8	2-3	1000

RB	Intermediate	6-7	-	817
RC	Intermediate	11	5-6	660-830
RD	Expert	10	10	660-1330
RE	Intermediate	10	-	1390-2780
RF	Basic to Interme-diate	2-3	10-15	1660
RG	Intermediate	4-5	2	1280
RH	Intermediate	7	3	260
RI	Intermediate	10	5	1300
RJ	Expert	10	12	1300
RK	Expert	2-3	5	830
RL	Basic	6-7	-	-
RM	Intermediate	6	6	610
RN	Intermediate	7-8	1	180
RO	Basic	1	2	330
RP	Intermediate	12	1	160
RQ	Intermediate	6	4	330
RR	Intermediate	8	1	430
RS	Intermediate	6	1	400
RT	Intermediate	8	6	1000

5.1.1 User awareness on data collection and security

In terms of awareness of data collection procedures and policies, it was noted that from all of our respondents who participated in the study, none of them actively sought to read the privacy policies on the e-commerce sites that they chose to use. Five out of twenty respondents expressed a lack of awareness in terms of data collection via the use of cookies to collect user data. When it comes to security features, seven out of twenty respondents displayed a lack of awareness of what these are and how they are used to ensure safe transfer of data when using the sites. Finally, twelve out of twenty respondents expressed a lack of awareness of the laws that are in place to govern data collection and usage, and protect users' rights in terms of legal procedures concerning data collection, usage and storage. A summary of the user awareness compiled from the categories in our empirical studies is displayed in Table 5.2 below.

Table 5.2: Respondents' awareness about data collection and related issues

Respondent	Actively reads privacy policy	Aware about data collection via cookies	Aware about site security features	Aware about laws governing data collection and use
RA	NO	YES	NO	YES
RB	NO	YES	NO	YES
RC	NO	YES	YES	YES
RD	NO	YES	YES	YES
RE	NO	YES	YES	NO
RF	NO	YES	YES	YES
RG	NO	NO	YES	YES
RH	NO	YES	YES	NO
RI	NO	YES	NO	NO
RJ	NO	YES	YES	YES
RK	NO	YES	YES	YES
RL	NO	NO	YES	NO
RM	NO	YES	YES	NO
RN	NO	YES	NO	NO
RO	NO	NO	NO	NO
RP	NO	NO	NO	NO
RQ	NO	YES	YES	NO
RR	NO	YES	YES	NO
RS	NO	NO	NO	NO
RT	NO	YES	YES	NO

5.2 Choice of site

To get an idea what motivates the respondents to choose a certain e-commerce site to perform online purchases, we asked each respondent what their main driver when deciding what e-commerce site to use is. This was asked in order to find out if respondents choose site based on privacy and security concerns, or if the product price is of higher importance. Related to the choice of site, we also asked the respondents if they did any research on the sites they potentially would use, and to find out the different methods of research employed by the respondents.

5.2.1 Drivers that influence site choices

The price of products was the most mentioned main driver for the respondents when deciding what site to shop from, since more than half of the respondents mentioned price as one of the most important factors when making decisions about what e-commerce site to use (1, 3, 7, 9, 12, 18-22, 24, 28).

The second most mentioned driver was the recognition of the retailer, as seven out of twenty respondents claimed that to be a main driver (1, 5, 7, 9, 11, 26, 30). The importance of the recognition of the retailer was further emphasized by RE, stating that the respondent in general does not use sites that aren't famous (9). RA stated that trustworthiness comes along with recognition of the retailer (1), and was another main driver noted by a total of 4 respondents (1, 14, 31, 32).

For three of the respondents, the delivery time the retailer has on its products was recognized as a main driver (18, 21, 28). Reputation of the retailer was noted by two respondents as a main driver (12, 18), which arguably can be seen as quite similar to "recognition of retailer", but it still causes for a distinction between the two. Security factors were identified as a main driver for two of the respondents (1, 12). RA specified that by security, the respondent means security in terms of privacy (1), meaning that only one of the respondents specifically mentioned privacy as a factor in their decision making process when deciding what retailer to make a purchase from. Simply clicking the ads that pop up on social media was enough of a main driver for one of the respondent (16).

5.2.2 Research done by interviewees before online shopping

The majority of the respondents performed some sort of research about e-commerce sites before contemplating to make a purchase from the site. The most dominant methods of research was to search for the site in question on Google (2, 13, 15, 19, 27), and reading online reviews and comments about the site (2, 4, 8, 10, 11, 15, 23, 29). This is explained by RA as "*[...] I usually Google it if I don't know about it and read what the other people wrote about it [...]*" (2). More extensive online research methods were also identified in the interviews, as RC would *"[...] hop on Reddit and see if people have used this, their opinions on it, and if that was good [...]"* (6), and looking at reviews on YouTube was used as a method by RD and explained as *"[...] look at reviews on YouTube, before I buy them, and buy them on the same website as they bought them."* (8).

The reasons for doing research about the sites however, had some variations as RO for instance would compare prices and other things (27), whereas RM would research whether the service is good, and looks for information about the delivery (23). Apart from turning to the Internet for research about e-commerce sites, doing research amongst friends if they have used the site and whether they would recommend it was mentioned by RE, RG and RP (10, 13, 29), with the slight distinction being that RE and RG specifically stated that they would ask friends about different sites (10, 13), whereas RP simply stated that they would often get recommendations from people they know, without necessarily having asked for the recommendation themselves (29).

5.3 Privacy policies

The main reason behind the questions regarding privacy policies was to find out whether users actively look through the policies on e-commerce sites and if the information available to them about how their data is collected and used plays a role in influencing their information disclosure. We also sought to find out whether the formats of the policies influenced the users' disclosure rules, and what they think could be changed in order to make the policies clearer and facilitate a better understanding from the user perspectives. From the results of our empirical investigation, it was found that none of our respondents actually actively read through privacy policies, claiming that for the most part it was a waste of time to read through and understand what the policies were talking about. RA argued that they were familiar with the contents of privacy policies, and that the policies in general contain the same kind of information across websites. They further implied that there was no point to read the privacy policy on each and every website they used, by saying that *"[...] I assume that everything looks the same. So if I have read one, yeah."* (34).

5.3.1 Formats of polices

Interview question number four was aimed at collecting the respondents' comments on the format of the existing privacy policies. It is clearly found that most of the respondents are not satisfied with the format of privacy policies. Two of the main reasons for this are that the respondents generally felt the content of privacy policies are too long (35, 36, 37, 40, 41, 42, 43, 46, 47, 55, 57, 58) and difficult to understand (34, 38, 42, 51, 56). A number of respondents said that the privacy policies were usually too long and detailed. They try to be specific, but they end up being vague to casual users. Additionally, there is a lot of jargon existing on the privacy policies, which increases the difficulty of reading for the respondents who were without good IT knowledge. 17 out of 20 respondents think reading these policies does not make much sense to them. RE was confident about the terms in privacy policies for trusted sites, stating that *"[...] I'm confident that they would have privacy policies there that wouldn't affect me pretty badly in any way [...]"* (39).

In addition, according to some of our respondents, reading through the privacy polices is a waste of time (39, 41, 47, 48). Some respondents just skim through the headings to see what they are talking about, and might skip doing this too if they are in a hurry to buy something. The findings show that the time consuming nature of privacy polices is due to the length of the content, as some of the respondents answered that they lost interest in reading when they saw the full text on the screen (41, 47). Moreover, when the respondents encounter uncom-

mon terms, they need to take time to study these terms, which potentially increases the burden of their reading. RR stated that *"I think reading these policies does not make much sense to me. And usually, there is a drop-down arrow in the privacy page, I guess the site doesn't really want us to read. Users can go directly to the bottom of the page and click "I agree"[...]."* (55).

Furthermore, based on the findings from our interviews, we found that some respondents would prefer a simpler format instead of existing format of privacy polices (38, 45, 50). Three respondents stated that if the privacy policies would have a summary, that would be helpful to them to understand the main terms that are stated in the policy (38, 41, 45). As RC and RN answered, they expected the sites could change the privacy agreement to like a short video, or infographic, in order to increase the relatability and interaction and make the policies easier to understand for casual users (36, 50).

5.4 Cookies and usage tracking

From the twenty respondents who participated in the interviews we conducted, it was interesting to note that five did not have awareness of cookies and their usage on e-commerce platforms. This is despite the fact that cookies are amongst the most widely used data collection methods on the internet today. A large proportion of respondents that were aware of cookies acknowledged and understood the business sense of having cookies present on websites (59, 61, 63, 86). RC emphasized further on this, talking about the mutual benefits for the user as well as the organization through provision of data for better service, stating that *"I really don't mind them [...] I think it's fine, we go into a mutual agreement, you provide me a service and in turn I give you something back."* (63). RB also elaborated on the usefulness of cookies for improving search quality in their experience on e-commerce platforms, *"What I expect them to do is just to improve my search quality [...]"* (61). A number of respondents also spoke about the convenience of having saved credentials (68, 77, 78) in order to increase the degree of convenience in login processes, searches and the general shopping experience.

However on the other hand, some respondents expressed concern about the risk of having saved credentials as a result of the presence of cookies, especially in the case of card information and payment details (65, 68). RE talked about the ease with which fraudulent payments can be made due to the saving of credit card information being stored on web pages, noting that while some of their friends did that, they themselves considered it to be a risky practice, stating that *"Sometimes you just need to type the CVV number, rest of the things are saved in the site already. So you just need to go to the portal, type the CVV number and pay. So that's quite scary, I would say [...]"* (68). Across the negative aspects of the presence of use of cookies on e-commerce websites, some of our respondents expressed dissatisfaction with the nature of how the cookies work, and felt like it was invasive and annoying (59, 82, 84). Furthermore, some of our respondents elaborated on their feelings about the purpose and usage of cookies, stating that this needs to be better defined, and transparency was key in use of cookies and online tracking (61, 63, 68). For example, RC spoke of how they didn't mind the presence and use of cookies, as long as this was clearly stated and they were informed about it, saying that *"I need to know that they're using cookies [...] I just need to be informed beforehand, and then I accept it and continue using."* (63). It was also interesting to note that some of our respondents expressed their concern on the lack of choice when it comes to use of cookies, feeling like they have their hands tied due to a lack of browsing options without

cookies (59, 65). Both RA and RD talked about this, stating that they would still want to use the e-commerce websites that they currently use, but would prefer an option to have reduced/no presence of cookies to track their behavior and store their data (59, 65).

5.4.1 Targeted advertisements

When it comes to personalized targeted advertisements, our empirical study found that some of our respondents actually liked the fact that the targeted ads were appearing to them, stating that this form of promotion makes life easier for them as online shoppers by giving them recommendations for products that they are actually interested in and may end up buying (62, 64, 67, 69, 88). RE spoke about how targeted ads are actually a key factor in their online shopping habits, discussing how they preferred to compare ads from different vendors tailored to their needs and analyze prices from these ads before committing to a purchase, stating that *"[...] I wait for it to reflect in Facebook and other social media sites which shows a comparison of things and then I buy [...] Half of my Facebook is basically ads."* (67). RF spoke about targeted ads as an advantage to them in the event that they forget about something they looked at, serving as a reminder for a purchase that they meant to make but didn't make immediately, saying that *"[...] on the other hand of course the ads are relevant to me because they concern things that I am interested in or have looked at, so it can also work as a reminder to me if I haven't made a purchase yet."* (69).

In contrast to this, we also had some respondents who talked about the targeted ads as being invasive and/or annoying (66, 69, 71, 80, 85, 88). RD spoke about how they would prefer to separate their shopping from other online activity, but couldn't because of constant ads popping up, stating that *"I don't like it, because if I look at shoes, the second I go into Facebook I have the same shoes on the side [...]"* (66). RG mentioned that constant ads made them feel pressured or pushed in terms of having to see these products all the time, stating that *"I find that personally I like to make a purchase from things that I like, I look through a brochure or catalog and pick my own stuff. Rather than having it come up [...] like they are being pushed on to you [...]"* (71). RQ talked about their dislike for invasion of their private space by ads, saying *"I want to be alone, I don't want that. I just simply don't want it, I don't like it."* (85). It was interesting to note that some of our respondents felt like they didn't necessarily want the targeted ads, but felt forced to accept them anyway (60, 73).

5.4.2 User measures for data protection against cookies

A key measure mentioned by a number of our respondents in order to protect their privacy and data was to clear or delete cookies (63, 68, 74, 75, 84), for example RK spoke about the use of high security browser add-ons in order to delete cookies (75). RC discussed the use of an antivirus program using a script running inside their browser in order to show them what cookies are active and are tracking them. Based upon this data, RC would then exit the browser and clear cookies if they found suspicious or unrecognized active cookies, explaining that *"I have an antivirus program that has a script running inside my browser, and that tells me if there are any cookies that are tracking my movement on that website. So sometimes I check that, to see if there is anything apart from that website's specific cookies tracking me.[...] if there's something else there, then I'd leave the browser, clear my cookies and then go back"* (63). Another measure that was mentioned in the empirical research to control the data collected by cookies is to set cookie preferences in browsers (68). RE spoke about this in

detail, talking about how cookie preferences can be set to ensure that passwords and credit card details are not being saved, therefore enhancing the privacy of user data *"[...] there are options to set your cookie preferences in such a way that your important passwords are not saved. Your banking and stuff shouldn't be saved [...]"* (68). Finally, two of our respondents talked about the use of incognito modes or private browsing modes on their web browsers in order to avoid data collection through cookies (68, 70).

5.5 Information disclosure

In order to investigate the opinions of information disclosure, we sought to determine what users believe is the limit for them in terms of willingness to disclose information, and also whether they would provide different or false information in order to protect their personal privacy on e-commerce platforms.

5.5.1 Limits to information disclosure

Interestingly, some of our respondents hold the opinion that the limitation of information disclosure depends on whether the e-commerce sites need that information to help them out or not (94, 96, 100, 107). Also, the trustworthiness of the e-commerce site is one of the main criteria for information disclosure, with five respondents talking about this point (94, 98, 109, 112, 122). These respondents stated that if they are using one of the sites which are famous and trusted, they won't mind sharing their personal information. However, in terms of less familiar or uncommon e-commerce sites, the same respondents were a little doubtful about giving the information, especially their credentials. In addition, RA and RB felt that, sometimes, the registration forms were too complicated, where many fields need to be filled in (90, 92), and some respondents also stated that when asked to provide data that is deemed irrelevant for the purpose of e-commerce, they would not give up the data (96, 100, 116, 118). RR stated that they would only provide the information that was mandatory, saying that *"As for the registration, I only provide my information that is mandatory. For the optional item, I will not fill out."* (118). According to our findings, most respondents would not give more details than what they found necessary for a purchase. For instance, RJ stated that *"[...] but I'm guessing like when my habits and my personal stuff like relationships, my health status, health information and stuff like that, when websites start to ask about that I would reject them pretty quickly."* (105). RO also stated that health status information would be too sensitive to disclose, *"[...] my income, and if I have any diseases for example."* (113). RH and RO answered they would rather not give out their social security number as well (102, 113).

5.5.2 False or different information

As for the willingness to provide false or different information for the e-commerce websites, four of our respondents explicitly stated they would give their real information in order to ensure the package can be successfully received (92, 103, 120, 121). It was found that they are willing to share their data on the premise that the sites are highly trusted, especially using familiar or well known e-commerce sites. It's interesting to note that RB believed the more information given to an e-commerce site, the more the benefits, stating that *"I consider myself*

as looking at information as not an issue, because the more you give about yourself to an e-commerce site, the better your experience will be [...]" (92).

On the other hand, respondents expressed concern about the issue of information disclosure (91, 93, 95, 97, 99, 103, 108, 109, 110), and of these, six respondents answered that they would use a separate email address when doing online shopping (91, 93, 95, 99, 108, 110). The reason given for this was that usually they would get too many promotional emails once they subscribed (91, 93, 99). Separate emails were used by the respondents in order to avoid annoyance and frustration of too many junk emails on their primary accounts. Different or incomplete addresses were used by three respondents (99, 109, 110). RM stated that *"Also, I will not provide my full address. Usually, I don't provide my room number. Only the street name and street number works in China [...]"* (110). As RE claimed, he would provide the office address instead of the house address (99). Meanwhile, some of the respondents would use different names as well (97, 110, 112). RD said that *"[...] I haven't written my full last name, because my last name, no one else has that, so it's very easy to know who I am [...]"* (97). RM stated that *"[...] if I am in China [...] I don't use my real name, my full address. I usually use [...] as online name. As long as I provide a useful phone number, it's ok."* (110).

5.6 Payment information

Disclosing credit or debit card information to online retailers may in some cases be seen as a potential threat to customers' privacy, and therefore we asked the respondents how they deal with protecting their information when it comes to card payments, and whether they preferred other payment methods over card payment.

5.6.1 Card security protection

Five of the respondents use Bank-ID as a protection method when paying with their credit or debit cards on e-commerce sites (135, 136, 138, 143, 146). It should however be noted that the use of Bank-ID is in many cases enforced by Swedish banks, and paying without using it therefore can be quite difficult.

There were concerns raised from three of the respondents about the fact that some e-commerce retailers save the card information disclosed by the customers (125, 129, 131). RD explicitly stated that *"[...] I didn't want them to save my card information, but the next time I was there they had saved it anyways[...]"* (129), showing that even though the respondent made the choice to not save the card information, it was indeed saved by the site. RE mentioned that in some cases, one only needs to type in the CVV number, since the rest of the information is saved by the site, which caused a feeling of uneasiness for the respondent (131).

Actively searching for secure payment programs or certifications on the sites were mentioned by two of the respondents (127, 133), and verification symbols from payment facilitators such as Visa or Mastercard was specifically noted by RC, stating that *"I scroll to the very bottom, and [...] the logos for verified by Visa, or Mastercard [...]"* (127). Performing virus scans as a security measure connected to using card payment were done by RJ and RT (138, 147). RQ mentioned the use of a software called OneVault as a measure, where all the credit card de-

tails and login information is saved, and which uses 32-bit encryption (146). The same respondent had also signed up for a service that sends them a letter every time someone does a credit check on them (146).

5.6.2 Alternative payment methods

As an alternative payment method, four of the 20 respondents claimed that they would rather use invoice as payment method over using their credit or debit cards to directly pay on the sites (124, 144, 145), whereas RI claimed to use invoice sometimes, with the motivation that one does not have to pay directly (137). This is however contrasted by RD, who prefers to pay directly, stating that invoice payments come with additional costs, and that the respondent personally does not want to pay afterwards, and that it has become more of a habit to pay directly with card (130).

PayPal was used by four of the respondents (124, 126, 128, 140). The use of PayPal was elaborated on further by RK who stated that *"I mostly use PayPal for payments [...] So that the shop will actually never have my payment information."* (140). Other third party payment methods, namely Alipay and WeChat Pay, were mentioned by respondents RL and RM (141, 142).

Cash on delivery was also mentioned as an alternative payment method, and was preferred by both RC and RE (128, 132), whereas RG touched upon cash on delivery as well as mobile money, stating that *"I find that mobile payments are safer than credit cards."* (134). The method of using Swish as an alternative payment option was mentioned by RJ, and was described as quite handy (139).

5.7 Social media login

A fair amount of e-commerce retailers nowadays offer their customers the option to sign in through their Facebook or Google account, but connecting one's Facebook or Google account to an e-commerce retailer may have implications related to privacy concerns for the users. Therefore, we asked the respondents whether they use this function or not, and to find out what motivated them to either use it or avoid it.

Six of the respondents normally use their Facebook account to login to e-commerce sites (149, 152, 158, 159, 160, 162). The reason for logging in through Facebook was claimed to be convenience by five out of the six respondents who use that feature (149, 158, 159, 160, 162). RE, the remaining respondent out of those who used this feature stated that for them it was more a case of comparing social media ads for the best available deal, saying that *"[...] I wait for it to reflect in Facebook and other social media sites which shows a comparison of things and then I buy [...]"* (152). RF sometimes uses this function only if the respondent has forgotten their password to that particular e-commerce account, and is not be bothered to create a new account, saying that *"I usually try to avoid that [...] I sometimes do that if I've forgotten my password to the other account, or if I can't be bothered to make another account [...] more often I create an account [...]"* (153). RF further elaborated that *"[...] if I use those accounts you are giving the website permission to use information, to use details from your so-*

cial media account, to direct advertisements and to track your details. And that feels a bit odd." (153).

For those respondents that never use their Facebook account to login to e-commerce sites, 3 of the respondents stated concerns regarding personal information collection that they were not comfortable with (156, 161, 163). RK specifically stated that *"[...] I know for example that Facebook gathers this information and sells it. And they target you with advertisements specifically for you."* (156). Advertising and marketing concerns were stated by four of the respondents as a reason for not logging in with their Facebook account (154, 155, 156, 161). This is explained by RG as "*[...] they give these advertisements every time on social media newsfeeds. And I think that to an extent is annoying [...]*" (154).

Logging in via a Google account is mentioned by two of the respondents (148, 150). RC uses their Google+ account if the respondent feels comfortable in doing so, because "*[...] it's faster, it's less of a hassle. And I trust those websites so it's fine.*" (150). However, the respondent also pointed out that their Google account only consists of basic information, such as name, age and country, and that the account lacks more detailed information, which the respondent has on their Facebook and Twitter account (150). RA uses a Google account or e-mail address that is normally not used, and feels it is "*[...] a little bit further away from my Facebook profile, which is fairly personal [...] Facebook is me online, and Google account is me a little bit further away online.*" (148), drawing a clear border between their Facebook account and Google account.

5.8 Security controls and regulations

The basis of this section was to investigate whether or not the respondents were vigilant about checking for security features and controls on the e-commerce platforms that they used. We also looked for whether or not they had awareness about the laws in place to protect users and their data on online platforms. The point of this was to check whether these factors had an influence on the disclosure of information by the users on the online platforms, and how they went about disclosure depending on their levels or vigilance and awareness.

5.8.1 Secure labels and website security features

In terms of website security features and secure labels on websites, we had ten respondents who told us that they actively check for security features on the e-commerce platforms that they use to undertake their online shopping activities (168, 170, 173, 175, 177, 179, 183, 185, 189, 191). Of these, four respondents spoke of how they actively check for certifications or verification symbols in order to ensure that the e-commerce platforms they were using were compliant with security regulations (168, 173, 177, 189). RC and RF said that they do this mostly when looking at certificates or verifications from financial services providers such as MasterCard or Visa, in order to facilitate safe payments on the e-commerce payment platforms (168). RH and RQ said that they look for *"trygg e-handel",* which is a Swedish certification for safe e-commerce that provides this label to stores that have gained their certification (177, 189).

There were three respondents who told us that they actively check for https protocols in the url:s of the websites that they go to for e-commerce activities (168, 179, 191). RC in particular talked about how the presence of the https protocol in the domain of the websites that they use for online shopping assists the user to view the website with more confidence in terms of safety of the data packets being sent and received, stating that *"If the domain is secure with https, then that's more confidence if they have, like when you hover over the https, it shows you what credentials they have [...]"* (168). In addition to this, there were three more respondents who stressed the importance for them of looking for the green lock symbol that shows up for secure pages next to the URL in their browser (170, 173, 175). RD spoke about how they look for this symbol of encryption for secure data transmission especially when they make payments online, stating that *"You get that little lock, with the color change. So usually when I pay with my card, I look for that [...]"* (170). RF and RG said that they get the feeling of being more secure when they are on a website that has the green lock symbol (173, 175). It was also interesting to note that RE told us that they entrust the checking of the security features aspect of the e-commerce website that they are on to their antivirus program, allowing it to do the job of checking whether pages are secure and bringing up warnings for those that are not (172). Similarly, RK spoke about the use of browser add-ons in order to monitor website security, depending on the add-on that they use to check site certificates and show them warnings for potentially dangerous e-commerce websites (181). To conclude, a handful of our respondents expressed a lack of knowledge about security features and labels available on e-commerce websites, saying that they either haven't heard about them before, or haven't checked for them during their online shopping activities (165, 166, 178, 188).

5.8.2 Laws and legal protection

From the twenty respondents that participated in our interviews, it was interesting to note that a good number of them expressed an awareness of the legislative protection that was available in their local countries to protect their online profiles and the data that they share over the internet (164, 167, 169, 171, 174, 176, 180, 182). Most of these respondents talked about a general awareness of the presence of laws in their local countries regarding data protection, however some of them expressed a lack of knowledge about the specifics of the laws in themselves, stating that they knew that the law was in place to protect them, but did not know about exactly what specifics the legislation covered and what it meant for them as users of online platforms (167, 169, 176). RG brought up an interesting point during their interview, talking about *"I know there is the data protection act, but I'm not sure as to what extent it really is implied, or enforced [...]"* (176).

In addition to this, four of our respondents also demonstrated knowledge of awareness about the new EU General Data Protection Regulation (164, 167, 169, 171). RA and RB both expressed their feelings about the new EU regulation as having positive repercussions for online privacy in general, talking about how the regulation is a step in the right direction in terms of transparency in user data collection, usage and storage by organizations (164, 167). Also, two of our respondents, RA and RF, showed their faith in the legal system in place by talking about how they trust the legal aspect enforced on the operation of e-commerce platforms (164, 174). Both respondents RA and RF were Swedish and were referring to Swedish legislation, expressing their confidence in the Swedish system in order to protect the rights of online shoppers. In contrast to this, it was interesting to note that six respondents expressed a total lack of awareness of legal protection and the presence of laws to protect their activity and data online (184, 186, 187, 190, 192, 193). RL expressed some apathy about the presence of laws

to protect online shoppers, talking about how they didn't care about it at all (184). RT spoke of how the ramifications of legal protection and presence of laws becomes important to users after there is an actual breach of their privacy online that causes harm to them, stating that *"I guess usually, when people have been violated, they will think about the law. Otherwise, no one would pay attention."* (193).

5.9 Other measures employed for data privacy protection

From the twenty respondents that we had in our interviews, two of them talked about the use of antivirus software in keeping themselves safe from online privacy issues on e-commerce platforms (194, 196). RC detailed the use of an antivirus to monitor the tracking activity of websites in their browser, allowing the user to identify unknown cookies and be able to clear and refresh their cookies as such in order to protect themselves from unwarranted collection of their browsing data (194). The practice of ensuring that a user's online accounts have different login passwords was also brought up as a measure for protection of data privacy by two of our respondents (195, 197). RD further elaborated that the most important password for them was the password for their email account, since using their email account, a malicious party may be able to access their other user accounts on e-commerce platforms by simply requesting password resets and changing them via the compromised email address (195).

Another measure that was mentioned by RI was to always ensure that the user has logged out after an online shopping session (198). RM and RN also mentioned that they feel safer undertaking online shopping on their own devices as opposed to shared devices (199, 200), with RN elaborating further that they would also consider the environment in which they are undertaking the online shopping, preferring not to do it over public Wi-Fi networks in fear of compromising sensitive information such as their credit card information (200).

6 Discussion

This chapter seeks to discuss the relationship between our empirical findings, existing literature and CPM theory. We discuss user awareness in depth as per our findings, and how our findings apply to the context of our adapted theoretical model. We also explain the rules and measures that apply to privacy concerns as per our findings.

6.1 User awareness about data collection

User awareness has been noted to have a key role in the behavior of users of e-commerce sites, as discussed previously in our literature review. As per our adapted CPM elements model, user awareness plays a key role in influencing the control of privacy, and influences the knowledge levels of the user regarding how their data is collected and used. From our findings, it becomes evident that users showed different levels of awareness regarding different elements of data collection and use from e-commerce contexts, as summarized in Table 5.2 in the findings section. These levels of awareness could be considered to play a role in the privacy control of their data in the adapted CPM elements model used for our study.

One of the key points from our findings was the level of user awareness regarding the clauses placed by the e-commerce site about data collection in the privacy policies. As discussed in our findings, none of our respondents took the time to read the privacy policies on the e-commerce sites that they used for their online shopping activities. This is in contrast with Metzger (2007) who proposed that users actively read through privacy policies in order to gain insights on what data is being collected and how it is being utilized, in order to weigh the risks of disclosure against the benefits before formulating disclosure rules. As one of the reasons for not reading through privacy policies, users mentioned that reading through the privacy policies of e-commerce sites is considered to be an activity that is far too time consuming, which is in line with Hillman (2006), who states that e-commerce by its design is meant to be convenient and fast. As such, users may not find it motivating to read through these policies, as they may lack the time and patience to carefully scrutinize each clause and consider the implications that they may lead to.

Users also suggested improvements for the privacy policies, such as making them shorter, more understandable and more concise, rather than the lengthy policies that are filled with difficult terminology that the users may not understand. As a result of this, it could be considered that the users have a lack of awareness of exactly what is declared within the policies of the specific sites that they use, and therefore they could be unaware of exactly what data is collected and what potential concerns this poses to them as users. Even though privacy policies across websites often contain quite similar information, it cannot be guaranteed that each and every privacy policy is exactly the same. By failing to read the policies on the sites therefore, it can be argued that users place themselves at risk by failing to find out what exactly is collected from them and what potential risks they may face.

In terms of awareness regarding data collection via the use of cookies, it was found that 75% of our respondents knew that cookies were being used in order to collect their usage data on e-commerce sites. The measures and rules put in place by users to deal with data collection issues posed by cookies are discussed in depth in section 6.2.3 later in this chapter. In terms of user awareness about website security features, more than half of our respondents demonstrated some knowledge about actively looking for security features on websites in order to guarantee the safety of their data. This could be interpreted as users actively checking for security features in order to maintain a higher degree of privacy control in accordance with our model based on CPM theory.

It is interesting to note as well the awareness levels of users in relation to how much they know about the laws in place to govern data collection procedures and usage, and how these laws can therefore impact the privacy control of their data on e-commerce sites. More than half of our respondents had no awareness about data laws, showing that these users as a result are not aware of legal procedures that govern privacy control. Of the respondents that did have awareness of data laws, majority were based in the EU and expressed trust in the legal protection that was afforded to them both locally and regionally, showing that these users felt that legal procedures gave them a higher level of privacy control in terms of the data that is collected on e-commerce sites.

When comparing user awareness and internet experience, it was interesting to note that the number of hours spent online by an individual did not necessarily influence whether or not they were aware of data collection via cookies, or their awareness about website security features either. This could mean that casual internet users may spent a lot of time online, for purposes not limited to just e-commerce, without the amount of time they spend online necessarily influencing their awareness about data collection procedures and privacy control. This is in contrast with Paine et al. (2007), whose findings proposed that internet experience was a key factor contributing to knowledge about internet security procedures, which is not the case with our sample of respondents.

6.2 Privacy turbulence initiators

Based on the triangulation of our empirical findings from the interview data as well as the analysis of privacy policies done in section 4.2.2, the following were identified as key initiators of potential privacy turbulence from user perspectives on e-commerce sites. These initiators could be seen as categories of data collection components and influences on privacy ownership and control that users could cite as reasons for implementing rules on the disclosure of their information, and reasons for taking measures to protect their information once it has already been collected.

6.2.1 Trustworthiness of e-commerce platforms

As discussed already in academia, user trust in online purchasing platforms plays a key role in transaction activity and use of the website by users (Belanger, Hiller, & Smith, 2002; Büttner & Göritz, 2008; Paine et al., 2007). Our empirical research yielded interesting results regarding the influence of trustworthiness of e-commerce platforms on user rules regarding infor-

mation disclosure and the measures they undertake in order to safeguard privacy and mitigate the threat of breaches.

Our findings showed that the reputation of the e-commerce website plays a key role in enhancing the perception of trust, which promotes the use of the site by consumers, and therefore plays a key role in information disclosure and sharing of data by the users. The reputation of the site from our interviewees is broken down firstly into the familiarity aspect, whereby they feel comfortable with sites that they have used before with positive results, therefore employing it as a rule to only use sites that have been used before, and therefore are willing to share data with them and re-use the websites. Bansal, Zahedi, and Gefen (2016) argued that a previous positive experience with a website would increase the likeliness of consumers to disclose personal information. This was also the case in our findings, as it was mentioned that mainly sites that have been used before and have not experienced any issues with are chosen when performing online shopping.

The relation between disclosing information and previous experiences can also be found within the CPM model, as the development of user's privacy rules may be influenced by past experiences, suggesting that users create rules for only disclosing information if they have had previous experience with a certain retailer, thereby mitigating the risk of privacy breaches and turbulence (Petronio, 2004). Our findings also suggest that when interacting with a less famous site, some respondents expressed doubt about giving up personal information. Recognition of retailer's brand and how it correlates with the willingness to disclose information was found in the literature, as Olivero and Lunt (2004) found that there is a higher level of willingness to disclose information if the consumer regards the retailer as well known and that it has a public image to uphold.

The trustworthiness is also enhanced by the presence of positive recommendations from fellow shoppers, revealing that the reliability and reputability aspects of online shopping platforms can be shaped by online reviews, user communities and endorsements from friends. As such, only using e-commerce sites that have been recommended by others was found as a rule amongst the respondents, as well as performing research about the sites in question. Platforms that have these positive reviews and endorsements are deemed more trustworthy, encouraging users to transact on these sites and as such feel more comfortable with sharing of information. This phenomenon is explained by McKnight, Choudhury, and Kacmar (2002), who proposed that customers are more willing to share information with e-commerce operators once trust has been established.

The aesthetics of the website also play a role in trustworthiness as per our findings, with an inviting layout instilling more trust from consumers and influencing their activity on the site, encouraging them to share information. Building on this, it was found that security labels on e-commerce websites, such as certifications like *trygg e-handel* in Sweden, or verifications from payment platforms such as MasterCard, VISA, PayPal and others, also increase the trust factor and encourage consumer activity on websites, and make them feel more secure when giving out details such as payment information. Customers also trust websites more when they use security protocols such as https for information transfer, and as such may be more willing to transact and share data on sites that have the protocols in place, an idea reflected as well by Belanger, Hiller, and Smith (2002). Checking for these types of certificates was mentioned by the respondents, and identified as a rule that is done before deciding whether to engage in financial transactions with the site in question.

In light of our findings, it can be established that users have a rule of only disclosing information to sites that are familiar and trusted, since the perception of trust allows them to establish a privacy boundary that incorporates the trusted site as a co-owner of the information, and reduces the risk of privacy turbulence due to the positive previous experiences that the user and their peers have had with the site in the past. In addition, users also have a rule of researching websites and using those that have positive reviews and user experiences, and are recognizable as trusted brands with good reputations. Checking for security features and trusted certificates was also mentioned by the respondents, and identified as a rule that is followed before deciding whether to engage in financial transactions with the site in question. Table 6.1 below shows a summary of the identified rules regarding trustworthiness.

Table 6.1: Summary of rules regarding trustworthiness

INFORMATION DISCLOSURE RULES	MOTIVATION
Only use sites that have been used before/familiar sites	Avoid potential privacy turbulence on unfamiliar sites
Check for security labels and security features on the website	Confirm legitimacy of site and security of disclosed data
Do research and use sites with positive reviews, recommendations and user experiences, and good reputation	Confirm reputation and user trust from fellow users

A key measure that was noted was that a user would leave the site if they would feel that security of the information provided is threatened, which can be connected to privacy turbulence within the CPM model, as it may lead to a sense of unclear boundaries of privacy of the provided data. This in turn has the effect of causing the user to withdraw from engagement from the site and instead searching for an alternative in order to avoid privacy turbulence. Table 6.2 below shows a summary of the identified measures regarding trustworthiness.

Table 6.2: Summary of measure regarding trustworthiness

MEASURES EMPLOYED	MOTIVATION
Leave the site if there is an emerging feeling of security threats	Avoid potential privacy turbulence

6.2.2 Information disclosure

As stated by Olivero and Lunt (2004), willingness to disclose information increases when the users perceive benefits such as time consumption. This was also found in our study to some extent, as six of the twenty respondents would sign in to e-commerce sites via Facebook, thereby letting e-commerce retailers gain more information about the consumer, in exchange that it saves the consumer time by not needing to create a new account for the specific retailer. On the other hand, it was also found that the other users were not comfortable with allowing e-commerce sites access to their social media profiles and data, also resulting in targeted ads which were not wanted. Therefore, a rule that was brought in light of this was avoiding the use of social media logins in order to access user accounts in e-commerce sites, and creating separate accounts for this, in order to avoid privacy turbulence.

Regarding what information to actually disclose when deciding to do so, a common theme identified from our findings is to only give out information that is mandatory, and in some cases only information that is deemed relevant in relation to the expected benefit (product or service) the users see, thereby neglecting to fill out optional information fields. Hence, a rule enforced by users is to only disclose information that they consider relevant, in order to limit the disclosure of too much personal information. As suggested by the CPM theory, users develop rules in order to maximize the benefits, but are also trying to minimize the risks following information disclosure at the same time, meaning the users want to make use of the benefits of information disclosure to e-commerce sites, while still trying to keep their information disclosure at a minimum. If sites request for disclosure of more personal data, such as relationships or the user's health status, it was mentioned by a couple of respondents that they would discontinue the usage of the site, thereby clearly stating what type of information becomes too sensitive to disclose within an e-commerce setting. This can be related to the claims made by Gupta, Iyer, and Weisskirch (2010), who state that consumers are more worried about giving up information of sensitive nature such as medical and health data.

Interestingly, results also show that some users don't consider themselves to have any clear limits as to what information to give up, motivated by reasons such as the shopping experience will be better if the retailer knows more about the individual, as long as the retailer does not act illegally or unethically, or example selling the information to other websites or companies. This correlates strongly to the theory of psychological contracts that Bansal, Zahedi, and Gefen (2016) discussed, stating that when a user discloses personal information to a vendor, the user may feel that a psychological contract is formed between user and vendor, acting as an assurance that the vendor will handle the information with responsibility. Having no clear limits as to what information to disclose in an e-commerce setting could partially be explained by the users putting their trust in the hands of the e-commerce retailers and expecting them to act with responsibility regarding their personal information. Similarly, as per the CPM theory, the retailer would become co-owner of the information provided, where the original owner of the information perceives the retailer to be responsible for the provided data the same way the original owner is.

It was noted through our empirical findings that some of the users may be inclined to provide false/different information to e-commerce websites, rather than revealing their actual details. This is done in order to retain a sense of ownership of data that can be used to identify the user personally, as well as to avoid potential privacy turbulence as per CPM theory. Using a separate email address when performing online shopping was identified as a rule as per our empirical findings, and this was done by users primarily in order to avoid receiving a large amount of unsolicited promotional communication. By using an alternative email address, this communication can be avoided, as the secondary accounts aren't accessed as frequently as users' primary email accounts. The user can therefore avoid having to deal with massive amounts of promotional email content that comes from using the e-commerce platforms. This in turn could be seen as avoidance of privacy turbulence, which could be caused through the misuse of email address information for unsolicited communication that could become a cause of annoyance to the user.

Providing different postal addresses was also identified as a rule, such as using one's office address rather than home address. The motivation behind this was to avoid the problem of junk mail such as advertising material. In addition, this rule could help keep the user's personal information private by not disclosing their residential address. Using different names was also found in the results of the study, for instance using separate profile names in order to

limit the disclosure of personal information. The motivation for this was to preserve the anonymity of the user on the e-commerce platforms, and avoid giving out personal information that could be used to identify them. These rules for information disclosure could be in place in order to avoid potential privacy turbulence caused by the mishandling and unauthorized use of data that could be used to identify a user, for example their names and postal addresses. Table 6.3 below shows a summary of the identified rules regarding information disclosure.

Table 6.3: Summary of rules regarding information disclosure

INFORMATION DISCLOSURE RULES	MOTIVATION
Only reveal mandatory/relevant information	Limit disclosure of detailed/sensitive information
Use separate email address	Avoid spam/junk mail
Use different address such as office address for delivery	Avoid junk post, keep personal information private
Use different profile or username rather than real name	Preserve anonymity, keep personal information private
Do not use social media login	Avoid sharing social media information and avoid targeted ads

6.2.3 Data collection through cookies

According to our findings, it was noted that some respondents have basic understanding on the use of cookies in e-commerce websites, and this understanding mostly comprised of the main functionalities of cookies such as storing the login information, password as well as page visits in the process of browsing e-commerce sites. However, it could be argued that there may be lack of in-depth understandings of cookies, evident from our findings whereby some respondents demonstrated a lack of knowledge regarding cookies and their functionality. This brings about an issue in the privacy boundary as per the CPM theory, as users continue to browse and transact without being aware of what is being collected via cookies and how it is being used. As a result, the ownership of the data, and the ownership of the privacy as a result, could be considered ambiguous due to the lack of knowledge on the part of the user. Through lack of knowledge of cookies, the user is essentially unintentionally adding the collecting entity to the privacy boundary by sharing ownership of their data in from of tracking browsing habits.

Third party, or persistent cookies, that track users across websites also came up as an area of interest during the research. These cookies have a preset expiration date, and remain on the user's hard drive until the preset expiration date is reached. Because the storage of navigational streams and login information, these types of cookies can be used for monitoring and tracking user browser behaviour and linking to any provided personal information (Turner & Dasgupta, 2003). Third party persistent cookies can be used across e-commerce sites linking to users' social media profiles, and according to the research that was conducted, there are two trains of thought regarding user behavior and this phenomenon. On one hand, some users see social media logins and sharing of data across e-commerce sites as useful, firstly for the convenience of centralized logins and not having to create multiple accounts, and also for the

advantage of tailored ads appearing to them on their social media platforms. On the other hand, some users avoided social media logins as they viewed the sharing of data across platforms as invasive to their privacy, and did not want to experience too many ads and promotions on social platforms. In such a scenario, the users reject sharing their social media data with e-commerce sites, attempting to retain ownership of their privacy and avoid potential privacy turbulence.

It is interesting to note however that despite this state of ambiguity regarding cookies, users still consent to the use of cookies that exist on the e-commerce websites. One of the reasons for this phenomenon is the respondents believed these sites they trusted would not pose a threat to their personal information, showing that the users would allow the site into their privacy boundary for that particular data. Also, as touched on before, some respondents claimed that they liked the fact that cookies resulted in targeted ads and customization of website experiences, showing that these users were in fact quite comfortable extending the ownership of their data to e-commerce sites in return for the perceived benefit brought about through customization and suggestions made through recommendation systems.

However on the other hand, some users expressed concerns about the use of cookies, particularly regarding the storage of critical information such as their bank details and payment information. Other brought up concerns regarding the fact that they could not use e-commerce sites without accepting the use of cookies, and felt like this was an invasion of their privacy. This shows that there is a group of users who are not willing to allow cookies into the privacy boundary they share with e-commerce sites, and are forced to share ownership of the data pertaining to their browsing habits and personal information against their wishes. These users brought up a number of rules and measures that they take for protecting the privacy of the data collected from them through the use of cookies on e-commerce websites and as such avoiding privacy turbulence.

A rule that was mentioned in order to avoid privacy turbulence through collection of data via cookies was to use incognito or private browsing modes on browsers, which do not track user activity and store browser history. Table 6.4 below shows a summary of the identified rules regarding cookies.

Table 6.4: Summary of rules regarding cookies

INFORMATION DISCLOSURE RULES	MOTIVATION
Use incognito/private browsing	Avoid tracking of usage behavior and site visits

As cookies store the data in the form of a file, which can be found on the local drive storage on the user's machine, one of the measures employed by users to remove information about user behaviour and to prevent privacy turbulence is to regularly clear their cookies. According to the study, another measure is the use of software such as browser add-ons to monitor cookie activity, or antivirus programs that notify the user about what cookies are tracking their movement on that website, after which the cookies can be cleared if desired. Some system management software may also provide the functionality of clearing up the cookie automatically. Table 6.5 below shows a summary of the identified measures regarding cookies.

Table 6.5: Summary of measures regarding cookies

MEASURES EMPLOYED	MOTIVATION
Clear cookies manually	Remove information that has been stored about usage behavior and avoid privacy turbulence
Use software to detect, display and delete cookies - antivirus, browser add-ons	Check for unauthorized cookies, maintain control over what cookies are storing data

6.2.4 Payment information

As discussed by Gupta, Iyer, and Weisskirch (2010), financial data may be considered as sensitive information to disclose within an e-commerce setting. As a result of this, users of e-commerce sites may wish to handle their payments in other ways than using their credit or debit cards. Our findings suggest three different main alternatives to paying with cards, namely invoice, third party payment options such as PayPal or Alipay, and cash on delivery. Reasons for using alternative payment methods vary, and may not in all cases necessarily take privacy protection into consideration per se. For instance, reasons for using invoice seem to be more of a convenience question rather than that of privacy for some users, since the users then don't have to pay directly upon ordering, thus first having the products delivered and pay at any time within the time frame issued by the invoice company. If the option of using invoice is available, using invoice was however identified as a rule by one respondent, as invoice was preferred by this respondent if the site in question is considered to be unfamiliar, which again can be linked to the importance of trustworthiness in an e-commerce site when it comes to disclosing sensitive information.

Using PayPal rather than paying with card was also identified as a rule to be used for privacy reasons, since it was mentioned that when using PayPal, the e-commerce site does not have access to the customer's payment details, thus protecting them from privacy related issues concerning their credit card information within the realms of e-commerce sites. From a CPM perspective, the rule of not using direct payment with credit or debit cards for e-commerce purchases, and rather use alternative payment methods so the e-commerce sites don't possess one's payment information may be linked to the fear of privacy turbulence, since if this information is disclosed to the retailers, they would become co-owners of this information, and there may arise questions regarding the privacy boundary structure. As CPM stipulates, privacy turbulence comes about in instances when organizations do not strictly follow the privacy rules set in place, which may lead to a lack of privacy coordination. This is because the shareholders of the information don't follow or implement the privacy rules as they are intended by the original owner of the information, in this case the consumer. Table 6.6 below shows a summary of the identified rules regarding payment information.

Table 6.6: Summary of rules regarding payment information

INFORMATION DISCLOSURE RULES	MOTIVATION
Use third party payment methods (such as PayPal for instance)	Avoid giving out sensitive bank card and other payment details
Use invoices instead of card payments	Avoid giving out sensitive bank card and other payment details to unfamiliar sites

It was noted in our findings that the use of Bank-ID was mentioned several times amongst our respondents as a measure when paying with cards online. However, as stated in the findings part, this doesn't necessarily have to do with actively and consciously protecting one's information. This is because many banks in Sweden, where the majority of respondents who mentioned Bank-ID are from, enforce the use of Bank-ID in order to avoid fraudulent transactions. It was noted in addition that users are uncomfortable with leaving their credit card information saved on e-commerce sites, and actively try to ensure that this sensitive data does not remain saved on the site after they have input it to make a payment. This was identified as a measure in trying to protect their card information in order to avoid potential privacy turbulence that could be caused by compromising their credit card details through saving it on the e-commerce platform. Table 6.7 below shows a summary of the identified measures regarding payment information.

Table 6.7: Summary of measures regarding payment information

MEASURES EMPLOYED	MOTIVATION
Use Bank-ID when making payments	Avoid potential fraudulent transactions
Do not save card information on e-commerce sites	Avoid compromising card details

6.2.5 Other general security rules and measures

Maintaining different login passwords and/or usernames across different platforms was brought up as a rule for protection of data privacy by two of our respondents. This could be considered to increase the perception of privacy control by users, as maintaining different usernames and passwords across platforms decreasing the chances of compromising multiple accounts in the event that one account is compromised. This is especially true in the case of email accounts, since malicious programs, individuals or organizations may be able to access the victim's other user accounts on e-commerce platforms by simply requesting password resets and changing them via the compromised email address. Using separate usernames and passwords on each platform could minimize this risk as such, allowing users more perceived control over their private data.

Moreover, the research shows that users consider the environment in which they are undertaking online shopping, preferring not to do it over public Wi-Fi networks or shared devices in fear of compromising sensitive information by malicious parties. Providing data over unsecured networks and devices could as well lead to privacy turbulence from user perspectives, leading to the rule of ensuring that secured networks and devices are used to conduct transactions involving sensitive information. As such, another rule identified is to not make transac-

tions on shared devices or unsecured networks. Table 6.8 below shows a summary of the identified rules regarding general security.

Table 6.8: Summary of rules regarding general security

INFORMATION DISCLOSURE RULES	MOTIVATION
Create separate accounts and passwords for each site	Avoid privacy turbulence in case one account is compromised
Avoid making transactions on shared devices or unsecured networks	Avoid interception of sensitive data by malicious parties

A measure identified regarding general security was to always ensure that the user has logged out after an online shopping session. This could be a measure to reduce the risk of their data being accessed by unauthorized parties who may log in with their credentials, thus logging out allows the user to maintain a sense of privacy ownership.

Based on our empirical findings, it can be noted that the use of antivirus software in order to keep users safe from privacy issues on e-commerce sites can also be considered to be a measure against privacy turbulence. This works by monitoring the tracking activity of websites in their browser and warning users about malicious sites that may seek to enter the privacy boundary of their data without authorization. As discussed in privacy boundary management in the CPM theory, users should be able to form rules to regulate at what times and at what circumstances information is to be revealed or to be withheld. The antivirus software as such could help users control data transfer between the browser, e-commerce sites and third parties, allowing them more control over the privacy boundary. Table 6.9 below shows a summary of the identified measures regarding general security.

Table 6.9: Summary of measures regarding general security

MEASURES EMPLOYED	MOTIVATION
Always log out after shopping session	Avoid unauthorized access to user account
Use an anti-virus software	Protection against malicious sites

In order to obtain a clear overview of the rules and measures identified in the study, the following tables (Table 6.10 & Table 6.11) have been included as a consolidated summary. The tables also show the motivation behind employing each rule and measure in order to highlight the reason for the existence of the rule/measure in question.

Table 6.10: Summary of rules

PRIVACY TURBULENCE INITIATOR	INFORMATION DISCLOSURE RULES	MOTIVATION
Trustworthiness	Only use sites that have been used before/familiar sites	Avoid potential privacy turbulence on unfamiliar sites
	Check for security labels and security features on the website	Confirm legitimacy of site and security of disclosed data
	Do research and use sites with positive reviews, recommendations and user experiences, and good reputation	Confirm reputation and user trust from fellow users
Information Disclosure	Only reveal mandatory/relevant information	Limit disclosure of detailed/sensitive information
	Use separate email address	Avoid spam/junk mail
	Use different address such as office address for delivery	Avoid junk post, keep personal information private
	Use different profile or username rather than real name	Preserve anonymity, keep personal information private
	Do not use social media login	Avoid sharing social media information and avoid targeted ads
Cookies	Use incognito/private browsing	Avoid tracking of usage behavior and site visits
Payment Information	Use third party payment methods (such as PayPal for instance)	Avoid giving out sensitive bank card and other payment details
	Use invoices instead of card payments	Avoid giving out sensitive bank card and other payment details to unfamiliar sites
General Security	Create separate accounts and passwords for each site	Avoid privacy turbulence in case one account is compromised
	Avoid making transactions on shared devices and unsecured networks	Avoid interception of sensitive data by malicious parties

Table 6.11: Summary of measures

PRIVACY TURBULENCE INITIATOR	MEASURES EMPLOYED	MOTIVATION
Trustworthiness	Leave the site if there is an emerging feeling of security threats	Avoid potential privacy turbulence
Cookies	Clear cookies manually	Remove information that has been stored about usage behavior
	Use software to detect, display and delete cookies - antivirus, browser add-ons	Check for unauthorized cookies, maintain control over what cookies are storing data
Payment Information	Use Bank-ID when making payments	Avoid potential fraudulent transactions
	Do not save card information on e-commerce sites	Avoid compromising card details
General Security	Always log out after shopping session	Avoid unauthorized access to user account
	Use an anti-virus software	Protection against malicious sites

7 Conclusion

This chapter concludes our study by answering the research question and showing whether the purpose of the study has been fulfilled. We also outline the knowledge contribution of this study and make suggestions for future research.

The use of B2C e-commerce sites has brought about a number of benefits for users, such as allowing them to shop remotely from the comfort of their homes and receive delivery of products saving them the hassle of transporting their purchases. In addition, users have the advantage of personalized services and suggestions that are tailored to their tastes and preferences in order to promote a satisfying online shopping experience. However, these benefits also come with significant risk attached, as in order to use and enjoy the benefits on B2C e-commerce platforms, users must give up their data to the websites. As such, the consumers are faced with various potential privacy risks associated with the disclosure and use of data on B2C e-commerce sites. The awareness about online privacy issues is a direct factor that influences the rules on information disclosure and the measures that users employ to minimize harms caused by privacy concerns on B2C e-commerce platforms.

This study has resulted in identifying both rules that users impose before agreeing to voluntarily disclose information, and measures they take for minimizing privacy concerns pertaining to the data has already been collected by the e-commerce sites. The study was conducted by taking a qualitative method of research, using interviews as the selected method of empirical data collection. The empirical data was collected after an analysis of potential privacy threats on existing privacy policies that was done to identify potential privacy turbulence initiators; namely cookies, information disclosure, trustworthiness, payment information and general security.

7.1 General findings

The research question for this thesis was “What measures and rules do users employ in order to mitigate data privacy concerns on B2C e-commerce sites?”

It was found that the rules and measures employed by users in order to govern information disclosure and protect data privacy may vary from one individual user to the other. However, the study found that there are a number of rules and measures that multiple users agreed upon as valid for mitigating data privacy concerns on B2C e-commerce platforms. In terms for the rules for information disclosure, it was found that users are more willing to disclose information to familiar sites, as well as sites with security features present and with positive recommendations from fellow shoppers. In addition, users are only willing to reveal mandatory information for transacting purposes, and may use separate email addresses, postal addresses and usernames in order to protect themselves from privacy threats. It was also found that users browse e-commerce sites in incognito/private browsing modes in order to try and avoid

data collection via cookies, and that they try to use third party payment methods (such as PayPal) and invoicing in order to avoid giving out credit card information. General security rules that were found included the use of separate usernames and passwords for each e-commerce site, and also avoiding the use of unsecured networks or shared devices when making transactions and purchases. A concise summary of all the rules identified and their motivations can be found in Table 6.10.

In terms of the measures taken by users to minimize the risk of privacy turbulence, it was found that users tend to leave sites without any further action immediately they feel that their security is threatened. Users also take part in clearing cookie data, both manually and by use of software such as antivirus software and browser add-ons to monitor and delete cookies. It was found that users are unwilling to save credit card details on sites, and also tend to rely on Bank-ID in order for protection when making payments on e-commerce platforms. General security measures found in this study indicate that users generally rely on antivirus software for all round security on the internet, including browsing e-commerce sites, as well as ensuring that they are always logged out after completing transactions. A concise summary of all the measures identified and their motivations can be found in Table 6.11.

By summarizing the rules and measures from our research, the purpose of this study has also been fulfilled, as the purpose was to identify the rules users of e-commerce set when disclosing information, and to identify the measures they employ in order to protect their data privacy. A better understanding on how users respond to and mitigate privacy concerns has been presented in this study. Meanwhile, the study also provides users of e-commerce sites with knowledge on improving their online privacy risk prevention awareness through applying the identified rules and measures during their online shopping activities. The study also allows researchers and practitioners to better understand the rules on information disclosure and measures for protecting privacy on B2C e-commerce platforms.

7.2 Contribution of study

This study identified the rules governing information disclosure and measures of privacy protection from the user perspective with a focus on B2C of e-commerce sites. This was carried out by applying the CPM theory formulated by Petronio (2002) into e-commerce contexts, building on the research done by Metzger (2007). The adapted CPM elements model explains the privacy boundary of user data as applied to B2C e-commerce sites in this study. The adapted model takes into account the contributing factors to privacy control, privacy ownership and privacy turbulence. This contributes to expanding on existing knowledge existing in the field. Furthermore, the study contributes to existing literature in the field by not only outlining the specific rules that users incorporate for information disclosure on e-commerce platforms, but expanding the scope of CPM theory by also outlining the measures taken in order to minimize privacy turbulence once their data has already been collected.

As the rules and measures have been identified in this thesis, performing a larger scale study using quantitative research methods could be of interest in order to see to what extent these measures and rules are employed by a wider population of e-commerce site users. This could be done in order to validate and obtain more in depth perspectives regarding user rules on information disclosure and the measures they employ to minimize privacy turbulence risks. To build on to the contribution of this study, it could be interesting also to establish the effec-

tiveness of rules and measures in future research, whereby future researchers could also test the importance and priority of the rules and measures. In addition, it would also be beneficial to understand more specifically what factors can affect these rules and measures, and how they impact the formulation of privacy protection rules and measures in different contexts.

Appendix I

Codes	Respondent	Content	Sub-codes	Reference Number
1-Choice of Site	RA	"Price, of course [...] Recognition of retailer, important [...]" [line 10] "Trustworthiness goes with recognition [...] security in terms of privacy, yeah." [line 12]	1a-Drivers	1
	RA	"[...] I usually Google it if I don't know about it and read what the other people wrote about it [...]" [line 10] "Yeah, reviews of the website. In general." [line 12] "[...] some basic research on whether the website is trustworthy or not [...] mostly I'm looking for the fact if it's been delivered, if people are happy with the customer service, or if the product looks like it does on the website [...]" [line 16]	1b-Research	2
	RB	"[...] firstly look at those websites that have the best price [...] I don't pay anything for shipping [...] good way for me to get a range of products at a good price [...] I look at things that I like, and that happens to be maybe brands [...]" [line 8]	1a-Drivers	3
	RB	"[...] read reviews about products [...] if I can see a few reviews that are happy with the product, the quality is good, the shipping didn't take too much time or anything like that. That influences me, a great deal. [...] I don't really do all that much of research about the website or about the	1b-Research	4

		company, just a little bit.” [line 10]		
	RC	“I go for the websites that I’ve used before mainly [...]” [line 8] “[...] I’ve used them before and haven’t had any issues [...]” [line 10] “[...] the website's overall look. If it looks nice, and appealing, that encourages me a bit more.” [line 14]	1a-Drivers	5
	RC	“I try to see if someone else has used it, like I’d hop on Reddit and see if people have used this, their opinions on it, and if that was good [...]” [line 14]	1b-Research	6
	RD	“How cheap the website is, of course, and also if it’s a known website and if a friend has shopped there. But I mainly buy clothes. So the main factor is how nice are the clothes.” [line 8]	1a-Drivers	7
	RD	“I usually do a lot of research before [...] I look at reviews on YouTube, before I buy them, and buy them on the same website as they bought them.” [line 10] “[...] if it’s an international site, I usually do that, well, if it’s a new site that I haven’t shopped before [...] I usually look for did they get the package, is the quality really bad [...]” [line 12]	1b-Research	8
	RE	“[...] they come back with good prices. And based on that I do my shopping.” [line 8] “[...] when they want a pricey and good stuff that they want to keep for some time then they go into the good websites. If they want the price to be	1a-Drivers	9

		low and the item to be thrown away in a few months then they go for cheap. At least I do that." [line 12] "I generally don't go into sites which are not that famous [...]" [line 14]		
	RE	"I check for reviews as well. Reviews are very important [...]" [line 10] "[...] I ask friends who have done shopping from there [...]" [line 14]	1b-Research	10
	RF	"I usually use online stores which I'm familiar with, that I know of because of their quality and they are reliable,[...] previous experience, good reviews." [line 8]	1a-Drivers	11
	RG	"[...] the security [...] the price, obviously. I would look at the reputation of who's selling online [...]" [line 8]	1a-Drivers	12
	RG	"[...] I ask friends, maybe check some reviews on the net, Google the site [...]" [line 10]	1b-Research	13
	RH	"How reliable the site is." [line 10]	1a-Drivers	14
	RH	"I Google it, and see what the reviews are, how famous it is." [line 15-16]	1b-Research	15
	RI	"I look at ads from the Internet that pop up." [line 8]	1a-Drivers	16
	RI	"No, no reviews, I look at their delivery time, but I don't read reviews." [line 14]	1b-Research	17
	RJ	"[...] reputation to start off. Or, it depends, first its price, if you find a good price. Then the reputation, I	1a-Drivers	18

		mean if they are reliable or not. So I think price, then reputation. And of course then we also have delivery time and stuff like that." [line 8]		
	RJ	"Yeah, I always Google them before. If I want to buy something that is offshore or abroad I always google them to see if they are reliable… if they deliver on time." [line 10]	1b-Research	19
	RK	"Mainly price, I decide on the product and then I look at the price - where to buy it from." [line 8]	1a-Drivers	20
	RL	"I'd like to say price and delivery." [line 8] "For instance, if I plan to buy some protein powder, which is very heavy. Also, the price is usually lower at Amazon England. If I do it online, then I don't have to carry it on my own. They will deliver it to the agency." [line 10]	1a-Drivers	21
	RM	"Price.. And payment measurement." [line 8]	1a-Drivers	22
	RM	"I used Zhihu (https://www.zhihu.m/). Sometimes." [line 14] "Check if the service is good? Delivery or something. Normally, I only do some research for the brand or store. Just go through some comments. To see the reputation of the sites [...]" [line 16]	1b-Research	23
	RN	"[...] the main driver is price." [line 10]	1a-Drivers	24

	RN	"I would look through the site directly. I do care about the product itself instead of the site. " [line 16]	1b-Research	25
	RO	"Recognition of retailer." [line 8]	1a-Drivers	26
	RO	"Yes, I Google and compare prices and stuff." [line 12]	1b-Research	27
	RP	"The cheapest, and the delivery time." [line 8]	1a-Drivers	28
	RP	"Yes, I look at the reviews. And often I get recommended from people I know." [line 10]	1b-Research	29
	RQ	"Recognition of retailer." [line 6]	1a-Drivers	30
	RR	"I'd like to say trustworthiness and convenience. [...] I will only go to my trusted site, such as Amazon, where I basically would not get the fakes. So the main driver is trustworthiness. Also, convenience, Sometimes, the registration is over needed complicated. They ask me input a lot of personal information. That's time consuming. And I feel my privacy and security are threatened. I will not do that." [line 8]	1a-Drivers	31
	RS	"Trustworthiness, Because I want to get high quality product. And I only go to the site I trusted, like Tianmao." [line 10]	1a-Drivers	32
	RT	"For me, it's time-saving [...] and convenience. I don't think the price is lower as for online shopping. It's almost the same price. Yeah, the main driver is time-saving." [line 8]	1a-Drivers	33

2-Privacy Policies	RA	"[...] it's too complicated [...]" [line 18] "I like simplicity, so the easier it is the better [...] I assume that every-thing looks the same. So if I have read one, yeah." [line 20]	2a-Formats	34
	RB	"[...] it's so long... [...]" [line 14] "[...]keep it in a format that the main points are delivered to the user[...]" [line 16] "[...] don't have to go into any details [...] We keep track of, this or this, or only this. As you see, like those are only three points that only take what, 30 seconds to read. Instead of having this small text and pages [...] [line 18]	2a-Formats	35
	RC	"They're just too long and they try to be specific, but they end up being vague because of the legal terms [...] I don't find them to be useful." [line 16] "[...] change the privacy agreement to like a short video, or infographic, or something like that, I'm more likely to see it." [line 18]	2a-Formats	36
	RD	"It takes too long." [line 18]	2a-Formats	37
	RD	"if there was like a summary in the beginning with a short bullet list maybe [...] then a longer explanation further down [...] also in language, if it's too difficult to understand then you won't read [...]" [line 20]	2a-Formats	38
	RE	"[...] if it pops up then maybe the first three lines, maybe the headings, but not like, okay I'm going to do shop-ping here so I need to read through the privacy policy, never done that."		39

		[line 16] "[...] it's a waste of time [...] I'm confident that they would have privacy policies there that wouldn't affect me pretty badly in any way [...] just the headings to see what they are talking about or something, and if I'm bored, maybe. Not if I'm in a hurry to buy something." [line 18]		
	RE	"It's supposed to be long and lengthy, [...] provide the headings in bold for you to understand more [...] any document is given to you which is lengthy you wouldn't read through it. You'd just go through the headings [...]" [line 20]	2a-Formats	40
	RF	"[...] you don't look through because it's long and you don't have the time.[...] assume that the details put down there are details that I'm aware of or that I would agree with [...]" [line 12] "[...] they could have a summary [...] could help you orientate and look for more details if you're interested." [line 14]	2a-Formats	41
	RG	"I just skim through it really fast, mainly because it's too long sometimes,[...] it's too technical [...]" [line 12] "[...] Making it a bit direct and to the point.[...] it could be a bit shorter, and maybe have some places where it could be expanded for those who want to go ahead and read more [...]" [line 16]	2a-Formats	42
	RH	"They are too long, but I don't think i would read them anyway." [line 22]	2a-Formats	43

	RI	"Because most of the privacy information is mostly the same anywhere, when we live in Sweden, so you kind of know what they are allowed to use and not." [line 18]		44
	RJ	"[...] I think they could be simplified." [line 16] "Like, four sentences "this is what's up" pretty much, but I guess it's part of their business plans to keep that in the dark to customers sometimes maybe. " [line 18]	2a-Formats	45
	RK	"[...] it's very long which I guess is the biggest thing that makes people not read it." [line 16]	2a-Formats	46
	RL	"Sometimes, I can't understand Swedish and sometime, it's too long. I don't have that much patience. It's boring and pointless." [line 28]	2a-Formats	47
	RM	"I am just so lazy. It's time-wasting. For me, I don't consider they are that important.[...]" [line 20] "[...] I would say yes. Because I don't encounter any problem with that.[...]" [line 22]	2a-Formats	48
	RN	"I just want to buy something. Why should I read that [...] I don't think I have to take care of these privacy policies." [line 22]		49
	RN	"No. I prefer to the graphic ways. It should be easy to understand. The existing formats are too boring." [line 24]	2a-Formats	50
	RO	"Maybe it's a bit complicated written; the language is perhaps hard to	2a-Formats	51

		understand.” [line 18]		
	RO	“I never thought about it.” [line 16] (regarding reading privacy policies)		52
	RP	“I don’t really know where to find that, and I don’t really care.” [line 14]		53
	RQ	“Why should I?” [line 12] (regarding reading privacy policies)		54
	RR	“No, never. I think reading these policies does not make much sense to me. And usually, there is a drop-down arrow in the privacy page; I guess the site doesn’t really want us to read. Users can go directly to the bottom of the page and click “I agree”[...].” [line 12]		55
	RR	“Personally, I think that is a lot of jargon, I do not know what they mean.” [line 14]	2a-Formats	56
	RS	“[...] it’s quite long and boring to read. Again, I trust these sites. I don’t think they would bring me into trouble.” [line 16]	2a-Formats	57
	RT	“[...] Here is too much information piled up together. That makes me lose the desire to read. It is not straightforward.[...]” [line 16]	2a-Formats	58
3- Cookies & Tracking	RA	“I understand the business perspective of it [...] it is what it is, it’s not going to get any less, it’s only going to increase. Of course, it’s a bit annoying [...] sometimes it can get too much.” [line 26] “I would wish for more choices [...] if		59

		I don't accept it I can't go and use the website either way, and that is the problem. [...] one possibility could be that you have your own privacy record, and then the business has to accept that from you. [...] I have to follow the rules, which is using cookies, if I want to use the website. [...] It's giving too much power to the business." [line 32]		
	RA	"I'm not willing, but I'm accepting it." [line 30]	3a-Targeted ads	60
	RB	"What I expect them to do is just to improve my search quality. I don't expect them to take what I do online or where I exit, or to what website i exit to from their website or whatever. [...] That doesn't matter, I don't see why that should matter [...]" [line 14] "I think it really depends on the purpose, on what you're going to do with the tracking, with the data [...]" [line 22] "[...] we can also go into more detailed ethical questions, how much is too much tracking [...]" [line 24]		61
	RB	"[...] see what things I like and then make suggestions for extra purchases, and I would maybe get advertisements towards myself about things that I like [...]" [line 22] "I think that's a good thing [...]" [line 24]	3a-Targeted ads	62
	RC	"I really don't mind them [...] I think it's fine, we go into a mutual agreement, you provide me a service and in turn I give you something back."		63

		[line 24] “I need to know that they’re using cookies [...] I just need to be informed beforehand, and then I accept it and continue using.” [line 26] “I have an antivirus program that has a script running inside my browser, and that tells me if there are any cookies that are tracking my movement on that website. So sometimes I check that, to see if there is anything apart from that website’s specific cookies tracking me.[...] if there’s something else there, then I’d leave the browser, clear my cookies and then go back” [line 42] “Only when I find a cookie that I don’t recognize or that I’m suspicious of, but very rarely do I actually do that. The last time I cleared my cookies was maybe three months or four months ago.” (on clearing cookies) [line 44]		
	RC	“[...] it makes my life a bit easier [...] they give me recommendations for products that I actually want.” [line 24]	3a-Targeted ads	64
	RD	“I don’t like them, [...] I wish it was more easy to decline the use of cookies [...] I don’t want to use cookies but I still want to use your website [...]” [line 24] “[...] I didn’t want them to save my card information, but the next time I was there they had saved it anyways[...]” [line 28]		65
	RD	“I don’t like it, because if I look at shoes, the second I go into Facebook I have the same shoes on the side	3a-Targeted ads	66

		[...]" [line 24] "I may be not willing, but I am willing since I'm doing it. [...] I'm not excited about it, but otherwise I wouldn't be able to use the websites." [line 26]		
	RE	"[...] I wait for it to reflect in Facebook and other social media sites which shows a comparison of things and then I buy[...]" [line 8] "Half of my Facebook is basically ads." [line 34]	3a-Targeted ads	67
	RE	"Sometimes you just need to type the CVV numbers, rest of the things are saved in the site already. So you just need to go to the portal type the CVV number and pay. So that's quite scary, I would say[...]" [line 14] "[...] there are options to set your cookie preferences in such a way that your important passwords are not saved. Your banking and stuff shouldn't be saved [...] a lot of friends who do a lot of shopping, 2-3 purchases per day, they don't have the time to sit down and type the number, so they keep it saved. Yeah I won't do that. I'm not saying it's not safe, but for me it's not." [line 22] "[...] you should know where to stop your things being tracked. But certain places you wouldn't know what is being tracked." [line 24] "[...] if you want your cookies not to be tracked or something, you have something called incognito mode, in your browsers [...] That's a measure you can take, there cookies are not tracked." [line 26] "[...] clear your cookies now and then		68

		[...]" [line 40]		
	RF	"[...] you tend to get up these advertisements from products that you've been looking at [...] it can be really annoying. But on the other hand of course the ads are relevant to me because they concern things that I am interested in or have looked at, so it can also work as a reminder to me if I haven't made a purchase yet." [line 18] "I'm not really bothered by the fact that there are cookies, and that I get these pop up ads, because if I want to buy something, then I will buy it, and I just sort of disregard the ad." [line 20]	3a-Targeted ads	69
	RF	"[...] if I'm looking to make a bigger investment which is usually buying a flight ticket, which costs several thousand kroner, then I tend to go incognito, because I don't want the websites to see my interests in certain flights [...]" [line 20]		70
	RG	"I find that personally I like to make a purchase from things that I like, I look through a brochure or catalogue and pick my own stuff. Rather than having it come up [...] like they are being pushed on to you [...]" [line 20] "[...] they give these advertisements every time on social media newsfeeds. And I think that to an extent is annoying [...]" [line 32]	3a-Targeted ads	71
	RH	"I think they are beneficial" [line 26]		72
	RH	"I don't think I would do it voluntar-	3a-Targeted	73

		ily, but I guess they somehow know that anyway." [line 34]	ads	
	RJ	"I usually always remove cookies, so… because you never know what they save about you." [line 22] "Plus when I close my web browser it deletes all cookies." [line 24] "[...] I mean if you get enough information you can like, combine all the information from different sites and get a pretty good picture of who I am. So that's why I delete them, usually." [line 28]		74
	RK	"I mean I'm not a big fan of the fact that your search history is sold to third parties in so many cases. But I generally keep very high security in my browser, so the cookies are cleared." [line 22] "I run add-ons on my browser that deletes them." [line 24]		75
	RK	"I would never sign up for advertisement unless there was some sort of incentive to do so. In that case, I might consider it." [line 26]	3a-Targeted ads	76
	RL	"Even I don't know cookies. I think it's beneficial. Sometimes, my e-mail address is quite long. Maybe I will use cookies in the future." [line 34]		77
	RM	"Yeah, it's convenient. I use cookie all the time. Especially, by Chrome. Since I don't want to type the account again and again. Technically, I can have these information in any computer as long as I log on my Google account." [line 26] "For me. No, I don't need any rec-	3a-Targeted ads	78

		ommendations. Especially, I have bought some products already. The site kept pushing the recommendation info. It's kind of stupid. I prefer to search by myself." [line 28]		
	RN	"For the e-commerce website, I don't know how they use cookies exactly. [...]at least cookies don't cause any problems for me." [line 28]		79
	RN	"To be honest, No. I don't want to share my personal information with the site. But the advertisements always pop up. No matter you provide the information or not. That sucks." [line 30]	3a-Targeted ads	80
	RO	"I want to keep my integrity as much as possible when online." [line 24]		81
	RP	"[...] think it's pretty annoying when it comes up, because before, there were never any problems with visiting a website. So I just think it's annoying that it comes up, you know? Like, "we use cookies". Because I don't see any difference." [line 22]		82
	RP	"[...] sometimes it's just...sometime I get commercial and I press that I don't want to see this commercial." [line 28] (positive towards targeted ads/willing to share)	3a-Targeted ads	83
	RQ	"They would track me. It's like bacteria rather than cookies." [line 18] "Because I want to be completely confidential of who I am. And anyway, they have my account numbers, and I have an account so they don't really need it I would guess." [line		84

		22] "I clear out sometimes, yes." [line 24]		
	RQ	"I want to be alone, I don't want that. I just simply don't want it, I don't like it." [line 28]	3a-Targeted ads	85
	RR	"[...] I personally think this is an advantage of e-commerce. I can totally understand. If you choose e-commerce, you can't avoid this trend. You should do some trade-offs. While, if you really care about your personal information, your privacy. You can always have choices.[...]" [line 16]		86
	RS	"I think they are beneficial but I usually ignore it." [line 26]		87
	RT	"I think it's convenient, but not smart enough. Before I make a purchase, I'd like to receive some recommendations. It's beneficial. But the site keep sending me the ads or recommendations after I bought already. I think it's quite annoying. Some things may not be daily necessities, I only buy it once. It's definitely not a good idea to push me the ads." [line 20]	3a-Targeted ads	88
4- Info Disclosure	RA	"[...] depending on how complicated it is, how much information they want, that could make me hesitate, definitely. [...] depending also on if it's something I can buy anywhere, if I can go to another website [...] and also my mood." [line 34]		89
	RA	"Too complicated, it's too many fields to fill out [...]" [line 38]	4a-Limits	90

	RA	"[...] because you get so much email once you subscribe, so I usually use another email." [line 38] "Several separate emails." [line 40] "[...] all the emails that I don't use anymore. That I still can access if I want to, but I don't have it close to me." [line 42]	4b-False / different information	91
	RB	"I consider myself as looking at information as not an issue, because the more you give about yourself to an e-commerce site, the better your experience will be. [...] As long as they're not acting illegally, or acting unethically about it, then I don't really care.[...] So, there is no limit for me, I think." [line 26] "I would say so, definitely." (in terms of more benefit of disclosure than risk) [line 28]	4a-Limits	92
	RB	"[...] that's maybe a downside for e-commerce and all these platforms [...] you always have to sign up, provide name, phone number, email, I provide my name and stuff like that, but, it's not a fake email it's an email that I created, only for these things. The email account I use everyday, I don't want to get all those advertisements and spam on that, so I have this separate one [...] it gets frustrating and it gets annoying. [...] and I don't check it everyday." [line 30]	4b-False / different information	93
	RC	"[...] it depends on type of website [...] something like eBay for example, if they ask for my credit card information, that makes sense [.... But I don't give them my shipping information because that's something I talk to the seller about.[...] Amazon, I give them all	4a-Limits	94

		the information they need, because they handle the whole supply chain from start to end. So to answer your question, it depends on whether I think they need this information to help me out or not." [line 28]		
	RC	"[...] separate email accounts definitely, especially when it's a brand new website that I haven't been using before. So I make a secondary account with a throwaway email, to explore the site, see how it works [...] if I become comfortable with that then I can delete that account and use my primary email account." [line 30]	4b-False / different information	95
	RD	"[...] if it's something that I think is irrelevant then I won't give it [...]" [line 28]	4a-Limits	96
	RD	"[...] I haven't written my full last name, because my last name, no one else has that, so it's very easy to know who I am [...] always use the same email for purchases, so I get all the advertisements there, but I still use that one." [line 32]	4b-False / different information	97
	RE	"If it's through one of the good sites which is famous, I won't mind sharing my personal information [...] there are some sites which are upcoming and who knows about their security and stuff, so in those places I'm a little doubtful about giving my credentials." [line 28]	4a-Limits	98
	RE	"I won't give my house address I'll give my office address [...]" [line 30] "[...] you keep getting junk mail, too many promotions keep coming, you don't want that to come to your personal mail ID where you have impor-	4b-False / different information	99

		tant mails coming. [...] I personally have another mail ID provided for that." [line 32]		
	RF	"I wouldn't give more details than what I find necessary for a purchase [...] I would just add details that I find relevant to the purchase [...]" [line 22]	4a-Limits	100
	RG	"[...] there is a line when they start asking about bank details especially if you're not making payments with a credit card at that time […]" [line 22]	4a-Limits	101
	RH	"I don't think I would share any information except my address or my phone number. Not my personal number." [line 34]	4a-Limits	102
	RH	"If I was to make a purchase, I would not provide false information." [line 36]	4b-False / different information	103
	RI	"If they specifically say that they are going to sell my information to other websites, then I would think it's too much. But other than that, no restrictions." [line 32]	4a-Limits	104
	RJ	"[...] but I'm guessing like when my habits and my personal stuff like relationships, my health status, health information and stuff like that, when websites start to ask about that I would reject them pretty quickly." [line 32]	4a-Limits	105
	RJ	"Sometimes when I just want to, like, enter a website, and you need to register I just enter some random words pretty much." [line 34]	4b-False / different information	106

	RK	"I don't really have a limit, like it depends from case to case. It's on a need to know basis. So if I think they don't need that information for what-ever I'm doing on their site I wouldn't give it." [line 28]	4a-Limits	107
	RK	"[...] I have a whole separate e-mail address for sites like that." [line 32]	4b-False / different information	108
	RL	"Again, that depends on the website. If the site is originally the online shopping site. I don't really care. I mean that's not important. If I give them my credit card information, I don't think they will give it to the other. As for the basic information, the name, the address, the phone, I don't care that much. If the site is randomly found by me, I will say no." [line 38] "For me, it depends. In Sweden, I will use my real information. In China, my Taobao profile name is "XY" (name masked in order to re-main anonymous). And I always use my company address. If I do have to get something delivered to my home. I usually only give it the name of my residential area." [line 40]	4a-Limits	109
	RM	"For my contact information, I don't want to." [line 32] "In Sweden, it's okay. I will not live here permanently. I just need to clean up my mail box. That's it. But if I am in China, I will not give them. I don't use my real name, my full address. I usually use "ZSF" (real name masked in order to remain anonymous) as online name. As long as I provide a useful phone number, it's ok. As you know, they only check the phone	4b-False / different information	110

		number instead of the ID. Only thing you have to do is telling them the phone number, then you will get your product." [line 34] "Yes, I have several email accounts. But I would use the same one for my all my online shopping. Because, it's too complicated if I used different email addresses. As for the fake name, definitely yes. But it doesn't work in Sweden. I have to show my ID when I pick up my packages. Also, I will not provide my full address. Usually, I don't provide my room number. Only the street name and street number works in China. They will call me." [line 36]		
	RN	"[...] that depends what information. If it's something about the bank account, yeah, the financial information. I will refuse it. Because it's dangerous. I know an example. Some websites ask me binding my credit card. I can't skip it if I want to finish my registration. [...]" [line 32]	4a-Limits	111
	RN	" [...] If it's totally a new site, I just want to use it for once. Because of the good price, or some other reason. I probably will give the fake information. For instance, I will give the fake name but the pronunciation is similar to my real name." [line 34]	4b-False / different information	112
	RO	"[...] my income, and if I have any diseases for example." [line 26] "I try to avoid giving out my social security number. If possible, I try to avoid informing about that." [line 42]	4a-Limits	113
	RP	"Because maybe I don't use that website that often, so I think it's un-	4a-Limits	114

		necessary.” [line 34]		
	RP	“[...] like where I live, only like general things, like if I’m a boy or a girl, because then I won’t get boy stuff. And maybe my profession.” [line 36]	4a-Limits	115
	RQ	“[...] I only give the minimum bare amount of information they would require for the purchase to go through.” [line 32]	4a-Limits	116
	RR	“I am not willing to share my information. I don’t like the ads trash. But I can understand this cannot be completely shielded. In my point view, I don’t want to provide the info.” [line 20]	4a-Limits	117
	RR	“It depends on the privacy level. If asked too specific info, I would refuse. [..] If I think my information security is threatened, I simply will leave the site and try to find a new one.” [line 22] “As for the registration, I only provide my information that is mandatory. For the optional item, I will not fill out.” [line 36]	4a-Limits	118
	RR	“[...] that’s the plan B. As I said, I will not buy it when I feel threatened. If I can only buy it on the untrusted website, I will provide the fake information. Whatever the name, address.” [line 24]	4b-False / different information	119
	RS	“Yes, I will. Some recommendations are even better than what I found. I’d like to get some advertisements. To know more products.” [line 28] “I think I will give all they need. Since I haven’t met the situation		120

		which I have to provide the too personal information. So basically, yes." [line 30]		
	RS	"I will give my real information when I purchase something online. They need my contact info to deliver the goods. As to other purpose, I won't give my info. But I did not give any false or different information before." [line 34]	4b-False / different information	121
	RT	"If I think the site's reputation is not good, or it's a small company, that means I do not know enough about this site, I will not provide with my personal information. For those sites that are not fully trusted, I am not sure if they will sell my information. So I guess I don't have to take these risks." [line 24] "[...] But I know something, you can create the separate account by using some special naming rule. For instance, you can name your Amazon account as [...] As for EBay, you can name is as [...] Then you can exactly know which site send you the spam or which one sell your data or extra.[...]." [line 36]	4b-False / different information	122
5- Payment Info	RA	"[...] depends on the reviews, if I don't know the website in advance. [...] yeah, fairly comfortable, otherwise I will leave the website." [line 44]	5a-Card security protection	123
	RA	"[...] if they use PayPal, or if they use other type of payment methods, because that shows that they are more serious. Or Klarna, it's a company in Sweden that provides credits, billing." [line 46] "If I don't know the website, I prefer	5b-Alternative payment methods	124

		the billing." [line 48]		
	RB	"[...] when you do a purchase, you type in your credit card number, and I assume they keep that, that's probably the most valuable thing I have because that is my money." [line 26] "[...] the security thing on my credit card number, I don't really see it as an issue." [line 32]	5a-Card security protection	125
	RB	"[...] they have this option to pay with credit card, or PayPal, these type of methods, all of them are equally good to me." [line 32]	5b-Alternative payment methods	126
	RC	"I scroll to the very bottom, and [...] the logos for verified by Visa, or Mastercard [...]" [line 14] "[...] if it has all the marks about secure payment, and they've been certified [...]" [line 32]	5a-Card security protection	127
	RC	"[...] see if they have PayPal [...]" [line 14] "[...] some websites have cash on delivery option, so whenever that's available I always use that over credit card." [line 32]	5b-Alternative payment methods	128
	RD	"[...] I didn't want them to save my card information, but the next time I was there they had saved it anyways[...]" [line 28] "[...] if someone would steal my computer, and it has saved my credit card information on my computer, it's very easy to use my credit card [...], for credit card. I would give out the information, but I wouldn't save it [...]" [line 30]	5a-Card security protection	129

	RD	"I like to pay direct [...] if I take an invoice, I don't like that because usually you have to pay extra, and I don't want to pay afterwards.[...] usually I do card, [...] I think it's just a habit, so I haven't really thought about it." [line 36]	5b-Alternative payment methods	130
	RE	"Sometimes you just need to type the CVV number, rest of the things are saved in the site already. So you just need to go to the portal type the CVV number and pay. So that's quite scary, I would say[...]" [line 14]	5a-Card security protection	131
	RE	"[...] cash on delivery, I would prefer that, even if it's a good site I would prefer that." [line 30]	5b-Alternative payment methods	132
	RF	" [...] the secure payment programs working, and sometimes you have to authorize with a code [...]" [line 26]	5a-Card security protection	133
	RG	"[...] option of paying with mobile money, or cash on delivery [...]" [line 24] "I find that mobile payments are safer than credit cards." [line 28]	5b-Alternative payment methods	134
	RH	"I don't think I do, I just write my information, I even have it stored on my Google account". [line 38] "I use my mobile Bank-ID, and that makes me feel safe." [line 52]	5a-Card security protection	135
	RI	"Sometimes I have a password that you have to type in, or I use my Bank-ID, where you have to type in your password in order to proceed with the purchase." [line 36]	5a-Card security protection	136

	RI	“Yes, sometimes I’ve used invoice payments so that you don’t have to pay directly.” [line 38]	5b-Alternative payment methods	137
	RJ	“Well I use my bank thingy (Bank-ID), whatever it’s called. That’s I’m guessing is the most precaution I take because I feel that’s pretty safe. Of course I do like virus scans on my computer pretty often. So I’m guessing that’s also a precaution. But as I said before I think looking up the website and check if it’s reliable or not.” [line 38] “[...] Checking out the website is the most important thing I think.” [line 38]	5a-Card security protection	138
	RJ	“I think I’ve used Swish once, and that’s quite handy I think. But that is the only one I think.” [line 40]	5b-Alternative payment methods	139
	RK	“I mostly use PayPal for payments.” [line 34] “So that the shop will actually never have my payment information.” [line 36]	5b-Alternative payment methods	140
	RL	“Well, I think all these questions are targeted Swedish people. We don’t use credit card for online shopping in China. We use the third party payment. We have WeChat pay, Alipay.” [line 42]	5b-Alternative payment methods	141
	RM	“Well I can only use my credit card in Sweden. I don’t have the Swedish personal number. That means I can’t	5b-Alternative payment	142

		open a Swedish bank card with the function of online transfer. [...] But in China, I can use Alipay. I can pay when my package delivered. I can also ask my friends to help me to pay for it. You must know what I mean. [...] I need to receive the temporary token by message when I use it online. It's safe. I guess." [line 38]	methods	
	RO	"Through Bank-ID." [line 30]	5a-Card security protection	143
	RO	"[...] I prefer invoice." [line 34]	5b-Alternative payment methods	144
	RP	"[...] I don't use my card number, I get a bill instead" [line 42]	5b-Alternative payment methods	145
	RQ	"I do have a software called OneVault, where I keep all my credit card details, and inloggings and everything [...] it's a 32-bit whatever it is to protect it. So it would be very difficult for them to get access. They only get the access to what I provide them so they can't, supposedly not. It's all the inloggings, credit card and everything [...] And the other one is Bank-ID. So when I'm logging in you open up with a long code word. And then you can click on the inlogging and it logs in automatically with your password. And also, when someone does a credit check on me, I get a letter about that." [line 46]	5a-Card security protection	146
	RT	"Not very special, but I would install the anti-virus software, security controls, anti-phishing software in ad-	5a-Card security	147

		vance [...] I usually would check my credit card bill every month. I would contact my bank, once I find suspicious records. But now everything is fine." [line28]	protection	
6-Social Media login	RA	"No, I use email, that I don't use, or Google account that I don't use. [...] I feel like it's a little bit further away from my Facebook profile, which is fairly personal [...] Facebook is me online, and Google account is me a bit further away online." [line 50]		148
	RB	"Yeah I do that. The reason isn't so I sign up with Facebook and they get the data, the reason is because it's quicker. It's the convenience. [line 34] "[...] The only thing that could be an issue, is if they are accessing private conversations, through messenger." [line 38]		149
	RC	"If I become comfortable with it then I can. I would use my Google+ account or gmail account to log in just because it's faster, it's less of a hassle. And I trust those websites so it's fine." [line 34] "[...] my Google account has very basic information, like name, age, country, not the more detailed kind of things that are on Facebook or Twitter." [line 36]		150
	RD	"[...] if they ask me if I want to make a new account or log in with Facebook, I usually make a new account [...] sometimes I click it off, and continue." [line 28]		151

	RE	"[...] I wait for it to reflect in Facebook and other social media sites which shows a comparison of things and then I buy [...]" [line 8] "[...] if that is available then I'll do that." [line 34]		152
	RF	"I usually try to avoid that [...] I sometimes do that if I've forgotten my password to the other account, or if I can't be bothered to make another account [...]more often I create an account [...]" [line 28] "[...] if I use those accounts you are giving the website permission to use information, to use details from your social media account, to direct advertisements and to track your details. And that feels a bit odd." [line 30]		153
	RG	"I just create an account, if I'm going to an e-commerce site I wouldn't prefer to have my Facebook linked to that." [line 30] "[...] they give these advertisements every time on social media newsfeeds. And I think that to an extent is annoying [...]" [line 32]		154
	RJ	"No, as I said before about the marketing stuff, so I try to avoid that." [line 42]		155
	RK	"[...] I know for example that Facebook gathers this information and sells it. And they target you with advertisements specifically for you." [line 42]		156
	RL	"No, I have a separate account. I don't want to use my Wechat account or Facebook account. I think that's		157

		more safe." [line 46]		
	RM	"Sometimes. Sometimes, I am lazy to create a new account. " [40]		158
	RN	"It's convenient. I used my Facebook account and my Weibo account." [40]		159
	RP	"It's easier" [line 50]		160
	RR	"No. No. it is another way to collect more personal information. I do not want to mix the two. Ads every-where. It's quite annoying. No, I will definitely not associate my social media account." [line 30]		161
	RS	"[...] it's convenient. I don't have to type the registration info again and again. And I trust my social media platform as well." [line 38]		162
	RT	"No. No. I want they are completely separated. Because once the shopping site can access to your chats record, it is really dangerous." [line 30]		163
7-Security Controls	RA	"[...]if I order from a Swedish web-site I feel like it's fine, I trust the le-gal aspect of it." [line 22] "[...] the new law now is really good, and the new EU regulation [...] be-cause that is what is needed, because it's not only Swedish. [...] good step towards more privacy online [...] I trust the legal system, I know about it and I trust it." [line 58]	7b-Laws	164
	RA	"No I don't." [line 54] "I haven't thought about it, I didn't	7a-Security features	165

		really know about it either [...]" [line 56]		
	RB	"No, what is that actually, I don't know. No I don't do that, you're actually telling me something new." [line 40]	7a-Security features	166
	RB	"No, I don't [...] I know there are laws in Iceland, that are considered about data and tracking of people's movement on websites, but I don't really know the law.[...] I also that there is the EU, they were setting some new law about data gathering.[...] setting this law where people could actually look at what is being collected [...] I think that's a good evolution, just for the sake of transparency, safety, and feeling secure." [line 44]	7b-Laws	167
	RC	"I scroll to the very bottom, and [...] the logos for verified by Visa, or Mastercard [...]" [line 14] "If the domain is secure with https, then that's more confidence if they have, like when you hover over the https, it shows you what credentials they have [...]" [line 32]	7a-Security features	168
	RC	"I know that Europe has a data protection act [...] I know there is a law, I don't know what it is or what its specific points are." [line 38]	7b-Laws	169
	RD	"You get that little lock, with the colour change. So usually when I pay with my card, I look for that. Other than that, I don't." [line 40]	7a-Security features	170
	RD	"Well I know in Sweden they have this, I think it's called the PUL, it's	7b-Laws	171

		about how they handle my personal information, and also the EU law about where you store data, [...] I'm a bit aware about the Swedish laws, but not any international ones. [...]" [line 44]		
	RE	"I don't check security labels I let the antivirus do it for me." [line 36]	7a-Security features	172
	RF	"[...] when I open up a website, I usually look at signs such as the green padlock for safe website, [...] when you come to the payment stage you can see if they have these certain certifications like safe e-commerce [...]" [line 10]	7a-Security features	173
	RF	"I know that there is Swedish legislation,[...] there is a law on protection of personal information, like your name, your social security number, and so on [...] I'm aware, and I know how to find information if I need it." [line 34]	7b-Laws	174
	RG	"I feel a lot more secure if I see the little green padlock on the side with the https." [line 34]	7a-Security features	175
	RG	"I know there is the data protection act, but I'm not sure as to what extent it really is implied, or enforced [...]" [line 36]	7b-Laws	176
	RH	"Yes, I look for this..I don't know what it's called, there's some kind of certificate." (trygg e-handel) [line 44-46] "To make sure it's not a scam." [line 48]	7a-Security features	177

	RI	“I didn’t even know they existed” [line 48]	7a-Security features	178
	RJ	“[...] I usually look for the https” [line 44]	7a-Security features	179
	RJ	“I only know it in Swedish... Personuppgiftslagen.” (PuL) [line 46]	7b-Laws	180
	RK	“Yea, I also have an add-on which checks the site’s certificate. So if I get any warning I will not make any confidential information entries.” [line 44]	7a-Security features	181
	RK	“[...] I know some general about Europe, mostly about Sweden.” [line 48]	7b-Laws	182
	RL	“Yes, it’s my habit.” [line 48]	7a-Security features	183
	RL	“No, I don’t care of it at all.” [line 50]	7b-Laws	184
	RM	“Yes, I will do that. For the security, that’s the basic check.” [line 42]	7a-Security features	185
	RM	“No, I have no idea about that.” [line 44]	7b-Laws	186
	RN	“No, I don’t know any law in China as well as Sweden.” [line 46]	7b-Laws	187
	RP	“No, but I only use those that I get recommended to use. I don’t use sites that have gotten bad reviews or things I only see on Facebook, because I don’t trust those ads. And usually only companies that have a store.” [line 54]	7a-Security features	188

	RQ	"Yes, "Trygg e-handel", yea, yea." [line 42]	7a-Security features	189
	RQ	"No, I don't know that." [line 44]	7b-Laws	190
	RR	"[...] every time. Every time when I pay online. This is the only thing worthy of me to do. I know the https." [line 32]	7a-Security features	191
	RR	"Totally no idea" [line 34]	7b-Laws	192
	RT	"No. I guess usually, when people have been violated, they will think about the law. Otherwise, no one would pay attention." [line 34]	7b-Laws	193
8-Other Measures	RC	"I have an antivirus program that has a script running inside my browser [...]" [line 42]		194
	RD	"I have a separate password for my email, because if they get a hold of my email they can get my information from all my other accounts, so that's the main thing I do [...]" [line 46]		195
	RE	"[...] have a good antivirus software installed in your system [...]" [line 36]		196
	RF	"I've become aware lately on the importance of having different passwords [...]" [line 36]		197
	RI	"Just to make sure to log out, and that everything is completed before signing off." [line 52]		198
	RM	"[...] Only use your own com-		199

		puter.[...]" [line 46]		
	RN	"I will think about the environment, equipment as well. I will not use the public Wi-Fi when I pay by my credit card. Also, I prefer to use my own laptop or phone to pay [...]." [line 36]		200

Appendix II

Respondent A (RA) – Face-to-face interview

Age: 26; F; Masters student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/19
Start time: 10.07
End time: 10.22

1. **IN: How much time per day do you spend browsing the internet?**
2. RA: Right now, like 8 hours.

3. **IN: How many online purchases have you made in the last 3 months, roughly?**
4. RA: 2. 2 or 3 maybe

5. **IN: How much money have you spent on those purchases?**
6. RA: 3000 maybe (kr)

7. **IN: Okay, now we're gonna move to the factors that influence online shopping choices, what are the main factors for you when you decide which website to use, when you're shopping online?**
8. RA: Can I choose all of them, could you read the choices you have?

9. **IN: We had price, recognition of retailer, delivery time, trustworthiness, convenience and security.**
10. RA: I have some comments on all of them. Price, of course, but it's depending on what you're looking at. Recognition of retailer, important, and you can always Google it, I usually Google it if I don't know about it and read what the other people wrote about it.

11. **IN: You mean like reviews?**
12. RA: Yeah, reviews of the website. In general. So you know that what you ordered has been delivered, and stuff like that. So that is a big thing, if I don't know the retailer in advance. Delivery time, not so much, usually it arrives on time. Trustworthiness goes with recognition, so you can always Google i think that's a really nice thing to do. Convenience goes with every website so it doesn't matter, really, and security, talking about cookies, I've noticed that I kind of reject the websites that are doing that too much, so security in terms of privacy, yeah.

13. **IN: So it's something that you always think about?**
14. RA: Yeah, it's not that prominent, but it exists, usually.

15. **IN: Okay, so the second question was about if you do any type of research, but you already said that you usually Google and read the reviews?**
16. RA: Yeah, some basic research on whether the website is trustworthy or not. And mostly I'm looking for the fact if it's been delivered, if people are happy with the customer service, or if the product looks like it does on the website.

17. **IN: Okay nice. We're going to move on now to privacy policies. Do usually read through the privacy policies on the sites that you use?**

18. RA: No, because it's too complicated, it's nothing for normal people to read.

19. **IN: Okay, that's interesting. So do you think there's anything that can be changed in the format, in terms of language or clarity that will make you want to read them before you do your shopping?**
20. RA: I like simplicity, so the easier it is the better, but still, since it's a lot of information, I understand why it is like it is, but I think I assume that everything looks the same. So if I have read one, yeah.

21. **IN: So you mean from site to site, you feel like it's all the same thing so you feel like you don't need to read?**
22. RA: Yeah, or I assume it's the same thing. But still, if I order from a Swedish website I feel like it's fine, I trust the legal aspect of it.

23. **IN: So, next questions are about uses of cookies and tracking of online behavior. Do you know what the purpose of cookies is, and a general understanding of what they do?**
24. RA: Yeah I would say so. To follow the user, and whatever they do, I guess.

25. **IN: So what's your opinion on cookies, are they useful for you, or is it a nuisance, and extra data?**
26. RA: Yeah, they are two camps, and I have one foot in each I would say. Because I understand the business perspective of it, I think that it's nice, I think you can do a lot with the data that you gather. It's 2017 so you can't turn it back, it is what it is, it's not going to get any less, it's only going to increase. Of course, it's a bit annoying, if you only look something up once, then you get commercials for three years, no but, sometimes it can get too much. But I still see the business perspective of it.

27. **IN: Very diplomatic answer.**
28. RA: But that is because we work with it, so I can see both positive and negative things with it.

29. **IN: So are you willing to provide that information then to websites in order to get personal targeted advertisements?**
30. RA: I'm not willing, but I'm accepting it. I would say that would be more accurate.

31. **IN: Okay interesting. So my understanding of that is that you're not against it, but if you had the choice you wouldn't share that data?**
32. RA: Yeah I would wish for more choices, because now it's in terms of ethics, it's on the business, I don't have anything to say on this question, if I don't accept it I can't go and use the website either way, and that is the problem. We read an article sometime, you should have, one possibility could be that you have your own privacy record, and then the business has to accept that from you. That would mean a lot of work, I know, but still, it's like, because now everyone does it, mentally, so I have to follow the rules, which is using cookies, if I want to use the website. And I don't really like being that dependant, I think they take away a little bit from the customer perspective. It's giving too much power to the business.

33. **IN: Okay, interesting insights. Okay, the next section is quite related to what we've talked about, it's your thoughts about giving up information. When you're asked to provide personal information on a website, are there any reasons that could make you refuse to give out information, and maybe move to another site, or not use that site anymore?**

34. RA: Yeah, it's different perspectives as well, depending on how complicated it is, how much information they want, that could make me hesitate, definitely. And, depending also on if it's something I can buy anywhere, if I can go to another website, and yeah, and also my mood. Mostly like, if you can understand that, I hesitate a little bit, I would rather not leave too much.

35. IN: You mentioned something about if it's too much information, too complicated, then you'd be reluctant to give it.

36. RA: By that I mean if there's too many fields to fill out, or too many steps, or do I have to have a confirmation email, and then go back there, and then go.. Yeah.

37. IN: Okay, so what is the limit for you, where does it become too complicated?

38. RA: Too complicated, it's too many fields to fill out, and also if I have to use, because you get so much email once you subscribe, so I usually use another email, and if I have to go into that email in order to confirm the fact that I have signed up for this website, then yeah, then it's getting too complicated. But that's because I don't want to use my original email.

39. IN: Okay, interesting. The next question is actually about that, if you do provide information, do you sometimes provide different or false information, for example a separate email, or separate card for online transactions?

40. RA: A separate email, yes. Several separate emails.

41. IN: So that's mostly to avoid the "junk" email?

42. RA: Yeah. I would never leave a false email, because that seems, not right. But yeah, all the emails that I don't use anymore. That I still can access if I want to, but I don't have it close to me.

43. IN: Next question, do you have any rules that you put to protect your information when you make payments with credit cards, or are you comfortable paying with credit cards online?

44. RA: I would say depends on the reviews, if I don't know the website in advance. So yeah, fairly comfortable, otherwise I will leave the website.

45. P: Okay, interesting. Have you ever used an alternative payment method, apart from paying with credit card, online?

46. RA: Yeah Klarna. You pay with invoice and stuff, you send the bill, all that. So that is also one thing I look for, if they use PayPal, or if they use other type of payment methods, because that shows that they are more serious. Or Klarna, it's a company in Sweden that provides credits, billing.

47. IN: Okay, would you say you prefer the alternatives, or is it okay with credit card?

48. RA: If I don't know the website, I prefer the billing. But, I don't mind, it's all about looking it up. But once they have Klarna, or any company like that, I feel more secure that they have accepted it.

49. IN: Okay, interesting. Next question, do you log in to e-commerce sites using your social media accounts? For example, a lot of sites let you sign in with Facebook, or Google. Do you do that?

50. RA: No, I use email, that I don't use, or Google account that I don't use. But it still has all my information, either way. It's different because I feel like it's a little bit further away from like my Facebook profile, which is fairly personal nowadays. I feel like Fa-

cebook is me online, and Google account is me a bit further away online. It still has all my information about like gender, and age and stuff like that, but it's a little bit more further.

51. **IN: Okay, nice. Now we have the last section. So, privacy concerns and controls. Do you actively check for secure labels or security features on sites?**
52. RA: What do you mean with that, could you evolve that a little bit

53. **IN: Security features, maybe for example, https instead of http, more secure transfer protocols?**
54. RA: No I don't… I wish I did though, I might start now.

55. **IN: Okay. Is there any reason why you don't check, maybe you didn't know about them, or haven't thought about it before?**
56. RA: I haven't thought about it, I didn't really know about it either. And since I do this Google search if I don't feel like it's transparent, I feel fairly okay. I know that it's not the most secure way, but it's still getting a more comprehensive understanding of the website.

57. **IN: Next question, do you know of any applicable laws that are in place to help you maintain privacy and protect your data?**
58. RA: Yes, do you know about the new Swedish law? I think that the new law now is really good, and the new EU regulation, that is for the EU, because that is what is needed, because it's not only Swedish. And I don't even know if the Swedish companies are placed in Sweden. And since the old one is fairly old, I think this is a good step towards more privacy online, and it's all about defining privacy which is really hard. But the way we are living and using the internet we can. Privacy doesn't really necessarily mean secret. It's just that I know that my information that I give away is secure. But I trust the legal system, I know about it and I trust it.

59. **IN: Okay, now the last question, are there any other measures that you take to keep your information safe when you're browsing e-commerce websites?**
60. RA: No.

61. **IN: Okay, thank you for your time.**

Appendix III

Respondent B (RB) – Face-to-face interview

Age: 24; M; Masters student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/19
Start time: 10.40
End time: 11.08

1. **IN: How much time do you spend browsing the internet, hours per day?**
2. RB: Too much… Probably up to 6 or 7 hours.

3. **IN: How many online purchases have you made in the last 3 months, roughly?**
4. RB: None in the last 3 months, but I did a lot of online purchases back home in Iceland. There you know because it's an island and everything is really expensive to ship the product there, the optimal thing for me to do, or just every Icelandic person to do is to buy online, through Aliexpress or Asos or whatever. So I did quite a lot of online spending back home in Iceland but I haven't done any online spending here in Sweden, yet.

5. **IN: How much money, back in Iceland, would you spend per month shopping online on average?**
6. RB: Let me think a bit... 10,000 ISK (approx 817 SEK)

7. **IN: Okay, so we're going to talk a little bit about the factors that influence your shopping choices online. What is the main factor that you look at when you think about what website to use, for an online purchase?**
8. RB: I firstly look at those websites that have the best price. Iceland has a free trade agreement with China, so I don't pay anything for shipping from China, so I usually first look at Aliexpress, because I know that's a cheap one, and a good way for me to get a range of products at a good price. So I think that's the first factor I look at when I look at online purchasing and where to go. Secondly I look at, I don't consider brands as much as other people but I look at things that I like, and that happens to be maybe brands. So, I don't know, I think these two are the main factors that I look at when I go into online purchasing. The most websites I've used are Aliexpress and Asos. I've used Amazon a few times but not as often as Aliexpress and Asos.

9. **IN: Okay. Next question, do you do any type of research, about a site, before you use it?**
10. RB: No, I sometimes read reviews about products, on the actual website. So if I can see a few reviews that are happy with the product, the quality is good, the shipping didn't take too much time, or anything like that. That influences me, a great deal. But I don't really do all that much of research about the website or about the company, just a little bit, I mean, we all know aliexpress and Amazon and Asos, if I would go on to some other websites, let's say just Boozt here in Sweden, yeah anything else, I don't really make all that much effort to research the company.

11. **IN: Okay. We're going talk a little bit about privacy policies. Do you normally read through the privacy policies?**

12. RB: Never.

13. IN: Is there any reason for that?

14. RB: I mean, who does? I mean, it always comes to these terms and conditions and privacy and all that. I mean, it's so long.. No I don't. And I'm not really scared of anything. What I expect them to do is just to improve my search quality. I don't expect them to take what I do online or where I exit, or to what website i exit to from their website or whatever. I mean, what are they going to do with it? That doesn't matter, I don't see why that should matter.

15. IN: Okay. You said something about policies being too long. So do you think there's something that can be changed in terms of language or clarity, or length, that will make buyers and make them read those?

16. RB: It could, there's so many things that companies need to take into consideration when they do these privacy policies, terms and conditions, but I feel that they could, you know, maybe not shorten it, but keep it in a format that the main points are delivered to the user.

17. IN: So make it more to the point, concise?

18. RB: Yeah, exactly. They don't have to go into any details, but they can say, actually, that this data will be used for this purpose. Like the activity we do here is used for this. We keep track of this or this, or only this. As you see, like those are only three points that only take what, 30 seconds to read. Instead of having this small text and pages and pages. They could do that.

19. IN: Okay, so we're going to talk a little bit about uses of cookies and tracking of online activity. Do you know the purpose of cookies on websites?

20. RB: Yeah, the main parts.

21. IN: So what's your opinion on cookies, are they beneficial for you, or is it an invasion of your privacy?

22. RB: I think it depends on what website we are talking about, I mean if it's an e-commerce website I don't have an issue about that, what I think they do with cookies is just to improve my search quality. And see what things I like and then make suggestions for extra purchases, and I would maybe get advertisements towards myself about things that I like. If it's a website that is not in e-commerce, or you know, just governmental website or whatever, why do they need to track what you do on a governmental website, why do they need to track anything? I think it really depends on the purpose, on what you're going to do with the tracking, with the data. I mean I can see why Amazon, and Aliexpress, and all of these websites do it, because I mean, improving the quality of my experience on their website helps their business, which makes total sense for me.

23. IN: So, my understanding of this is you are willing to provide personal information in order to get targeted advertisements and suggestions?

24. RB: Yeah, definitely. I think that's a good thing, but then again we can also go into more detailed ethical questions, how much is too much tracking? I don't know, I don't see it as an issue, for now, at least.

25. IN: Okay, let's talk a little bit about your thoughts, as a consumer, about giving up information. We've already talked about cookies, now I'll ask, what about personal information, are there any reasons that could make you refuse to give

personal information, on an e-commerce site? What is the limit for you, when giving up information, what is too much information?

26. RB: I don't know actually, I consider myself as looking at information as not an issue, because the more you give about yourself to an e-commerce site, the better your experience will be. I think that's my philosophy at least. So when you talk about too much information, it doesn't really matter. As long as they're not acting illegally, or acting unethically about it, then I don't really care. Because, when you do a purchase, you type in your credit card number, and I assume they keep that, that's probably the most valuable thing I have because that is my money. All of the other information I don't really care about, because what can they do with it? The only thing they could actually take away from me is maybe, charge the credit card, over and over again. But then of course I would notice, that's unethical, and I would sue them. So, there is no limit for me, I think.

27. IN: So what you're saying then is there is definitely more benefit than risk?

28. RB: I would say so, definitely.

29. IN: Alright, interesting. Have you ever been in a situation whereby you've provided fake or different information, for example a separate email account for signing up, or a separate bank card?

30. RB: I do do that actually. Because, that's maybe a downside for e-commerce and all these platforms, for example if you want to get some kind of software, you always have to sign up, provide name, phone number, email, I provide my name and stuff like that, but, it's not a fake email it's an email that I created, only for these things. The email account I use everyday, I don't want to get all those advertisements and spam on that, so I have this separate one, where I sign up for these type of things, which I will use for maybe a month, or six months, I just use that other email. That's maybe a downside to the thing of willingly giving up information about yourself, all this core information, name, email address, address, it's the constant emailing commercial thing, it gets frustrating and it gets annoying. So what I have done is to create this, it's not a fake account but it's my account where I keep all of this and I don't check it everyday. Just sometimes. I have it there so I can have my email account that I use on a daily basis, keep that just for things that I actually, you know am doing right now, like applying for jobs and stuff.

31. IN: Is there any way that you protect yourself when using your credit card online, maybe separate bank card, alternative payment methods?

32. RB: No not really. In Iceland, we have our banks and they give out the credit cards, and it's just usually when you go through a website, and you know on Aliexpress or whatever they have this option to pay with credit card, or PayPal, these type of methods, all of them are equally good to me, but Iceland doesn't have all of those services, like PayPal, because our geographical location is kind of bad, and there have been capital controls, trying to keep the money inside of Iceland, and that means it's harder for us to use services like PayPal. But I wouldn't mind to use those kind of services, because why do they exist? Probably to help people make purchases more efficient, more transparent. I wouldn't mind trying them out. So the security thing on my credit card number, I don't really see it as an issue.

33. IN: Okay, interesting. Do you ever use your social media account to log in to e-commerce sites instead of signing up and creating a new account?

34. RB: Yeah I do that. The reason isn't so I sign up with Facebook and they get the data, the reason is because it's quicker. It's the convenience.

35. **IN: So you don't have to go through all the fields and fill everything separately..**
36. RB: Yeah, that's the reason for me to do it. And also, about the data that they get from signing in with Facebook, it's not really... I mean, I do nothing on Facebook. The things that I do are maybe groups, or I talk to people. Do you know what data they get?

37. **IN: I think they usually get profile information, friends list..**
38. RB: Yeah, that doesn't matter to me. The only thing that could be an issue, is if they are accessing private conversations, through messenger. But I don't believe that, that would be some kind of unethical thing to do. So signing in with Facebook or Google, it doesn't really matter.

39. **IN: Okay, interesting. Next question. Do you ever check for secure labels or security features on websites, for example https transfer protocols?**
40. RB: No, what is that actually, I don't know. No I don't do that, you're actually telling me something new.

41. **IN: Okay, do you know of any applicable laws that are in place to help you maintain privacy and protect your data?**
42. RB: No, I don't, but I know there are laws in Iceland, that are considered about data and tracking of people's movement on websites, but I don't really know the law. I should maybe go and read it. I know there is a law, at least. I also that there is the EU, they were setting some new law about data gathering.

43. **IN: Yeah, the EU data protection act.**
44. RB: Okay I think that's actually a pretty good involvement with data gathering, because everything is getting so much data involved, every company is involved in all of it. The amount of data is growing exponentially, so setting this law where people could actually look at what is being collected on this company and this company and this company, I think that's a good evolution, just for the sake of transparency, safety, and feeling secure. There's probably a lot of people for example that feel like I can't use Facebook, because they're watching me all the time. I mean of course it's not true, they are just tracking you to maybe improve the experience of your usage of it, but people are paranoid. So I think this could be a good evolution, for getting this discussion about data gathering more on the right track.

45. **IN: Okay, interesting. I have just one more question, is there any other rule that you have to keep your information safe, that you might not have already mentioned?**
46. RB: No, not really.

47. **IN: Okay, thank you for your time.**

Appendix IV

Respondent C (RC) – Face-to-face interview

Age: 24; M; Masters student; Intermediate to expert IT knowledge.

Place and date: Lund, 2017/04/19
Start time: 12.01
End time: 12.17

1. **IN: How much time do you spend browsing the internet, hours per day?**
2. RC: Most of the day, I'd say somewhere around 11 hours, I'm basically connected to the internet all the time.

3. **IN: How many online purchases have you made in the last 3 months?**
4. RC: I guess around 5-6. Maybe 7.

5. **IN: And roughly how much have you spent on those?**
6. RC: I'd say around 2000-2500 SEK.

7. **IN: Okay, so we're going to talk a little bit about the factors that influence online shopping choices, the choice of retailer and information disclosure. What are the main drivers for you, when you decide what website to use, is there anything in particular you look for?**
8. RC: I go for the websites that I've used before mainly, so stuff like Amazon, eBay, there's this Japanese website called Rakuten. If I don't find anything on that then I go to the second hand websites, like blocket or craigslist.

9. **IN: Okay. Do you think about things like trustworthiness, and security, when you look at these sites?**
10. RC: Yeah, that's mainly why I go to, my first choices, I've used them before and haven't had any issues, and they have security measures in place, in the case of Amazon for example if you don't get what you asked for, you can get back to customer service and they'll refund you.

11. **IN: So the familiarity of these websites makes you trust that you'll get what you need, and your information will be secure?**
12. RC: Yeah, exactly. And to build on that, the secondary websites that I go to, especially craigslist, you always take a risk with that, because it's a random person posting on a random website, so it's hard to build trust on that.

13. **IN: Okay. So when you're using a new site, do you do any type of research before you make a purchase?**
14. RC: When I go to a new website, I scroll to the very bottom, and see if they have PayPal, and the logos for verified by Visa, or Mastercard, that kind of stuff, to see firstly will they even accept my money or not. And I try to see if someone else has used it, like I'd hop on Reddit and see if people have used this, their opinions on it, and if that was good, then I go back to the website, maybe do my purchase then. And the website's overall look. If it looks nice, and appealing, that encourages me a bit more.

15. **IN: That's interesting, that the aesthetics also play a role. Let's talk a little bit about privacy policies. When you use e-commerce websites, do you usually read through the privacy policies?**
16. RC: As a consumer, no. I have never done that. They're just too long and they try to be specific, but they end up being vague because of the legal terms and that kind of thing they use, and I don't find them to be useful, to be honest.

17. **IN: Okay. You mentioned the length and the language, do you think if that is changed then it will be easier for users to understand?**
18. RC: Definitely, without a doubt. If they change the privacy agreement to like a short video, or infographic, or something like that, I'm more likely to see it than just a wall of text.

19. **IN: So something a bit more interactive?**
20. RC: Exactly, no one wants to read half a book before buying something that's worth $10 or something.

21. **IN: Okay, so we're going to talk a little bit about use of cookies and tracking of user activity. Do you know the purpose of cookies on websites?**
22. RC: I know they exist and they are stored on my machine, and they can send back to whoever gave me that cookie, some of my usage, some diagnostics about my device, something like that, like the websites I went to after theirs, and stuff like that.

23. **IN: So what's your opinion on cookies, are they useful, or is it an invasion of your privacy?**
24. RC: My opinion is think is unpopular about this, I really don't mind them, some people think it's an invasion of privacy and that these companies know all of these things about me that I don't want them to know, and I can see that and respect that but I think it's fine, we go into a mutual agreement, you provide me a service and in turn I give you something back. And it makes my life a bit easier so, Amazon, I know they use cookies and their cookies are very invasive, but at the end of the day they give me recommendations for products that I actually want. So I really don't mind them.

25. **IN: So, what you are saying is you are willing to provide personal data in order to get tailored advertisements and suggestions?**
26. RC: Exactly. But I need to know that they're using cookies. So tell me that you're going to be collecting cookies, I never read what they're collecting but I just need to be informed beforehand, and then I accept it and continue using.

27. **IN: Okay, that's pretty interesting. Let's talk a little bit about your thoughts, as a consumer, on giving up information. Have you come across a scenario where a website requests personal information, but you refuse to give it? What is the limit for you, what you're willing to disclose? How much data are you willing to provide in order to use the website and make purchases?**
28. RC: I think for me it depends on type of website, so a website like craigslist that just connects to people, they don't need to know my address and postcode and definitely not my credit card information. But something like eBay for example, if they ask for my credit card information, that makes sense, because I need to be able to place bids and that kind of thing. But I don't give them my shipping information because that's something I talk to the seller about. EBay has nothing to do with that. Amazon, I give them all the information they need, because they handle the whole supply chain from

start to end. So to answer your question, it depends on whether I think they need this information to help me out or not.

29. **IN: Alright, interesting. Have you ever been in a situation whereby you've provided fake or different information, for example a separate email account for signing up, or a separate bank card?**
30. RC: Never bank cards, because I'm from Egypt, and back home the process to get a bank card is long and annoying. But separate email accounts definitely, especially when it's a brand new website that I haven't been using before. So I make a secondary account with a throwaway email, to explore the site, see how it works, what kind of stuff do they send me, and if I become comfortable with that then I can delete that account and use my primary email account.

31. **IN: I'm going to ask about online payments with cards, are there any measures that you have to protect yourself when making payments? Maybe using alternative payment methods, or is there something you look for before you make a payment that makes you feel like it's a secure payment?**
32. RC: Yeah, like I said before, if it has all the marks about secure payment, and they've been certified and all that stuff. If the domain is secure with https, then that's more confidence if they have, like when you hover over the https, it shows you what credentials they have and if they have that I become even more confident, then I can use my credit card. But then, at least back home, some websites have cash on delivery option, so whenever that's available I always use that over credit card, just because in Egypt we don't have a big online shopping culture.

33. **IN: Okay, interesting. The next question is about logging in to e-commerce sites with social media accounts. Do you do that, or do you create new accounts?**
34. RC: It depends on if it's a secondary website like craigslist, then no, because I don't want that to be linked back to me for whatever reason. If I become comfortable with it then I can. With websites like Amazon, EBay etcetera, I would use my Google+ account or Gmail account to log in just because it's faster, it's less of a hassle. And I trust those websites so it's fine.

35. **IN: So you don't mind them having access to your social media data, when you sign in?**
36. RC: That's why I use my Google account, not Facebook. Because my Google account has very basic information, like name, age, country, not the more detailed kind of things that are on Facebook or Twitter.

37. **IN: Okay, so we'll talk a bit about privacy concerns and controls. You already told me you check for secure labels, things like https security features. Do you know of any applicable laws that are in place to protect your data as a user?**
38. RC: I know that Europe has a data protection act, and some of the websites have for cookies, they say in accordance with Europe's something, I know there is a law, I don't know what it is or what it's specific points are.

39. **IN: Okay so you're aware of the existence, but not the specifics.**
40. RC: Yeah, I never needed to, hopefully I never will need to.

41. **IN: Okay, to wrap up, is there any other measure that you take to protect your privacy on these websites that you might not have already mentioned?**
42. RC: Yes, I have an antivirus program that has a script running inside my browser, and that tells me if there are any cookies that are tracking my movement on that website.

So sometimes I check that, to see if there is anything apart from that website's specific cookies tracking me, for example if I'm on Amazon, I click on that script, it tells me okay, the cookie that is tracking you is from Amazon, if there's something else there, then I'd leave the browser, clear my cookies and then go back, before making a purchase.

43. **IN: You mentioned that you'd go back and clear your cookies, do you do that often?**
44. RC: Only when I find a cookie that I don't recognize or that I'm suspicious of, but very rarely do I actually do that. The last time I cleared my cookies was maybe three months or four months ago.

45. **IN: And what antivirus software did you say you use?**
46. RC: It's Avira, the free version they have.

47. **IN: Okay, thank you very much for your time. This was very useful.**
48. RC: Yeah anytime. If you have any follow up questions please feel free to contact me.

Appendix V

Respondent D (RD) – Face-to-face interview

Age: 24; F; Masters student; Expert IT knowledge.

Place and date: Lund, 2017/04/20
Start time: 15.11
End time: 15.25

1. **IN: How much time per day do you spend browsing the internet?**
2. RD: 10, at least.

3. **IN: How many online purchases have you made in the last 3 months, roughly?**
4. RD: 10, maybe.

5. **IN: How much money have you spent on those purchases?**
6. RD: Does travelling count, because then it is a lot. It's a bit higher, these last three months because I travelled, so usually it's not that much. Maybe between 5000-7000 SEK, but that's because I travelled, so that's about half of the expenses. A normal three months, maybe 2000-4000.

7. **IN: Okay, I'm going to ask you a bit about the factors that influence your online shopping choices, what is the main driver for you when you decide which web-site to use, are there any factors you look for?**
8. RD: How cheap the website is, of course, and also if it's a known website, and if a friend has shopped there. But I mainly buy clothes. So the main factor is how nice are the clothes.

9. **IN: Okay, so personal preference?**
10. RD: Yeah, but I usually don't just go to one website, I usually do a lot of research be-fore, or maybe if I'm going to buy makeup I look at reviews on YouTube, before I buy them, and buy them on the same website as they bought them.

11. **IN: Okay, so do you do some research about the site, if it's a completely new site that you've never used before?**
12. RD: Yes, if it's an international site, I usually do that, well, if it's a new site that I ha-ven't shopped before, I usually turn to YouTube, a lot, and online they have a lot of reviews. So I usually look for did they get the package, is the quality really bad, some-times with the cheap clothing sites, they say don't buy from here it's really bad quality, so I usually look up things like that. I don't look up maybe the website itself, how they handle information and stuff like that, I usually don't.

13. **IN: So it's more the product reviews then?**
14. RD: Yeah and the shipping, and stuff like that.

15. **IN: Alright. The next questions are about the privacy policies. Do you ever read through the privacy policies on the sites that you use?**
16. RD: No. I want to say yes, but I don't.

17. **IN: Is there a reason for that?**
18. RD: It takes too long. I think I've done it sometimes, if it's a new site and it's a bit sketchy, like I don't know it, then maybe I'll look into it more, but usually no.

19. **IN: Okay. So you said that the privacy policies are too long, it takes a lot of time, do you think there's something that can be changed, in terms of language or clarity that will make it easier for people?**
20. RD: Absolutely, if there was like a summary in the beginning with a short bullet list maybe, or something like that, with a statement about we do this and we do that, and then a longer explanation further down maybe. And also in language, if it's too difficult to understand then you won't read, two sentences and then you won't bother.

21. **IN: I'm going to ask you about cookies and tracking of online behavior. Do you know the purpose of cookies, are you familiar with what they are?**
22. RD: Yeah

23. **IN: So what's your opinion on cookies, are they a benefit, or do you think it's invading privacy?**
24. RD: Both. I don't like it, because if I look at shoes, the second I go into Facebook I have the same shoes on the side. I know the reason why they are there, and I don't like it, but I usually fall for it, so I mean, it works. And I understand the purpose of it, it could be useful. When I look for jobs, or apply for jobs, it was very good, because then I got like, job offers, that I hadn't heard of, that was really good. But at the same time I don't like them, I know that they have all this information about me, I don't like it. So I wish it was more easy to decline the use of cookies. Like today usually you can't, if you surf on this website, you accept cookies. I don't like that, I want to have like, no I don't want to use cookies but I still want to use your website, option, but usually, there isn't one.

25. **IN: So would you say are you willing to provide personal information then to websites in order to get targeted advertisements?**
26. RD: I may be not willing, but I am willing since I'm doing it. I mean, I could not shop online, and they wouldn't get the information, so I guess, I'm not excited about it, but otherwise I wouldn't be able to use the websites.

27. **IN: Okay, interesting. The next few questions are about your opinions about giving up information. When you're asked to provide personal information, are there any reasons that could make you refuse to give it out, is there a limit that you set for yourself?**
28. RD: Usually, if they ask me if I want to make a new account or log in with Facebook, I usually make a new account. Because I know, like sometimes on Facebook as well, they ask you, to use this, we have to get some information about this and this, and sometimes I click it off, and continue. So there is a limit, I don't know what the limit is, but if it's something that I think is irrelevant then I won't give it. I try to not give out so much information, but then I know I can't "win" against them. A funny fact is that on EBay, I bought some things on EBay, and I clicked in that I didn't want them to save my card information, but the next time I was there they had saved it anyways. And I was very aware that I clicked "No I don't want you to save this information", and I've done that every time, but they still save it. And I don't like that.

29. **IN: So if I understand this right, the credit card information is where the most valuable information is for you?**

30. RD: Yeah I would say so. And also because, if someone would steal my computer, and it has saved my credit card information on my computer, it's very easy to use my credit card. So usually, it's not just to leave out the information, but also actually saving it on my computer, or on a website, because I'm logged in, on the website, so if you get a hold of my computer then you can just buy stuff. So yeah, for credit card. I would give out the information, but I wouldn't save it.

31. IN: Okay. Have you ever provided different or false information to sign up for a website, for example a separate email, or separate bank card?

32. RD: Yeah I've done that actually, I haven't written my full last name, because my last name, no one else has that, so it's very easy to know who I am. So, sometimes. Mostly not, but for some websites I did, and also I always use the same email for purchases, so I get all the advertisements there, but I still use that one.

33. IN: What about bank card, do you have a separate one for online purchases or is it just your regular card?

34. RD: No it's my regular card.

35. IN: Okay, nice. So how do you protect your information when making online payments with cards, you had mentioned when you used eBay you clicked that you didn't want it saved, is there anything else, alternative payment methods?

36. RD: I could do that, but I like to pay direct. And usually if I take an invoice, I don't like that because usually you have to pay extra, and I don't want to pay afterwards. I want to pay right away, because otherwise then I get an invoice, like oh right, I forgot about this, but I don't have money left. So usually I do card, I could do bank as well, but usually I don't do that. I think it's just a habit, so I haven't really thought about it.

37. IN: Okay. So it's more convenient in that way, for you?

38. RD: Yeah, exactly.

39. IN: Okay, nice. So next we're going to talk about privacy concerns and controls. Do you ever check for secure labels or security features on the websites?

40. RD: Sometimes, when I do card payments. You get that little lock, with the color change. So usually when I pay with my card, I look for that. Other than that, I don't.

41. IN: Okay, so just when you're doing the payment itself, not when you're browsing for products?

42. RD: Yeah.

43. IN: Next question, do you know of any applicable laws that are in place to help you maintain privacy and protect your data?

44. RD: Well I know in Sweden they have this, I think it's called the PUL, it's about how they handle my personal information, and also the EU law about where you store data, I don't know if it's valid yet, but I know they talked about it. I guess also in Sweden you can't save information, like personal information, about like politics, or religion, in a list, and I'm a bit aware about the Swedish laws, but not any international ones. But I usually shop from international websites as well.

45. IN: Okay, the last question, are they any other measures that you take to keep your information safe that you haven't shared already, anything else you do?

46. RD: I have a separate password for my email, because if they get a hold of my email they can get my information from all my other accounts, so that's the main thing I do, other than that, no.

47. IN: Okay, thank you very much for your time.

Appendix VI

Respondent E (RE) – Face-to-face interview

Age: 30; M; Masters student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/21
Start time: 13.31
End time: 13.51

1. **IN: How much time per day do you spend browsing the internet?**
2. RE: All of the awake hours, most of the time I'm on the system, Facebooking or checking news, seeing if some ads have popped up that help me in shopping, so out of 24, at least 10 hours minimum.

3. **IN: How many online purchases have you made in the last 3 months?**
4. RE: None, but before I came for my education in Sweden, I've done a lot of online shopping, back at home. Electronics, sometimes food and groceries, clothes, books.

5. **IN: On average, in a month, how much would you spend on online shopping?**
6. RE: Around 10,000-20,000 INR. Less than 20,000. (approx 1390-2780 SEK).

7. **IN: We're going to talk a bit about the factors that influence your online shopping choices, what is the main driver for you when you decide which website to use for online shopping?**
8. RE: I basically don't do online shopping as online shopping, what I do is I go check things out. I check things out and I wait for it to reflect on my Facebook or any social media website. So that they come back with good prices. And based on that I do my shopping. I don't go thinking I want this and I'll buy this, because that's when you don't get good offers maybe. And maybe you're on a site which doesn't have good offers. So what I do is I'll go check it out on some few sites, for example in India we have Flipkart and Myntra, which are for basically for clothes and electronics and stuff. So I go there if I'm looking for something to buy, like electronics, I go there and check out the laptop, I don't shop at that time. And I wait for it to reflect in Facebook and other social media sites, which shows a comparison of things and then I buy. I bought my cell phone also online this way.

9. **IN: So you mean you wait for the targeted ads to show up, and then shop based on that?**
10. RE: Yeah. It does a lot of comparison, it shows you reduced prices, and I check for reviews as well. Reviews are very important, because there was a time in India when there was a company called Snapdeal, there was a major blunder which they did and there was some chap who ordered a cell phone, but he got delivered a brick, in a box. So Snapdeal's reputation went for a toss with that, people stopped buying there. So reviews are very important, if you go to Snapdeal you'll find negative reviews, but they have really cheap prices so it's a chance people take. So the crappy stuff like things which you want to throw off in like six months or something, people might buy there. But the pricey stuff, the good stuff they go into a good website.

11. **IN: So it's kind of like a trade off between risk and benefit then**
12. RE: Yeah, so when they want a pricey and good stuff that they want to keep for some time then they go into the good websites. If they want the price to be low and the item to be thrown away in a few months then they go for cheap. At least I do that.

13. **IN: Okay, so you talked about targeted ads that come up, and the price comparisons, so when you find a new site that you want to use from there, that you haven't used before, do you do research about it? You said you read reviews, is there anything else you do?**
14. RE: I read reviews, I ask friends who have done shopping from there, I generally don't go into sites which are not that famous. Because I've had this experience, well not me but a friend of mine who did shopping in a new venture called Shop Close, there were some issues and her targeted mail was going to some other person. And there was a big issue there. She was getting mails of that person, he was getting her mails, he kept forwarding it to her. She tried to change it and call them but nothing helped, to the point that she had to change her bank account and all. Not that money was going, but she was scared. Sometimes you just need to type the CVV number, rest of the things are saved in the site already. So you just need to go to the portal type the CVV number and pay. So that's quite scary, I would say. After that episode at least I have stopped, I've never shopped on small sites, but after that I've sealed the deal and never done that. Not worth the risk.

15. **IN: Okay nice. The next thing we're going to talk about is privacy policies. Have you ever read through the privacy policy before using a site?**
16. RE: No, if it pops up then maybe the first three lines, maybe the headings, but not like, okay I'm going to do shopping here so I need to read through the privacy policy, never done that.

17. **IN: Is there any reason for that?**
18. RE: I would say it's a waste of time. First thing, I do shopping in places where I'm confident of. And I'm confident that they would have privacy policies there that wouldn't affect me pretty badly in any way. So I wouldn't completely read through everything. But I would sometimes see the headings, sometimes it's a complete scroll down, before you click the check box and submit, so just the headings to see what they are talking about or something, and if I'm bored, maybe. Not if I'm in a hurry to buy something, I won't read through it.

19. **IN: Do you think there's anything that can be changed in the format, in terms of language or clarity to make it more appealing for a user to read?**
20. RE: It's supposed to be long and lengthy, as far as I know they provide the headings in bold for you to understand more, and it's in bigger font. When any document is given to you which is lengthy you wouldn't read through it. You'd just go through the headings and you might sign saying yeah, I'm done. I wouldn't be able to comment on that because I'm not sure what they can change in that, but as far as I know at least the good sites are okay with privacy policies. Yeah there's a lot of breaching of privacy and stuff like that. But yeah if it helps 100 people, it might cause trouble to one person, it's something that's inevitable I feel, at least.

21. **IN: So, next questions are about uses of cookies and online tracking. Do you know what the purpose of cookies?**
22. RE: Yeah one thing is to track your movements, from your IP address, at least in workplaces, a lot of passwords need to be saved in your system, because it changes from one thing to another, you just need to know what things need to be saved and

what things shouldn't be saved. So there are options to set your cookie preferences in such a way that your important passwords are not saved. Your banking and stuff shouldn't be saved, as far as I know, because if just entering a three digit number is going to take you to a purchase, then you should be careful of that, your 16 digits should be with you, not with anybody else. I have a lot of friends who do a lot of shopping, 2-3 purchases per day, they don't have the time to sit down and type the number, so they keep it saved. Yeah I won't do that. I'm not saying it's not safe, but for me it's not.

23. **IN: So what you mean by that is that cookies are useful, but only to a limit?**
24. RE: Yeah you should know where to stop your things being tracked. But certain places you wouldn't know what is being tracked.

25. **IN: So, as you said before, you are willing to provide personal information then to websites in order to get personal targeted ads?**
26. RE: Yeah, it's through cookies. They track where you've been and what you're doing, and if you want your cookies not to be tracked or something, you have something called incognito mode, in your browsers, you can go through that. That's a measure you can take, there cookies are not tracked. Even browser history is not tracked in incognito mode.

27. **IN: Okay, the thing we'll talk about is your opinions about giving up information. When you're asked to provide personal information on a website, are there any reasons that could make you refuse to give out information, or set a limit as to what you will give?**
28. RE: Yeah, it depends upon which site it is again. If it's through one of the good sites which is famous, I won't mind sharing my personal information, my address and stuff. Whereas there are some sites which are upcoming and who knows about their security and stuff, so in those places I'm a little doubtful about giving my credentials. In spite of them having good offers, I wouldn't shop there because you don't know. You're giving your address and you're giving your personal stuff from your system, and for things to be delivered you give your address as well so I wouldn't take a risk on that.

29. **IN: Okay, that's interesting. So, if you do provide information to an ecommerce site, do you sometimes provide different or false information, for example a separate email, or separate card for online transactions?**
30. RE: If I'm buying from a not so trusted, upcoming one, you can't give a wrong bank ID, but maybe I can give cash on delivery. You needn't provide bank credentials with cash on delivery. The second thing I'll do is that I won't give my house address I'll give my office address. So it comes to my office and I take it home. One of the reasons I give my office address is because I've been in the office more than at home, and they deliver from 10-5 or something like that, not after 5 or 6, so I won't be at home at that time. So giving my office address is a better option, for convenience sake rather than safety, but yeah safety also plays a role in it. And cash on delivery, I would prefer that, even if it's a good site I would prefer that. I'm not sure if in Sweden they have that since everything is online, but in India we have the option of cash on delivery.

31. **IN: What about email address, do you use the same one for subscribing to these sites?**
32. RE: I have a separate one. One bad thing about this is you keep getting junk mail, too many promotions keep coming, you don't want that to come to your personal mail ID

where you have important mails coming. So you have another mail ID provided for that, I personally have another mail ID provided for that.

33. **IN: Okay, interesting. Next question, I think you've already answered this before, do you log in to e-commerce sites using your social media accounts, for example Facebook account?**
34. RE: There are certain sites that will require me to create an account for them, then there are some that have a pop up that says log in with Google or Facebook, if that is available then I'll do that. That's when it will reflect in Facebook as well, the promotions and stuff. Half of my Facebook is basically ads. And not only online purchase, sometimes booking flights, even that comes up. That is 100% a benefit.

35. **IN: Okay, nice. Now we'll talk about privacy concerns and controls. Do you actively check for secure labels or security features on sites, such as https?**
36. RE: Yes, particularly in the banking sides I check, and on the ecommerce side as well I check, https is one important thing that you need to check. If you have a good anti virus software installed in your system, they do it for you, like if you go into a site that has a lot of malware and downloads stuff into your system, that will prevent you from going into those sites. Like for example I have an experience where I saw a link, which showed a good offer for something I was going to buy, I clicked on it and before it went, it said this page will be harmful, so I don't even try to go there. Personally I don't check security labels I let the antivirus do it for me, and a good antivirus should do that for you as well. Unless they are dedicatedly trying to rob you, I'm not sure if any sites are there like that. You can get a lot of mail promotion from things like that, never open that. A lot of malware locks into your system, which is even worse than cookies, keeping track of every movement that you make. And that's not needed for you. That's a complete invasion of privacy, not by the good ones, by the illegal bad ones. So stay clear of that.

37. **IN: Next question, do you know of any applicable laws that are in place to help you protect your privacy and protect your data?**
38. RE: Laws.. Nope.

39. **IN: Okay, now the last question, are there any other measures that you take to keep your information safe when you're browsing e-commerce websites?**
40. RE: Yeah trusted websites, cash on delivery as much as possible, and clear your cookies now and then. Keep it cleared sometime for a month, or three months, clearing cookies might help.

41. **IN: Okay, thank you for your time, this was very useful.**

Appendix VII

Respondent F (RF) – Face-to-face interview

Age: 23; F; Masters student; Basic to intermediate IT knowledge.

Place and date: Lund, 2017/04/23
Start time: 22.13
End time: 22.30

1. **IN: How much time per day do you spend browsing the internet?**
2. RF: 2-3 hours.

3. **IN: How many online purchases have you made in the last 3 months, roughly?**
4. RF: I'd say around 10-15.

5. **IN: How much money have you spent on those purchases?**
6. RF: Around 5000 SEK.

7. **IN: Okay, now we're going to talk about the factors that influence online shopping choices, what is the main driver for you when you decide which website to use, when shopping online?**
8. RF: I usually use online stores which I'm familiar with, that I know of because of their quality and they are reliable, like usually if I look for clothes then I have a certain number of websites which I look at. And yeah, previous experience, good reviews.

9. **IN: If you're using a new e-commerce site, do you do any type of research about it, before you use it?**
10. RF: No I wouldn't say that I do pre-research per se, but when I open up a website, I usually look at signs such as the green padlock for safe website, that symbol, and if I'm going to make a purchase, usually when you come to the payment stage you can see if they have these certain certifications like safe e-commerce, and five star ratings, and so on. So that usually helps me to get an idea. I tend to become a bit suspicious if I'm thinking of buying something from a website which doesn't signal those certifications.

11. **IN: Okay nice. We're going to talk a little bit now about privacy policies. Do usually read through the privacy policies on the sites that you use?**
12. RF: No, I know that I should, but I think, just as most people, you don't look through because it's long and you don't have the time. And I guess that I just assume that the details put down there are details that I'm aware of or that I would agree with. So it's based on previous experience and what I assume, that I feel safe within the website in itself, and the company. That makes me less vigilant.

13. **IN: Okay, that's interesting. So do you think there's anything that can be changed with the format, in terms of language or clarity that might influence you to read through them?**
14. RF: Maybe they could have a summary or something, like you have the terms and conditions and policies available, but before that there is a summary of a couple of points, the most important things. It still doesn't help you, because if you haven't read

the terms and there is a breach, then you can't claim your rights. But at least it could help you orientate and look for more details if you're interested.

15. **IN: Okay interesting insights. We'll talk a bit about the use of cookies and online tracking. Do you know what the purpose of cookies is?**
16. RF: Yes, I think cookies are, I can't exactly what they are, but they collect, or trace your pattern, your choices, and your clicks on the website, and they see what you've looked at, and with that information, companies can allocate advertisements directed to you because they know, they base it on your history.

17. **IN: So what do you think about cookies, are they useful for you as a consumer, or is it invasive?**
18. RF: I think both, it's negative in the sense that it's very obvious when you go onto Facebook or some other website that you tend to get up these advertisements from products that you've been looking at, and then you know that the cookies have been used to trace my interests, and it can be really annoying. But on the other hand of course the ads are relevant to me because they concern things that I am interested in or have looked at, so it can also work as a reminder to me if I haven't made a purchase yet, like "oh yes that item was interesting, I'll go back and look at it". So I'd say both.

19. **IN: So as I understand this, for you as a consumer, you are willing to give out personal information to websites in order to get targeted advertisements, then?**
20. RF: Yes and no, I think that my approach is that when it comes to for example clothes, shoes, items of fashion that I usually buy on the net, I'm not really bothered by the fact that there are cookies, and that I get these pop up ads, because if I want to buy something, then I will buy it, and I just sort of disregard the ad when it pops up, if it's an item that I looked at and don't want it, so I kind of source it away, concentrate on what I'm doing. But it depends on what I care about, what I find important, for example if I'm looking to make a bigger investment which is usually buying a flight ticket, which costs several thousand kroner, then I tend to go incognito, because I don't want the websites to see my interests in certain flights, and that can help to not trigger the prices because they will rise if I keep browsing the tickets non-incognito. So I'd say it boils down to what matters to me.

21. **IN: Okay. The next few questions are about your thoughts on giving up personal information. When you're asked to provide personal information on an ecommerce website, are there any reasons that could make you refuse to give out information, or set a limit as to what you want to share?**
22. RF: When I make a purchase I have to fill in my name, my address, my credit card number, but that is in the payment part in the authorization of payment phase, and I look at the green symbol or the lock and secure commerce signals. Of course, like I wouldn't give more details than what I find necessary for a purchase. To make a purchase I have to give up my address, my name, my number, my email address and my credit card number, because those are obvious pieces of information that they need, for the transaction to go through. But if they ask, maybe also because I'm a woman, not often but sometimes websites ask "are you a man or a woman", I don't think I've seen that so much, and if it does occur then it's usually optional, it's not a red asterisk, it's not obligatory to add. So I think that I would just add details that I find relevant to the purchase. It depends on what I'm doing, if I'm filling in a survey for a thesis, or if I'm buying a pair of shoes, so I think I'm sensitive to what it concerns.

23. **IN: Okay, interesting. The next question is, if you do provide information, do you sometimes provide different or false information, for example a separate email address, or used a fake name, or separate card for online transactions?**
24. RF: No not that I can recall.

25. **IN: Okay. The next question is about how you protect your information when making online payments with credit cards, you already talked about looking for the secure labels and certifications, is there anything else that you do?**
26. RF: I think that's mainly it. It feels safe to use certain websites because when you go through the payment process you see how they have like the secure payment programs working, and sometimes you have to authorize with a code, so like I said before it depends on those symbols, those signals of safe commerce. Right now I can't really think of anything else.

27. **IN: Okay, interesting. Next question, do you log in to e-commerce sites using your social media accounts? For example, a lot of sites let you sign in with Facebook, or Google. Do you do that, or do you create separate accounts?**
28. RF: It's happened a few times, but I usually try to avoid that. What happens is that I sometimes do that if I've forgotten my password to the other account, or if I can't be bothered to make another account. It happens once in a while, but more often I create an account or if I forget my password I ask for a new, request for a new password.

29. **IN: Is there a reason for that, for why you don't feel as comfortable logging in with Facebook or Google+?**
30. RF: It feels like if I use those accounts you are giving the website permission to use information, to use details from your social media account, to direct advertisements and to track your details. And that feels a bit odd, for example if you're going to buy a pair of shoes, then it feels a bit odd to log in with your Facebook account. So I prefer to create an account, I usually do that. But once in a while for different reasons, I get lazy, or I get the feeling that I can't login in any other way, they don't provide me with an option, that has also happened a few times. Or maybe I'm blind to the other option.

31. **IN: So it becomes more because of the convenience of it?**
32. RF: Yeah. Because of the convenience.

33. **IN: Okay. Next question, do you know of any applicable laws that are in place to help you maintain privacy online and protect your data?**
34. RF: I know that there is Swedish legislation, I don't know exactly what it's called, I can't really pick it up right now, but I know that there is certain protection laws, and also there is a law on protection of personal information, like your name, your social security number, and so on. So yeah, I'm aware, and I know how to find information if I need it.

35. **IN: I just have one more question, are they any other measures that you take to keep your information safe when you use e-commerce websites, that we might not have talked about already?**
36. RF: I've become aware lately on the importance of having different passwords, on the other hand I tend to forget what my password it, so quite often when I log on to a website again I have to ask to make a new password. But at the same time I think it's a good thing, because then you keep changing your password and updating it, so I think it's a good thing in one sense. And yeah, I think that's it really.

37. IN: Okay, that's it actually. Thank you for your time and participation.

Appendix VIII

Respondent G (RG) - Skype interview

Age: 22; M; Bachelors student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/23
Start time: 21.46
End time: 22.00

1. **IN: How much time per day do you spend browsing the internet?**
2. RG: Quite a few hours, 4 or 5 hours in total, aggregate.

3. **IN: How many online purchases have you made in the last 3 months, roughly?**
4. RG: About 2.

5. **IN: How much money have you spent on those purchases?**
6. RG: In KES, 15,000. (approx 1286 SEK)

7. **IN: Okay, now we're going to move to the factors that influence online shopping choices, what is the main driver for you when you decide which website to use, when you're shopping online?**
8. RG: I think it's the security, that would be the main factor. And the price, obviously. I would look at the reputation of who's selling online, that would be the number one.

9. **IN: Okay, do you do any type of research, about a new site, before you use it?**
10. RG: Yeah, I ask friends, maybe check some reviews on the net, google the site and see if it's fishy or if it's a scam, before I decide to make a purchase. For the new sites that I find out about, if they are reputable, if I'm using it for the first time but I know it's reputable I wouldn't really do a lot of such research.

11. **IN: Okay. We'll talk a bit now about privacy policies. Do you normally read through the privacy policies on the sites that you use?**
12. RG: To be honest, not really. I just skim through it really fast, mainly because it's too long sometimes, and sometimes it has some technical terms in there and it's too technical.

13. **IN: So as I understand you're not satisfied with the format, in terms of language or clarity?**
14. RG: Yes, to some extent.

15. **IN: Do you think that it should be changed?**
16. RG: Yeah I think summarizing what the policy is trying to say into a shorter thing could make it a lot easier when trying to skim through it. Making it a bit direct and to the point. Some policies have pages after pages, and usually guys are just going through it and agreeing as fast as possible. But if it could be a bit shorter, and maybe have some places where it could be expanded for those who want to go ahead and read more about it, but just summarize it and have a brief overview of what the policy entails. I know it would be not so practical in some case because the legal definitions must be stated in full, but ideally if it were shorter I think it would be better.

17. **IN: Okay, so we'll move on to the next sections, use of cookies and tracking of online behavior. Do you know what the purpose of cookies is, on e-commerce sites?**
18. RG: Actually not really.

19. **IN: Okay. In your case, are you willing to provide personal information to websites in order to get targeted advertisements for your tastes and interests?**
20. RG: I would prefer not to, I find that personally I like to make a purchase from things that I like, I look through a brochure or catalog and pick my own stuff. Rather than having it come up on a social media site, kind of like they are being pushed on to you, like this offer is there and this offer is there. Personally I find that it's pushing it onto the consumer, like buy this and buy this.

21. **IN: Okay, let's move on to the next question. When you're asked to provide personal information on a website, are there any reasons that could make you refuse to give out information, is there a limit as to what you would be willing to share?**
22. RG: For me personally if there's information they want like gender, and age, I'm sure they're using that for some kind of statistical analysis anyway, but there is a line when they start asking about bank details especially if you're not making payments with a credit card at that time, it's kind of fishy.

23. **IN: So payment information, credit cards, that's the most valuable data for you?**
24. RG: Yes, yes. That's the most personal. Here in Kenya, we have the M-Pesa option of paying with mobile money, or cash on delivery. So you don't really have to use bank or credit cards. So if it's a site that's really imposing about what bank I use, then that's where I draw the line.

25. **IN: Okay, nice. In the case when you do provide personal information to ecommerce sites, do you sometimes provide different or false information, for example a separate email, or fake name?**
26. RG: Well, no. Whenever I've made my purchases I've used my real name, and used my email address which is the only email address I have.

27. **IN: The next question is about online payments, you already mentioned that you use mobile payments and cash on delivery as opposed to credit cards?**
28. RG: Yeah I think that's a place where I find it to be quite risky, I think that's where the demerits of online shopping comes in because you have these guys who steal your information and cards becomes so risky, they can easily steal your money if it falls in the wrong hands. Like with mobile money, as long as the mobile is on you, you're the only one who can authorize the payments at the touch of a button, so I find that mobile payments are safer than credit cards.

29. **IN: Okay, nice. Next question is about social media accounts and e-commerce, do you log in to e-commerce sites using your social media accounts? For example, Facebook, or Google?**
30. RG: No, I just create an account, if I'm going to an e-commerce site I wouldn't prefer to have my Facebook linked to that. I would rather create a profile within their own website, and fill my details in for them.

31. **IN: Are there any reasons behind that?**

32. RG: Not really a specific reason, but if I was to give a reason, you find that if you log in with your Facebook, you find that they give these advertisements every time on social media newsfeeds. And I think that to an extent is annoying. So I prefer not to log in with my social media accounts, just to avoid that.

33. IN: Okay, makes sense. So, the next question talks about security features. Do you actively check for secure labels or security features such as https on e-commerce sites?

34. RG: Yes indeed, that's the first thing I check. When the site isn't https I feel that these guys are a bit iffy. I feel a lot more secure if I see the little green padlock on the side with the https.

35. IN: Next question, do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?

36. RG: Well I know there is the data protection act, but I'm not sure as to what extent it really is implied, or enforced for that matter. I hope it is being enforced, because personal data out on the internet could be used in the wrong way in various ways.

37. IN: Okay, now we have the last question, are they any other measures that you take to keep your information safe when you're browsing e-commerce websites, that we might not have talked about already?

38. RG: No I think we've covered it all, I think personally I just give out information as to what is required on a website, no more than what's asked for, because when you give out data you're not sure whether it's going to be safe or if it gets into the wrong hands.

39. IN: Okay, thank you for your time and for participating.

Appendix IX

Respondent H (RH) - Skype Interview

Age: 26; M; Masters Student, Intermediate IT knowledge

Place and date: Lund, 2017/04/20
Start time: 12.10
End time: 12.22

1. **IN: How much time do you spend browsing the Internet per day?**
2. RH: 7 hours

3. **IN: How many online purchases have you made in the last 3 months?**
4. RH: 3

5. **IN: And how much money have you spent on online shopping during those months, or those times, in the last 3 months?**
6. RH: Does this include subscriptions such as Netflix?

7. **IN: Yea**
8. RH: Maybe 800 (SEK)

9. **IN: Okay, so now we'll get into online shopping a bit more; what is the main driver for you when deciding what website to use when shopping online? Is it the price, maybe the recognition of the retailer, delivery time, convenience etc?**
10. RH: Eh, it's how reliable the site is.

11. **IN: Okay, like trustworthiness?**
12. RH: Yes

13. **IN: Nice, do you do any type of research about an e-commerce site when using it for the first time?**
14. RH: Yes.

15. **IN: And how do you do that?**
16. RH: I Google it, and see what the reviews are, how famous it is.

17. **IN: Okay. Now we'll talk a bit about privacy policies. Do you normally read through the privacy policies of the e-commerce websites that you have used?**
18. RH: Never

19. **IN: Can I ask why not?**
20. RH: It takes too much time

21. **IN: Okay, are you satisfied with the existing formats in terms of language and clarity of the privacy policies on the e-commerce websites, if you have read them sometimes maybe?**
22. RH: They are too long, but I don't think i would read them anyway.

23. IN: Okay, now we'll talk about cookies. Do you know what the purpose of cookies on e-commerce websites are?
24. RH: I think I have a clue, they want to see what I look at.

25. IN: What is your opinion on cookies? Are they beneficial or are they more of a nuisance, like annoying?
26. RH: I think they are beneficial.

27. IN: Okay, how do you deal with cookies? Do you sometimes clean them or remove them from your computer?
28. RH: No

29. IN: Okay, are you willing to provide personal information to websites so that online advertisements can be targeted to your interests?
30. RH: I don't think I would do it voluntarily, but I guess they somehow know that anyway.

31. IN: Okay, and why do you not want to do that voluntarily?
32. RH: Why would i spend time on that.

33. IN: Okay, so now we'll talk about thoughts on giving up information. If asked to provide personal information, are there any reasons that would make you refuse to give up the requested information, what is your limit as to what information becomes too personal to give up?
34. RH: I don't think I would share any information except my address or my phone number. Not my personal number.

35. IN: Okay, if you do provide your personal information to e-commerce sites, do you sometimes provide false or different information such as separate e-mail or a separate bank card?
36. RH: If I was to make a purchase, I would not provide false information.

37. IN: Okay. How do you protect your information when making online payments with your card?
38. RH: I don't think I do, I just write my information, I even have it stored on my Google account.

39. IN: Okay, have you used an alternative payment method online that you might prefer over your cards?
40. RH: No, I just use my card.

41. IN: Okay. Do you log in to an e-commerce site using your social media account such as Facebook or Google+?
42. RH: No, I do not.

43. IN: Okay. So now we'll talk about privacy concerns and controls. Do you actively check for secure labels, or website security features when visiting e-commerce sites?
44. RH: Yes, I look for this... I don't know what it's called, there's some kind of certificate.

45. IN: The swedish one?
46. RH: Yea, that's the one.

47. IN: And why do you do that?
48. RH: To make sure it's not a scam.

49. IN: Do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?
50. RH: No, I don't.

51. IN: Okay, so the last question. Are there any other measures that you take to keep your information safe when using e-commerce websites?
52. RH: I don't think so. It feels quite safe since I use my mobile Bank-ID, that makes me feel safe.

Appendix X

Respondent I (RI) - Skype Interview

Age: 28; F; Masters Degree, Intermediate IT knowledge

Place and date: Lund, 2017/04/20
Start time: 16.50
End time: 17.04

1. **IN: How much time do you spend browsing the Internet per day, how many hours?**
2. RI: If I'm not working, maybe 10 hours.

3. **IN: Okay, how many online purchases have you made in the last three months?**
4. RI: Maybe 5.

5. **IN: Okay, and how much money have you spent in those months, roughly?**
6. RI: Maybe 3000-4000. (SEK)

7. **IN: Okay. Now we'll talk about e-commerce a bit more. What is the main driver for you when deciding what website to use when shopping online? Price, recognition of retailer, delivery time..?**
8. RI: I look at ads from the Internet that pop up.

9. **IN: Okay, so if you see an ad of a product that you like?**
10. RI: Yes, then I log on and see if they have the things that I like.

11. **IN: Okay, and where do you usually see this ads? Is it like on any websites or Facebook?**
12. RI: Mostly Facebook, or sometimes television commercials.

13. **IN: Okay. Do you do any type of research about an e-commerce site when using it for the first time? Like reading reviews or..**
14. RI: No, no reviews, I look at their delivery time, but I don't read reviews.

15. **IN: Okay, so now we'll talk about privacy policies. Do you normally read through the privacy policies of the e-commerce websites that you have used?**
16. RI: No, I don't.

17. **IN: Okay, can I ask why not?**
18. RI: Because most of the privacy information is mostly the same anywhere, when we live in Sweden, so you kind of know what they are allowed to use and not.

19. **IN: Okay. Are you satisfied with the existing formats in terms of language and clarity of the privacy policies if you have read them sometime maybe?**
20. RI: Yes, I think they are easy to understand.

21. **IN: Okay, now we'll talk about cookies.**

22. RI: About what?

23. IN: Cookies; do you know the purpose of cookies on e-commerce websites?
24. RI: I think I have an idea.

25. IN: So what is your opinion on cookies? Do you think they are beneficial or like annoying?
26. RI: I think it is annoying if you have already bought something you want, and then, like ads still come up. Like, here, you can have some more shampoo, it's like I don't want it right now because I already bought it. So that's a bit annoying. Other than that I don't really care.

27. IN: So you never remove cookies for example?
28. RI: No.

29. IN: Are you willing to provide personal information to websites so that online advertisements can be targeted to your tastes and interests?
30. RI: It depends, sometimes I like it, sometimes I think it's too much.

31. IN: Okay, so now we'll talk about giving up information online. If asked provide personal information, are there any reasons that would make you refuse to give up the requested personal information? Like, what is your limit as to what information that becomes too personal to give out?
32. RI: If they specifically say that they are going to sell my information to other websites, then I would think it's too much. But other than that, no restrictions.

33. IN: Okay. If you provide personal information to websites, do you sometimes provide false or different information, such as separate email?
34. RI: No I don't, always the same.

35. IN: How do you protect your information when making online payments with credit cards or debit cards?
36. RI: Sometimes I have a password that you have to type in, or I use my Bank-ID, where you have to type in your password in order to proceed with the purchase.

37. IN: Yea. Have you used an alternative payment method online that you might prefer, instead of cards?
38. RI: Yes, sometimes I've used invoice payments so that you don't have to pay directly.

39. IN: Okay. Do you log in to an e-commerce site using your social media accounts, such as Facebook or Google+, or something like that?
40. RI: Yes.

41. IN: So when you are at an e-commerce site and there's an option to sign in with Facebook?
42. RI: Yes.

43. IN: Okay, what are the reasons for doing that, for you?
44. RI: No, sorry, I don't.

45. IN: No? Okay, yea. Now we'll talk about privacy concerns and controls. Do you actively check for secure labels or website security features when visiting e-commerce sites?

46. RI: No, I don’t.

47. IN: Can I ask why not?
48. RI: I didn’t even know they existed.

49. IN: Okay. Do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?
50. RI: No

51. IN: Okay. So last question. Are there any other measures that you take to keep your information safe when using e-commerce websites?
52. RI: Just to make sure to log out, and that everything is completed before signing off.

53. IN: Okay, I guess that’s it then.
54. RI: Okay, thank you

55. IN: Thank you.

Appendix XI

Respondent J (RJ) - Skype Interview

Age: 23; M; Masters Student, Expert IT knowledge

Place and date: Lund, 2017/04/20
Start time: 20.15
End time: 20.32

1. **IN: How much time do you spend browsing the Internet per day; how many hours?**
2. RJ: 10, maybe.

3. **IN: How many online purchases have you made in the last three months?**
4. RJ: Maybe 12.

5. **IN: Okay. And how much money have you spent on online shopping during those three months, roughly?**
6. RJ: Maybe 4000 (SEK)

7. **IN: 4000, yes okay. Now we'll talk a bit more about online shopping. What is the main driver for you when deciding what website to use when shopping online? Is it price, recognition of retailer, delivery time…?**
8. RJ: Reputation to start off. Or, it depends, first it's price, if you find a good price. Then the reputation, I mean if they are reliable or not. So I think price, then reputation. And of course then we also have delivery time and stuff like that.

9. **IN: Okay, yea. Do you do any type of research about an e-commerce site when using it for the first time?**
10. RJ: Yeah, I always Google them before. If I want to buy something that is offshore or abroad I always Google them to see if they are reliable… if they deliver on time.

11. **IN: Okay. Now we move on to privacy policies. Do you normally read through the privacy policies of the e-commerce websites that you have used?**
12. RJ: No.

13. **IN: Can I ask why not?**
14. RJ: Well, as I said before I always Google them before if people say something bad about them. If something bad is written in the terms of agreement and privacy stuff someone else would have acknowledged that.

15. **IN: Yea, okay. Are you satisfied with the existing formats in terms of language and clarity of privacy policies if you have read them sometimes, or at least looked at them sometimes?**
16. RJ: No, not really. I think they could be simplified.

17. **IN: Okay, simplified?**
18. RJ: Like, four sentences "this is what's up" pretty much, but I guess it's part of their business plans to keep that in the dark to customers sometimes maybe.

19. IN: Okay, we move on to cookies. Do you know what the purpose of cookies on e-commerce websites is?

20. RJ: I could guess, I mean for example if I Google shoes, and then that cookie saves that information. Whenever I visit a website I get a recommendation from a certain website where to buy shoes for example. But of course it's both for marketing and… yea I guess it's mostly marketing purposes.

21. IN: Yea, okay. So what is your opinion on cookies, are they beneficial or more of a nuisance, like annoying?

22. RJ: I usually always remove cookies, so… because you never know what they save about you.

23. IN: Okay, that's actually my next question. How do you deal with cookies, but you said that you remove them?

24. RJ: Yea, yea. Plus when I close my web browser it deletes all cookies.

25. IN: Okay, so every time you close your browser...?

26. RJ: Yea.

27. IN: Okay.

28. RJ: Cause I…. I mean I'm not doing shady stuff… I don't know, I don't like the thought of that someone is storing information about me and somehow, maybe, I mean if you get enough information you can like, combine all the information from different sites and get a pretty good picture of who I am. So that's why I delete them, usually.

29. IN: Yea, so my next question, are you willing to provide personal information to websites so that online advertisements can be targeted to your tastes and interests?

30. RJ: No, then I would find that website myself. Something like that.

31. IN: Okay. The next topic is about giving up information online. If asked to provide personal information, are there any reasons that would make you refuse to give out the requested personal information? Like, what is your limit as to what information becomes too personal to give out?

32. RJ: Okay… umm… I mean, we've got public data about ourselves, like our name, or sometimes our address, sometime our phone numbers, but I'm guessing like when my habits and my personal stuff like relationships, my health status, health information and stuff like that, when websites start to ask about that I would reject them pretty quickly.

33. IN: Okay. If you do provide personal information to websites, do you sometimes provide false or different information, such as separate e-mails, or…?

34. RJ: Sometimes when I just want to, like, enter a website, and you need to register I just enter some random words pretty much.

35. IN: Okay, yea.

36. RJ: Because, if sometimes, not always do you get these confirmation e-mails.

37. IN: Mm, yea. How do you protect your information when making online payments with credit cards, or debit cards, is there any like precaution that you take?

38. RJ: Well I use my bank thingy, whatever it's called. That's I'm guessing is the most precaution I take because I feel that's pretty safe. Of course I do like virus scans on my computer pretty often. So I'm guessing that's also a precaution. But as I said before I think looking up the website and check if it's reliable or not. Because I remember my brother bought something on a web shop in the UK and used his card. Then one week after he got a phone call from his bank saying that someone wants to take out like... I don't how much, but it was from like Greece or something and that was not true. Checking out the website is the most important thing I think.

39. IN: Yea… have you used an alternative payment method online that you might prefer, instead of using card payment.

40. RJ: I think I've used Swish once, and that's quite handy I think. But that is the only one I think.

41. IN: Okay. Do you log into any e-commerce site using your social media account, like Facebook or Google+?

42. RJ: No, as I said before about the marketing stuff, so I try to avoid that.

43. IN: Yea and the last topic is about privacy concerns and controls. Do you actively check for secure labels or website security features when visiting e-commerce sites?

44. RJ: Umm… not actively, but I usually look for the https, so it's a criteria that I look for, but actively I don't look for these pictures.

45. IN: No, okay. Do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?

46. RJ: I only know it in swedish...Personuppgiftslagen (PuL).

47. IN: Yea, many websites refer to that law in the policies.

48. RJ: Yea.

49. IN: Okay, last question. Are there any other measures that you take to keep your information safe when using e-commerce websites that you can think of?

50. RJ: You mean if I take any precautions…?

51. **IN: Yea.**

52. RJ: Okay, no, not what I haven't said already I think.

53. IN: Okay, well, that was it.

54. RJ: Thank you very much.

55. IN: Thank you for taking the time to be in this interview.

56. RJ: No problem.

Appendix XII

Respondent K (RK) - Skype Interview

Age: 24; M; Bachelors Degree, Expert IT knowledge

Place and date: Lund, 2017/04/20
Start time: 21.30
End time: 21.46

1. **IN: How much time do you spend browsing the Internet; how many hours per day?**
2. RK: Around 2-3

3. **IN: Okay. How many online purchases have you made in the last three months?**
4. RK: 5, around there.

5. **IN: 5, yea? And how much money have you spent on online shopping during those months, roughly?**
6. RK: 2500 SEK

7. **IN: Yea, okay. So now we'll talk a bit more about online shopping. What is the main driver for you when deciding what site to use when shopping online? Like price...**
8. RK: Mainly price, I decide on the product and then I look at the price - where to buy it from.

9. **IN: Yea, okay. Do you do any type of research about an e-commerce site when using it for the first time? Like reading reviews or googling it?**
10. RK: Not always, but that's because usually the sites that I found the most cheap or respectable sites.

11. **IN: Okay, then we'll move on to privacy policies. Do you normally read through the privacy policies of the e-commerce websites that you have used?**
12. RK: Never.

13. **IN: Never? Can I ask why not?**
14. RK: Purely cynicism I would guess. Like, I mean it's important but I just don't. I should, but I just don't.

15. **IN: Okay. Are you satisfied with the existing formats in terms of language and clarity of the privacy policies, if you ever read one?**
16. RK: I mean, with the stuff that I have read, yea, but it's very long which I guess is the biggest thing that makes people not read it.

17. **IN: Yea, okay. Now we'll talk about cookies. Do you know what the purpose of cookies on e-commerce websites is?**
18. RK: Yes.

19. **IN: Yea, can you maybe explain a bit?**

20. RK: To track your search history and also, like how your previous visits to that specific store was.

21. IN: What is your opinion on cookies, are they beneficial or are they of a nuisance?

22. RK: Well, they're… I mean I'm not a big fan of the fact that your search history is sold to third parties in so many cases. But I generally keep very high security in my browser, so the cookies are cleared.

23. IN: Yea, that's my next question. How do you deal with cookies, if you remove them?

24. RK: Yea, I run add-ons on my browser that deletes them.

25. IN: Okay, so the next one is a bit repetitive, but are you willing to provide personal information to websites so that online advertisements can be targeted to your tastes and interests?

26. RK: I would never sign up for advertisement unless there was some sort of incentive to do so. In that case, I might consider it.

27. IN: Yea. The next topic is about giving up information. So, if asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? Like, what is your limit as to what information becomes too personal to give out?

28. RK: I don't really have a limit, like it depends from case to case. It's on a need to know basis. So if I think they don't need that information for whatever I'm doing on their site I wouldn't give it.

29. IN: So, like, if it's relevant?

30. RK: Yea.

31. **IN: Okay. If you do provide personal information to websites, do you sometimes provide false or different information?**

32. RK: Yea, I have a whole separate e-mail address for sites like that.

33. IN: Okay. How do you protect your information when making online payments with credit cards? Do you take any sort of measure, security measure, or privacy measure?

34. RK: I mostly use PayPal for payments.

35. IN: Okay.

36. RK: So that the shop will actually never have my payment information.

37. IN: Yea, that's my next question. Have you used an alternative payment method online that you might prefer?

38. RK: I've used a few. Like Skrill, PayPal. But mainly PayPal, because it's so widely available.

39. IN: Yea, okay. Do you log into e-commerce sites by using your social media account, like Facebook or Google+?

40. RK: No.

41. IN: What are the reasons for that?

42. RK: Because I don't… I know for example that Facebook gathers this information and sells it. And they target you with advertisements specifically for you.

43. IN: Okay, so the last topic is about privacy concerns and controls. Do you actively check for secure labels or website security features when visiting e-commerce sites?

44. RK: Yea, I also have an add-on which checks the site's certificate. So if I get any warning I will not make any confidential information entries.

45. IN: Okay. So what's the main reason for using that? To feel safe, or…

46. RK: No, it's more like precaution, better safe than sorry.

47. IN: Yea. Do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?

48. RK: I know some general about Europe, mostly about Sweden.

49. IN: Yea, okay. Do you know what, like some of the main points of those laws? Or have you just heard about them?

50. RK: I mean, mainly I just read if there is anything in the paper about it, or like online newspapers. I don't actively look it up.

51. IN: Yea, okay. So the last question; Are there any other measures that you take to keep your information safe when using e-commerce websites?

52. RK: Yea, I mean it all depends on which website it is. Like, the more I trust them, the more I might be willing to give out personal information. But I mean on a technical level I try to do my best to not get any information leaked.

53. IN: Okay. That is about it. So thank you for taking the time to take part.

54. RK: No problem.

Appendix XIII

Respondent L (RL) – Face-to-face interview

Age: 26; Male; Masters student; Basic IT knowledge.

Place and date: Lund, 2017/04/20
Start time: 14.07
End time: 14.22

1. **IN: How much time per day do you spend browsing the internet?**
2. RL: More than 6 hours

3. **INJ: How many online purchases have you made in the last 3 months?**
4. RL: 0, it's because I am in Sweden. If I am in China, maybe continuously

5. **IN: How much money have you spent on those purchases? Nothing?**
6. RL: Sorry.

7. **IN: Well, now we're going to ask something about the factors that influence online shopping choices. Firstly, what are the main factors for you when you decide which website to use, when you're shopping online? For instance, like price, recognition of retailer delivery time, trustworthiness, convenience, security?**
8. RL: I'd like to say price and delivery.

9. **IN: So I guess that's more convenient for you, compared with the normal shopping activities?**
10. RL: Yes, for me, it is. For instance, if I plan to buy some protein powder, which is very heavy. Also, the price is usually lower at Amazon England. If I do it online, then I don't have to carry it on my own. They will deliver it to the agency. So, yes..

11. **IN: Well, nice, so the second question was do you do any type of research about an e-commerce site when using it for the first time? Like reviews, find out from friends' experiences and so on.**
12. RL: What is e-commerce website?

13. **IN: For instance, eBay, Amazon or any online retailer, H&M?**
14. RL: Aha, I only use Amazon. You mean the first time of using Amazon in Sweden or in my whole life?

15. **IN: Well, in your life maybe, if you can remember.**
16. RL: I bought some books, I think. But in China, no really. We have Taobao. You don't have to do research on Taobao

17. **IN: So you don't do any research for that.**
18. RL: Yeah

19. **IN: Nice, so let's move to privacy policies. Do usually read through the privacy policies on the sites that you use?**

20. RL: I have never read that. Just never.

21. IN: Why? But you know that exists there, right?
22. RL: Yes, sure. I know the cookie policy. It says “I agree” and something.

23. IN: So how do you deal with that? Will you click “I agree” or other options?
24. RL: In my own computer, I will do it.

25. IN: Okay, that’s interesting. So are you satisfied with the existing formats of privacy policies on the e-commerce websites you use? Including language, clarity, everything in your mind.
26. RL: Not really

27. IN: Why?
28. RL: Sometimes, I can’t understand Swedish and sometime, it’s too long. I don’t have that much patience. It’s boring and pointless.

29. IN: So, next questions are about uses of cookies. Do you know what the purpose of cookies is, and what are the cookies?
30. RL: Sorry, I don’t know cookies.

31. IN: Alright. But do you know there are cookies in site? Usually it is displayed at the top of the page
32. RL: Yes. I don’t know cookies from technical perspective.

33. IN:So What is your opinion on cookies, are they beneficial or a nuisance? How do you deal with them?
34. RL: Even I don’t know cookies. I think it’s beneficial. Sometimes, my e-mail address is quite long. Maybe I will use cookies in the future.

35. IN: Okay, So next question, are you willing to provide that information then to websites in order to get personal targeted advertisements? I think it’s quite a common phenomenon. If you search something on Taobao, you can always receive some recommendations or so on.
36. RL: For me, it depends on which site I am using and what product. If it’s the protein powder, clothes. Maybe I will. If something is far away from my daily life. I will not provide. When I want to buy some tickets. If it can provide me some cheaper options, even I don’t buy it now. It’s still good to know the site. Maybe I will use it next time.

37. IN: That’s good idea. Well Question No. 8. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?
38. RL: Again, that depends on the website. If the site is originally the online shopping site. I don’t really care. I mean that’s not important. If I give them my credit card information, I don’t think they will give it to the other. As for the basic information, the name, the address, the phone, I don’t care that much. If the site is randomly found by me, I will say no.

39. IN: Nice, The next question if you do provide personal information to web sites, do you sometimes provide false/different information? Do you use separate email, bank card, nickname for online shopping use?

40. RL: For me, it depends. In Sweden, I will use my real information. In China, my Taobao profile name is “X Y” (real name masked in order to remain anonymous). And I always use my company address. If I do have to get something delivered to my home. I usually only give it the name of my residential area.

41. **IN: Okay, Next question, how do you protect your information when making online payments with credit cards? Have you used an alternative payment method online that you might prefer? Do you use Alipay, Swish, paypal or something similar?**
42. RL: Well, I think all these questions are targeted Swedish people. We don’t use credit card for online shopping in China. We use the third party payment. We have WeChat pay, Alipay.

43. **IN: Yeah, totally understand. So do you think it’s more convenient by using Alipay?**
44. RL: Of course, but in Sweden, we don’t have choice. We can only use the credit card.

45. **IN: Okay, Do you log in to an e-commerce site using your social media account like Facebook, Google?**
46. RL: No, I have a separate account. I don’t want to use my WeChat account or Facebook account. I think that’s more safe.

47. **IN: Okay, so do you actively check for “secure labels” or website security features (eg https) when visiting e-commerce sites? If so, why?**
48. RL: Yes, I don’t know why. But it’s my habit.

49. **IN: Same here. So do you know of any applicable laws that are in place to help you maintain your privacy and protect your data? Wherever you are in China or Sweden.**
50. RL: No, I don’t care of it at all.

51. **IN: Okay, last question, do you have any other measures that you take to keep your information safe when you’re browsing e-commerce websites?**
52. RL: Well, I will only use the site with good reputation. And I will try to avoid to using my credit card. If I have to, I always double check with my bank after my shopping. The last one is to try Alipay or any type of third party payment.

53. **IN: Okay, thank you for your time.**

Appendix XIV

Respondent M (RM) – Face-to-face interview

Age: 23; F; Masters student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/22
Start time: 11.02
End time: 10.32

1. **IN: How much time per day do you spend browsing the internet?**
2. RM: 6 hours per day

3. **IN: How many online purchases have you made in the last 3 months? Have you bought something online?**
4. RM: In general, I bought some medicine, shampoo, conditioner and clothes

5. **IN: How much money have you spent on those purchases in the last 3 months?**
6. RM: Around 2000kr

7. **IN: Well, now we're going to ask something about the factors that influence online shopping choices, what is the main factor for you when you decide which website to use, when you're shopping online? For instance, like price, recognition of retailer, delivery time, trustworthiness, convenience, security?**
8. RM: Price… And payment measurement.

9. **IN: so, that means it's more convenient for you?**
10. RM: Ah..it depends

11. **IN: What do you mean?**
12. RM: Well, it depends on my mood. And the area. If I am not eager to get this product, I can buy it online.

13. **IN: Okay, so the second question was do you do any type of research about an e-commerce site when using it for the first time? like reviews, find out from friends' experiences and so on.**
14. RM: I used Zhihu. Sometimes.

15. **IN: Nice, so what kind of research? How to use Zhihu?**
16. RM: Check if the service is good? Delivery, or something. Normally, I only do some research for the brand or store. Just go through some comments. To see the reputation of the sites. Nothing special

17. **IN: Okay so let's move to privacy policies. Do usually read through the privacy policies on the sites that you use?**
18. RM: No, never

19. **IN: Why?**
20. RM: I am just so lazy. It's time-wasting. For me, I don't consider they are that important. I don't care.

21. **IN: Okay, that's interesting. So are you satisfied with the existing formats of privacy policies on the e-commerce websites you use? Including language, clarity, everything in your mind.**
22. RM: I would say yes. Because, I don't encounter any problem with that. It's not the priority to consider that. Instead of, I will take care of the product.

23. **IN: So, next questions are about uses of cookie. Do you know what the purpose of cookies is, and do you know what the purpose of cookies is, and what are cookies?**
24. RM: Yes, I know cookies. By using cookies, it can store our username, password and other information. After that, you can use it ,without typing again.

25. **IN: So what is your opinion on cookies, are they beneficial or a nuisance? How do you deal with them?**
26. RM: Yeah, it's convenient. I use cookie all the time. Especially, by chrome. Since I don't want to type the account again and again. Technically, I can have these information in any computer as long as I log on my Google account.

27. **IN: So are you willing to provide that information then to websites in order to get personal targeted advertisements?**
28. RM: For me. No, I don't need any recommendations. Especially, I have bought some products already. The site kept pushing the recommendation info. It's kind of stupid. I prefer to search by myself.

29. **IN: Since you don't trust these sites?**
30. RM: Since I had some bad experience. The site send me the spam everyday. That's terrible actually. I trust them. But still, they will agonize me somehow. Sometimes, they even change the email address to give me the spam.

31. **IN: Sorry for bad experience. Well Question No. 8. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?**
32. RM: For my contact information, I don't want to.

33. **IN: such as address, phone and so on, right? But if you want the good be delivered, you have to give the address. How do you think about it?**
34. RM: In Sweden, it's ok. I will not live here permanently. I just need to clean up my mail box. That's it. But if I am in China, I will not give them. I don't use my real name, my full address. I usually use "Zhang Sanfeng" as online name. As long as I provide a useful phone number, it's ok. As you know, they only check the phone number instead of the ID. Only thing you have to do is telling them the phone number, then you will get your product.
35. **IN: Okay, interesting. The next question If you do provide personal information to web sites, do you sometimes provide false/different information? Do you use separate email, bank card, nickname for online shopping use? As you mentioned, you will use your fake name.**
36. RM: Yes, I have several email accounts. But I would use the same one for my all my online shopping. Because, it's too complicated if I used different email addresses. As for the fake name, definitely yes. But it doesn't work in Sweden. I have to show my ID when I pick up my packages. Also, I will not provide my full address. Usually, I don't

provide my room number. Only the street name and street number works in China. They will call me.

37. **IN: That's true, Okay, Next question, How do you protect your information when making online payments with credit cards? Have you used an alternative payment method online that you might prefer? Do you use Alipay, Swish, paypal or something similar?**
38. RM: Well I can only use my credit card in Sweden. I don't have the Swedish personal number. That means I can't open a Swedish bank card with the function of online transfer. I can't use Swish. But in China, I can use Alipay. I can pay when my package delivered. I can also ask my friends to help me to pay for it. You must know what I mean. Here, I can only use my Visa card. It's ok. I need to receive the temporary token by message when I use it online. It's safe. I guess.

39. **IN: Okay, Do you log in to an e-commerce site using your social media account like Facebook, Google+, Wechat?**
40. RM: Yeah, sometimes. Sometimes, I am lazy to create a new account.

41. **IN: Okay, so do you actively check for "secure labels" or website security features (eg https) when visiting e-commerce sites? If so, why?**
42. RM: Yes, I will do that. For the security, that's the basic check.

43. **IN: Same here. So do you know of any applicable laws that are in place to help you maintain your privacy and protect your data? Wherever you are in China or Sweden.**
44. RM: No, I have no idea about that.

45. **IN: Okay, last question, do you have any other measures that you take to keep your information safe when you're browsing e-commerce websites?**
46. RM: Only use your own computer. Yeah, that's my idea.

47. **IN: Okay, thank you for your time.**

Appendix XV

Respondent N (RN) – Face-to-face interview

Age: 24; F; Masters student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/22
Start time: 19.56
End time: 20.11

1. **IN: How much time per day do you spend browsing the internet?**
2. RN: it's about 7 or 8 hours, I guess

3. **IN: How many online purchases have you made in the last 3 months?**
4. RN: Only once

5. **IN: How much money have you spent on those purchases? Nothing?**
6. RN: around 500kr, I bought some makeup stuff

7. **IN: Well, now we're going to ask something about the factors that influence online shopping choices. Firstly, what is the main factor for you when you decide which website to use, when you're shopping online? For instance, like price, recognition of retailer, delivery time, trustworthiness, convenience, security?**
8. RN: I can only choose one factor? Or more than one

9. **IN: All works. You can select from these options. Still you can answer it based on your situation.**
10. RN: I think the main driver is price.

11. **IN: Okay, why price?**
12. RN: Because it's cheap. I don't have too much money. Also, I don't have too much time to go to the store or the mall.

13. **IN: So online shopping is convenient for you, right?**
14. RN: Yep, sure

15. **IN: Okay, so the second question was do you do any type of research about an e-commerce site when using it for the first time?**
16. RN: No, I usually do not do any research on the site. I would look through the site directly. I do care about the product itself instead of the site.

17. **IN: Well. Let's move to privacy policies. Do usually read through the privacy policies on the sites that you use?**
18. RN: No, never.

19. **IN: Aha, but you know the policy things exist on the site, right?**
20. RN: Yeah, I know.

21. **IN: Then, Why you do not read about that? Are you afraid of the information disclosure?**
22. RN: I just want to buy something. Why should I read that? It depends on what product. Normally, I would buy some clothes and makeup at Taobao, Tianmao or Amazon. I don't think I have to take care of these privacy policies.

23. **IN: Okay, that's interesting. So are you satisfied with the existing formats of privacy policies on the e-commerce websites you use? Such as language, clarity**
24. RN: No. I prefer to the graphic ways. It should be easy to understand. The existing formats are too boring.

25. **IN: Yeah, that's right. Next questions are about uses of cookies. Do you know what the purpose of cookies is, and what are cookies?**
26. RN: I know it. I had some lectures about it. Cookies, also session. I know cookie could store the data with formats of key-value. But I can't remember everything. Maybe it will store the browsing history, the account information or something. For the e-commerce website, I don't know how they use cookies exactly.

27. **IN: So what is your opinion on cookies, are they beneficial or a nuisance? How do you deal with them?**
28. RN: I don't know, at least cookies don't cause any problems for me.

29. **IN: Okay, so next question, are you willing to provide that information then to websites in order to get personal targeted advertisements?**
30. RN: To be honest, No. I don't want to share my personal information with the site. But the advertisements always pop up. No matter you provide the information or not. That sucks.

31. **IN: True, I have same problems. Well next one. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?**
32. RN: That depends what information. If it's something about the bank account, yeah, the financial information. I will refuse it. Because it's dangerous. I know an example. Some websites ask me binding my credit card. I can't skip it if I want to finish my registration. That's stupid.

33. **IN: Yeah, I think I know this situation. It's quite annoying. Well, if you do provide personal information to web sites, do you sometimes provide false/different information? Do you use separate email, bank card, nickname for online shopping use?**
34. RN: Yeah maybe. But it depends. If these e-commerce site are what I usually use. I mean they are trustworthy. I will provide my real information. If it's totally a new site, I just want to use it for once. Because of the good price, or some other reason. I probably will give the fake information. For instance, I will give the fake name but the pronunciation is similar to my real name.

35. **IN: Okay, How do you protect your information when making online payments with credit cards? Have you used an alternative payment method online that you might prefer? Do you use Alipay, Swish, PayPal or something similar?**
36. RN: I will think about the environment, equipment as well. I will not use the public Wi-Fi when I pay by my credit card. Also, I prefer to use my own laptop or phone to

pay. Aha. I remind something. I will use the bank app to pay the bill in Sweden. That's similar to Alipay. And it's convenient and easy to use.

37. **IN: Okay, Do you log in to an e-commerce site using your social media account like Facebook, Google?**
38. RN: Yes, I did.

39. **IN: Why?**
40. RN: it's convenient. I used my Facebook account and my Weibo account. I don't think most people will care about the privacy issues.

41. **IN: Ok, I get your point. You will use your social media account, which are not that important. You will not use your WeChat account to log in to the site, right?**
42. RN: Yes!

43. **IN: Okay, so do you actively check for "secure labels" or website security features (e.g. https) when visiting e-commerce sites? If so, why?**
44. RN: I have no idea about that. I don't even know the secure labels exist.

45. **IN: So do you know of any applicable laws that are in place to help you maintain your privacy and protect your data? Wherever you are in China or Sweden.**
46. RN: No, I don't know any law in China as well as Sweden.

47. **IN: Okay, last question, do you have any other measures that you take to keep your information safe when you're browsing e-commerce websites?**
48. RN: Firstly, you have to use the safe network, especially when you pay by our credit card.

49. **IN: Okay, thank you for your time.**

Appendix XVI

Respondent O (RO) – Face-to-face Interview
Age: 61; F; High School Diploma, Basic IT knowledge

Place and date: Lund, 2017/04/23
Start time: 17.40
End time: 17.55

1. **IN: How much time do you spend browsing the Internet, how many hours per day?**
2. RO: Roughly one hour per day.

3. **IN: One hour, how many online purchases have you made in the last three months?**
4. RO: Two.

5. **IN: Okay. How much money have you spent on online shopping in those months, roughly?**
6. RO: 1000 kronas (SEK)

7. **IN: Okay, now we'll talk a bit more about online shopping. What is the main driver for you when deciding what website to use when shopping online? Is it price, recognition of retailer, delivery time...what's the most important thing for you?**
8. RO: Recognition of retailer.

9. **IN: Do you do any type of research about an e-commerce site when using it for the first time?**
10. RO: Yes, I do.

11. **IN: Okay, how do you do that? Do your read reviews or google it?**
12. RO: Yes, I Google and compare prices and stuff.

13. **IN: Okay, so now we'll talk about privacy policies. Do you normally read through the privacy policies of the e-commerce websites that you have used?**
14. RO: Not really.

15. **IN: Can I ask why not?**
16. RO: I never thought about it.

17. **IN: Are you satisfied with the existing formats in terms of language and clarity of privacy policies of the e-commerce sites, if you've ever read one, or looked at them?**
18. RO: Maybe it's a bit complicated written, the language is perhaps hard to understand.

19. **IN: Okay. Do you know what the purpose of cookies are on the e-commerce websites?**
20. RO: No.

21. IN: Are you willing to provide personal information to websites so that online advertisements can be targeted to your tastes and interests?
22. RO: No.

23. F. Why not?
24. RO: I want to keep my integrity as much as possible when online.

25. IN: Okay. Now we'll talk about giving out information. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?
26. RO: Umm… my income, and if I have any diseases for example.

27. **IN: Okay. If you do provide personal information to websites, do you sometimes provide false or different information?**
28. RO: No, never.

29. IN: How do you protect your information when making online payments with credit cards or debit cards?
30. RO: Through Bank-ID.

31. IN: Have you used an alternative payment method online that you might prefer?
32. RO: Yes.

33. IN: Can you give an example?
34. RO: Invoice. I find that better, I prefer invoice.

35. IN: Do you log into an e-commerce website using your social media account such as Facebook or Google+?
36. RO: No.

37. IN: Okay. Now we'll talk about privacy concerns and controls. Do you actively check for secure labels or website security features when visiting e-commerce websites?
38. RO: No. I'm not familiar with that. As I said I have basic IT knowledge.

39. IN: Yes. Do you know of any applicable laws that are in place to help you maintain your privacy and protect your information and data?
40. RO: No.

41. IN: Are there any other measures that you take to keep your information safe when using e-commerce websites?
42. RO: I try to avoid giving out my social security number. If possible, I try to avoid informing about that.

43. IN: Okay, thank you, that was all.

Appendix XVII

Respondent P (RP) – Face-to-Face Interview

Age: 20; F; High School Diploma, Intermediate IT knowledge

Place and date: Lund, 2017/04/22
Start time: 18.50
End time: 19.04

1. **IN: How much time do you spend browsing the Internet, how many hours per day?**
2. RP: Very much, like every day, all day. 12 hours

3. **IN: Okay, how many online purchases have you made in the last three months?**
4. RP: One.

5. **IN: How much money have you spent on online shopping in the last three months?**
6. RP: 50 Euros...500 swedish crowns.

7. **IN: Okay. What is the main driver for you when deciding what website to use when shopping online?**
8. RP: The cheapest, and the delivery time.

9. **IN: Okay, good. Do you do any type of research about an e-commerce site when using it for the first time, like reading reviews or googling it?**
10. RP: Yes, I look at the reviews. And often I get recommended from people I know.

11. **IN: Okay. So now we'll talk about privacy policies. Do you normally read through the privacy policies of the e-commerce websites that you have used?**
12. RP: No.

13. **IN: Can I ask why not?**
14. RP: I don't really know where to find that, and I don't really care.

15. **IN: Okay. Are you satisfied with the existing formats in terms of language and clarity of the privacy policies of e-commerce websites, if you have ever looked at one?**
16. RP: I haven't.

17. **IN: Okay. Now we'll talk about cookies.**
18. RP: Yes.

19. **IN: Do you know what the purpose of cookies on e-commerce websites is?**
20. RP: It's supposed to make my personal web experience better, but I don't really know how it works..

21. IN: Okay. What is your opinion on cookies? Are they beneficial or are they more annoying?
22. RP: I think it's pretty annoying when it comes up, because before, there was never any problems with visiting a website. So I just think it's annoying that it comes up, you know? Like, "we use cookies". Because I don't see any difference.

23. IN: Okay. How do you deal with cookies? Do you sometimes remove them?
24. RP: No, I just accept.

25. IN: Are you willing to provide personal information to websites so that online advertisements can be targeted to your tastes and interests?
26. RP: Yes.

27. IN: Yes. Is there any reason for that?
28. RP: No, sometimes it's just...sometime I get commercial and I press that I don't want to see this commercial.

29. IN: But you are willing to provide personal information so that you can get targeted advertisements?
30. RP: Yea.

31. IN: Okay. Now we'll talk about giving up information online. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information?
32. RP: Yes.

33. IN: Okay, can you name a reason?
34. RP: Because maybe I don't use that website that often, so I think it's unnecessary.

35. IN: What is your limit as to what information becomes too personal to give out, for you?
36. RP: Like where I live, only like general things, like if I'm a boy or a girl, because then I won't get boy stuff. And maybe my profession.

37. IN: So you don't want to give out that?
38. RP: No, that's okay. Like general things, but not like where I live. But that they can find anyways.

39. IN: Okay. If you do provide personal information to websites, do you sometimes provide false or different information?
40. RP: No.

41. IN: How do you protect your information when making online payments with credit cards or debit cards?
42. RP: I use...I don't use my card number, I get a bill instead.

43. IN: Okay, so that's my next question. If you use an alternative payment method online that you might prefer.
44. RP: Yea.

45. IN: So invoice?
46. RP: Yes.

47. IN: Do you log into e-commerce sites by using your social media account, like Facebook or Google+?
48. RP: Yea.

49. IN: And why do you do that?
50. RP: It's easier.

51. IN: Okay. So now we'll talk about privacy concerns and controls. Do you actively check for secure labels or website security features when visiting e-commerce sites?
52. RP: I don't know...what was the question?

53. IN: Do you actively check for secure labels?
54. RP: No, but I only use those that I get recommended to use. I don't use sites that have gotten bad reviews or things I only see on Facebook, because I don't trust those ads. And usually only companies that have a store.

55. IN: Like a physical store?
56. RP: Yea. And not only like e-buy (e-shop), because I don't think it's pretty safe, like Nelly, because they don't have a store that I can visit if something goes wrong. So personal contact is kind of important.

57. IN: Do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?
58. RP: No, I don't think so.

59. IN: Okay, so last question. Are there any other measures that you take to keep your information safe when using e-commerce websites?
60. RP: No... Only like use those that I know from others that are safe and... But I don't... I used to register, but I don't do that anymore, so I only write in the information once, and that they don't get access to it.

61. IN: Okay, thank you, that was all.
62. RP: Thank you.

Appendix XVIII

Respondent Q (RQ) – Face-to-Face Interview
Age: 59; M; Master's Degree, Intermediate IT knowledge

Place and date: Lund, 2017/04/24
Start time: 20.00
End time: 20.14

1. **IN: How many hours do you spend online, and how many online purchases have you made in the last three months?**
2. RQ: Six hours per day. Maybe three or four purchases in the last three months.

3. **IN: And how much money have you spent on online shopping during those months?**
4. RQ: Maybe 1000 krona (SEK)

5. **IN: Now we'll talk a bit more about online shopping. What is the main driver for you when deciding what website to use when shopping online? Is it the price, recognition of retailer, delivery time…?**
6. RQ: Recognition of retailer.

7. **IN: Okay. Do you do any type of research about an e-commerce site when using it for the first time?**
8. RQ: I usually only use one, I buy books only on the Internet. I have an account on one of those places.

9. **IN: Do you normally read through the privacy policies of the e-commerce website that you use?**
10. RQ: No.

11. **IN: Why not?**
12. RQ: Why should I?

13. **IN: Right, okay. If you have ever looked at a privacy policy, are you satisfied with the existing formats, in language and clarity?**
14. RQ: I don't know. I've never looked at it.

15. **IN: Okay. Do you know what the purpose of cookies on e-commerce websites is?**
16. RQ: I think so, but not 100%.

17. **IN: You can tell me what you think it is?**
18. RQ: They can track who has been on the website. They would track me. It's like bacteria rather than cookies.

19. **IN: Okay. And what is your opinion on cookies? Are they beneficial or..?**
20. RQ: I don't like them at all.

21. IN: Why not?
22. RQ: Because I want to be completely confidential of who I am. And anyway, they have my account numbers, and I have an account so they don't really need it I would guess.

23. IN: Do you do anything, to maybe remove them or something?
24. RQ: I clear out sometimes, yes.

25. IN: Okay. Are you willing to provide personal information to websites so that online advertisements can be targeted to your tastes and interests?
26. RQ: No, I don't want that.

27. IN: Why not?
28. RQ: I want to be alone, I don't want that. I just simply don't want it, I don't like it.

29. IN: Okay. Now we'll talk about giving up information. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information - what is your limit as to what information becomes too personal to give out?
30. RQ: Obviously they would need my delivery address, my card numbers so I can pay. Usually I pay by invoice anyway. I pay actually by invoice. I book a lot of hotels actually on the Internet, so it's much more than 1000 kronas (SEK) by the way. It would be 25000, something like that. (for work)

31. IN: Okay.
32. RQ: I book hotels on the Internet, so that's what I do. So I only give the minimum bare amount of information they would require for the purchase to go through.

33. IN: Okay. If you do provide personal information, do you sometimes provide false or different information?
34. RQ: No, I don't.

35. IN: How do you protect your information when making online payments with credit cards?
36. RQ: I don't protect it. I mean I give the information they require, so I don't do anything special.

37. IN: Do you prefer invoice?
38. RQ: I prefer invoice, if possible. And sometimes I book hotels, that's why I have for instance, I usually book hotels on this booking sites, Expedia. It was very complicated in terms of payment. So I started to use them for finding the hotels, but call the hotels directly and contact them. Partly because they were giving out information, but also it's difficult to pay. They pay two or three different times. And if you book at the hotel directly it's only one time you pay it.

39. IN: Okay. Do you actively check for secure labels or website security features when visiting e-commerce sites?
40. RQ: I don't know what that is.

41. IN: Like "Trygg e-handel"
42. RQ: Yes, "Trygg e-handel", yea, yea. I have two or three I'm buying from, so. And it worked well.

43. IN: Do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?

44. RQ: No, I don't know that.

45. IN: Are there any other measures that you take to keep your information safe when using e-commerce websites?

46. RQ: I do have a software called OneVault, where I keep all my credit card details, and inloggings and everything in one specific...I bought that application actually, so that's why...it's a 32-bit whatever it is to protect it. So it would be very difficult for them to get access. They only get the access to what I provide them so they can't, supposedly not. It's all the inloggings, credit card and everything. OneVault it is called. And the other one is Bank-ID. So when I'm logging in you open up with a long code word. And then you can click on the inlogging and it logs in automatically with your password. And also, when someone does a credit check on me, I get a letter about that.

47. IN: Alright, thank you.

48. RQ: Thank you.

Appendix XIX

Respondent R (RR) – Face-to-face interview

Age: 25; Male; Masters Student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/24
Start time: 15.27
End time: 15.42

1. **IN: How much time per day do you spend browsing the internet?**
2. RR: All day, 8 hours maybe

3. **IN: How many online purchases have you made in the last 3 months?**
4. RR: I only bought some air tickets. I went to London for business trip.

5. **IN: How much money have you spent on those purchases?**
6. RR: I can't remember the total exactly. Around 1000 Danish krona

7. **IN: Well, now we're going to ask something about the factors that influence online shopping choices. Firstly, what is the main factor for you when you decide which website to use, when you're shopping online? For instance, like price, recognition of retailer, delivery time, trustworthiness, convenience, security?**
8. RR: I'd like to say trustworthiness and convenience. Because I rarely shop online, I prefer to go to the store to buy the clothes. Then I could really touch these things and try on. So if I shop online, I will only go to my trusted site, such as Amazon, where I basically would not get the fakes. So the main driver is trustworthiness. Also, convenience, sometimes, the registration is over needed complicated. They ask me input a lot of personal information. That's time consuming. And I feel my privacy and security are threatened. I will not do that.

9. **IN: Okay, so the second question was do you do any type of research about an e-commerce site when using it for the first time?**
10. : No, because I only go to the large e-commerce site, like Amazon. So no research on that.

11. **IN: Well. Let's move to privacy policies. Do usually read through the privacy policies on the sites that you use?**
12. RR: No, never. I think reading these policies does not make much sense to me. And usually, there is a drop-down arrow in the privacy page, I guess the site doesn't really want us to read. Users can go directly to the bottom of the page and click "I agree". As I mentioned, I only use the large e-commerce platform. The amount of user is high. I don't worry about the privacy issues.

13. **IN: Okay, So are you satisfied with the existing formats of privacy policies on the e-commerce websites you use? Such as language, clarity**
14. RR: No. Personally, I think that is a lot of jargon, I do not know what they mean.

15. **IN: Yeah, that's right. Next questions are about uses of cookies. Do you know what the purpose of cookies is, and what are cookies?**
16. RR: I guess cookie could track my preferences and push me advertisements. I personally think this is an advantage of e-commerce. I can totally understand. If you choose e-commerce, you can't avoid this trend. You should do some trade-offs. While, if you really care about your personal information, your privacy. You can always have choices. You could go to the mall instead of giving any information online.

17. **IN: So what is your opinion on cookies, are they beneficial or a nuisance? How do you deal with them?**
18. RR: It's ok, no comments. I don't know how to argue it.

19. **IN: Okay, So next question, are you willing to provide that information to websites in order to get personal targeted advertisements?**
20. RR: I am not willing to share my information. I don't like the ads trash. But I can understand this cannot be completely shielded. In my point view, I don't want to provide the info.

21. **IN: True, Well next one. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?**
22. RR: It depends on the privacy level. If asked too specific info, I would refuse. When I found a product on a small site, in which I have no idea the reputation of the site, what is the site? I will definitely not give my information. If I think my information security is threatened, I simply will leave the site and try to find a new one.

23. **IN: If you do provide personal information to web sites, do you sometimes provide false/different information? Do you use separate email, bank card, nickname for online shopping use?**
24. RR: That's the plan B. As I said, I will not buy it when I feel threatened. If I can only buy it on the untrusted website, I will provide the fake information. Whatever the name, address.

25. **IN: Okay, How do you protect your information when making online payments with credit cards? Have you used an alternative payment method online that you might prefer? Do you use Alipay, Swish, paypal or something similar?**
26. RR: I only use my credit card. As I usually shopping on Amazon. And I will follow the payment operations without any doubt. So trustworthiness again.

27. **IN: Okay, Do you log in to an e-commerce site using your social media account like Facebook, Google?**
28. RR: No, No.

29. **IN: Why?**
30. RR: It is another way to collect more personal information. I do not want to mix the two. Ads everywhere. It's quite annoying. No, I will definitely not associate my social media account.

31. **IN: Okay, so do you actively check for "secure labels" or website security features (e.g. https) when visiting e-commerce sites? If so, why?**
32. RR: Every time. Every time when I pay online. This is the only thing worthy of me to do. I know the https. Yeah.

33. **IN: So do you know of any applicable laws that are in place to help you maintain your privacy and protect your data? Wherever you are in China or Sweden.**
34. RR: Totally no idea.

35. **IN: Okay, last question, do you have any other measures that you take to keep your information safe when you're browsing e-commerce websites?**
36. RR: Firstly, I only shop on my trusted website. Amazon, the large platform. As for the registration, I only provide my information that is mandatory. For the optional item, I will not fill out. Also, I will not make the site store my credit card information.

37. **IN: Okay, thank you for your time.**

Appendix XX

Respondent S (RS) – Face-to-face interview

Age: 23; Male; Master student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/24
Start time: 11.57
End time: 12.11

1. **IN: How much time per day do you spend browsing the internet?**
2. RS: About 7 hours

3. **IN: How many online purchases have you made in the last 3 months?**
4. RS: Only once. I bought a watch for my brother.

5. **IN: Nice, How much money have you spent on those purchases?**
6. RS: 1350 kr (SEK). A DW watch.

7. **IN: Well, now I'm going to ask something about the factors that influence online shopping choices. Firstly, what is the main factor for you when you decide which website to use, when you're shopping online? It's like price, recognition of retailer, delivery time, trustworthiness, convenience, security?**
8. RS: Trustworthiness

9. **IN: Okay, and why?**
10. RS: Because I want to get high quality product. And I only go to the site I trusted, like Tianmao.

11. **IN: Okay, so the second question was do you do any type of research about an e-commerce site when using it for the first time?**
12. RS: Not really. As I mentioned, I only go through the famous sites. Lots of my friends are using it as well. So I trust it.

13. **IN: Well. Let's move to privacy policies. Do usually read through the privacy policies on the sites that you use?**
14. RS: No.

15. **IN: But you know the privacy policies exist, right?**
16. RS: Yeah. it's quite long and boring to read. Again, I trust these sites. I don't think they would bring me into trouble.

17. **IN: Okay, So are you satisfied with the existing formats of privacy policies on the e-commerce websites you use? Such as language, clarity**
18. RS: Yes.

19. **IN: And how come, you just mentioned you thought they are quite long and pointless. Then you are satisfied?**
20. RS: I don't know. I have never read through these kinds of things. But I guess they are useful for other users.

21. **IN: Alright, next questions are about uses of cookies. Do you know what the purpose of cookies is, and what are cookies?**
22. RS: Sorry, I have no idea what cookies are.

23. **IN: but you know the cookies exist on the page, right? Usually, it's displayed on the top of the page. Some buttons stated "I agree".**
24. RS: Yeah, I know it.

25. **IN: So what is your opinion on cookies, are they beneficial or a nuisance? How do you deal with them?**
26. RS: I think they are beneficial but I usually ignore it.

27. **IN: Okay, are you willing to provide that information to websites in order to get personal targeted advertisements?**
28. RS: Yes, I will. Some recommendations are even better than What I found. I'd like to get some advertisements. To know more products.

29. **IN: Interesting, Well next one. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?**
30. RS: I think I will give all they need. Since I haven't met the situation which I have to provide the too personal information. So basically, yes.

31. **IN: So are you afraid of the privacy or security threats?**
32. RS: Yeah, I mean I don't care of them that much. When I was in China, I used Alipay. I think everyone would use it, at least all my friends and my family. So honestly, I don't think about these issues seriously.

33. **IN: Ok, if you do provide personal information to web sites, do you sometimes provide false/different information? Do you use separate email, bank card, nickname for online shopping use?**
34. RS: I will give my real information when I purchase something online. They need my contact info to deliver the goods. As to other purpose, I won't give my info. But I did not give any false or different information before.

35. **IN: Okay, how do you protect your information when making online payments with credit cards? Have you used an alternative payment method online that you might prefer? Do you use Alipay, Swish, paypal or something similar?**
36. RS: I think it's ok. It need be verified by the message. I think it's safe enough. Even if someone know my credit card number, he still cannot get the message token.

37. **IN: Okay, Do you log in to an e-commerce site using your social media account like Facebook, Google?**
38. RS: Yes, it's convenient. I don't have to type the registration info again and again. And I trust my social media platform as well. Sometimes, I am just quite lazy to create a new one.

39. **IN: Okay, so do you actively check for "secure labels" or website security features (e.g. https) when visiting e-commerce sites? If so, why?**
40. RS: No. I don't know what it is. And I usually go to the same e-commerce site.

41. **IN: So do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?**
42. RS: No, not at all, sorry

43. **IN: Okay, last question, do you have any other measures that you take to keep your information safe when you're browsing e-commerce websites?**
44. RS: No, Sorry, I am not a girl who takes the privacy thing seriously.

45. **IN: Okay, thank you for your time.**

Appendix XXI

Respondent T (RT) – Face-to-face interview

Age: 24; Male; Masters student; Intermediate IT knowledge.

Place and date: Lund, 2017/04/27
Start time: 22.57
End time: 23.16

1. **IN: How much time per day do you spend browsing the internet?**
2. RT: About 8 hours

3. **IN: How many online purchases have you made in the last 3 months?**
4. RT: 5 or 6 times, I bought some tickets for my travelling. I'll go to Amsterdam to see the concert next month.

5. **IN: Super, How much money have you spent on those purchases?**
6. RT: More than 3000kr

7. **IN: Well, now I'm going to ask something about the factors that influence online shopping choices. Firstly, what is the main factor for you when you decide which website to use, when you're shopping online? It's like price, recognition of retailer, delivery time, trustworthiness, convenience, security?**
8. RT: For me, it's time-saving... And convenience. I don't think the price is lower as for online shopping. It's almost the same price. Yeah, the main driver is time-saving.

9. **IN: Okay, so the second question was do you do any type of research about an e-commerce site when using it for the first time?**
10. RT: You mean a new site?

11. **IN: Yeah. Maybe not totally a new site. It could be any e-commerce website when you using it at the first time**
12. RT: Alright. I think I will, I need to know the reliability of this site in case of the security issue. But if it's really a famous one, like Amazon, maybe not. .. it depends

13. **IN: Do usually read through the privacy policies on the sites that you use?**
14. RT: No. the reason, for me, is I am still in the study, the address as well as my phone number is temporary. I am not a celebrity. And my privacy value is not that important. So I do not pay much attention to privacy issue. Aha, if I receive some spam from the e-commerce site, I may not go to this site again.

15. **IN: Okay, so are you satisfied with the existing formats of privacy policies on the e-commerce websites you use? Such as language, clarity?**
16. RT: No. Definitely no. Here is too much information piled up together. That makes me lose the desire to read. It is not straightforward. I don't like it at all.

17. **IN: Alright, next questions are about uses of cookies. Do you know what the purpose of cookies is, and what are cookies?**
18. RT: Yeah, I know what it is. It's a kind of memories, I think, it will store my information, the browsing history or extra. Yeah my shopping preference as well. I may get some recommendations and ads.

19. **IN: So what is your opinion on cookies, are they beneficial or a nuisance? How do you deal with them?**
20. RT: I think it's convenient, but not smart enough. Before I make a purchase, I'd like to receive some recommendations. It's beneficial. But the site keeps sending me the ads or recommendations after I bought already. I think it's quite annoying. Some things may not be daily necessities, I only buy it once. It's definitely not a good idea to push me the ads.

21. **IN: Okay, are you willing to provide that information to websites in order to get personal targeted advertisements?**
22. RT: Yes, I will. But the premise is that my personal information would not able to be leaked.

23. **IN: That's true. If asked to provide personal information, are there any reasons that would make you refuse to give the requested personal information? What is your limit as to what information becomes too personal to give out?**
24. RT: If I think the site's reputation is not good, or it's a small company, that means I do not know enough about this site, I will not provide with my personal information. For those sites that are not fully trusted, I am not sure if they will sell my information. So I guess I don't have to take these risks.

25. **IN: Okay, if you do provide personal information to web sites, do you sometimes provide false/different information? Do you use separate email, bank card, nickname for online shopping use?**
26. RT: Sure, due to the security concerns, I will give some false information. Yeah, sometimes.

27. **IN: Okay, how do you protect your information when making online payments with credit cards? Have you used an alternative payment method online that you might prefer? Do you use Alipay, Swish, paypal or something similar?**
28. RT: Not very special, but I would install the antivirus software, security controls, anti-phishing software in advance. It's just the same as any normal user did. I guess. Also, the credit card is safe. I usually would check my credit card bill every month. I would contact my bank, once I find suspicious records. But now everything is fine.

29. **IN: Okay, Do you log in to an e-commerce site using your social media account like Facebook, Google?**
30. RT: No. No. I want they are completely separated. Because once the shopping site can access to your chats record, it is really dangerous.

31. **IN: Okay, so do you actively check for "secure labels" or website security features (e.g. https) when visiting e-commerce sites? If so, why?**
32. RT: Sure, I know https, yeah.

33. **IN: So do you know of any applicable laws that are in place to help you maintain your privacy and protect your data?**

34. RT: No. I guess usually, when people have been violated, they will think about the law. Otherwise, no one would pay attention.

35. IN: Okay, last question, do you have any other measures that you take to keep your information safe when you're browsing e-commerce websites?

36. RT: No, no special one. As I told, I am quite temporary now. Online shopping and privacy issues are not the focus of my life. But I know something, you can create the separate account by using some special naming rule. For instance, you can name your Amazon account as jerryamazon. As for EBay, you can name is as jerryebay. Then you can exactly know which site sends you the spam or which one sell your data or extra. Yeah, maybe this is one kind of measure. Hope it's helpful.

37. IN: Okay, thank you for your time.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker Jr, J. F. (2010). Detecting fake websites: the contribution of statistical learning theory. *Mis Quarterly, 34*(3), 435-461.

Allen & Overy. (2017). The EU General Data Protection Regulation. Retrieved from http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

Ashford, W. (2016). D-Day for GDPR is 25 May 2018. Retrieved from http://www.computerweekly.com/news/450295538/D-Day-for-GDPR-is-25-May-2018

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Mis Quarterly, 30*(1), 13-28.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Basit, T. (2003). Manual or electronic? The role of coding in qualitative data analysis. *Educational research, 45*(2), 143-154.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The journal of strategic Information Systems, 11*(3), 245-270.

Bhattacherjee, A. (2012). *Social science research: principles, methods, and practices* (2nd ed.).

Bishop, M., & Klein, D. V. (1995). Improving system security via proactive password checking. *Computers & Security, 14*(3), 233-249.

Brinkmann, S., & Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of constructivist psychology, 18*(2), 157-181.

Bucholtz, M. (2000). The politics of transcription. *Journal of pragmatics, 32*(10), 1439-1465.

Butler, T. (1998). Towards a hermeneutic method for interpretive research in information systems. *Journal of Information Technology, 13*(4), 285.

Büttner, O. B., & Göritz, A. S. (2008). Perceived trustworthiness of online shops. *Journal of Consumer Behaviour, 7*(1), 35-50.

Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016). *An empirical study of web cookies*. Paper presented at the Proceedings of the 25th International Conference on World Wide Web.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors. *Computers in Human Behavior, 70*, 291-302.

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *Mis Quarterly, 36*(4), 1165-1188.

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: a study of consumer perceptions. *Electronic commerce research and applications, 2*(3), 203-215.

Culnan, M. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of direct marketing, 9*(2), 10-19.

Davidson, C. (2009). Transcription: Imperatives for qualitative research. *International Journal of Qualitative Methods, 8*(2), 35-52.
Dunfee, T. W., Smith, N. C., & Ross Jr, W. T. (1999). Social contracts and marketing ethics. *The Journal of Marketing, 63*(3), 14-32.
Earp, J. B., Antón, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management, 52*(2), 227-237.
Electronic Privacy Information Center. (2017). EPIC - EU Data Protection Directive. Retrieved from https://epic.org/privacy/intl/eu_data_protection_directive.html
Encio, H. A. (2014). Consumers' Perceptions on Privacy and Security in E Commerce. *Journal of Information Engineering and Applications, 4*(4), 14-19.
European Commission. (2017). Protection of personal data. Retrieved from http://ec.europa.eu/justice/data-protection/
Frackman, A., Martin, R. C., & Ray, C. (2002). *Internet and Online Privacy: A Legal and Business Guide*: ALM Publishing.
Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior, 29*(6), 2257-2264.
Gaw, S., & Felten, E. W. (2006). *Password management strategies for online accounts.* Paper presented at the Proceedings of the second symposium on Usable privacy and security.
Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega, 28*(6), 725-737.
Griffith, D. A., & Palmer, J. W. (1999). Leveraging the Web for corporate success. *Business Horizons, 42*(1), 3-10.
Gummesson, E. (2003). All research is interpretive! *Journal of business & industrial marketing, 18*(6/7), 482-492.
Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating Global e-commerce: A Comparison of Consumers' Willingness to Disclose Personal Information Online in the US and in India. *Journal of electronic commerce research, 11*(1), 41.
Hann, I.-H., Hui, K.-L., Lee, T., & Png, I. (2002). *Online information privacy: Measuring the cost-benefit trade-off.* Paper presented at the ICIS 2002 proceedings.
Hillman, R. A. (2006). Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire? *Michigan Law Review, 104*(5), 837-856.
Iachello, G., & Hong, J. (2007). End-user privacy in human–computer interaction. *Foundations and Trends® in Human–Computer Interaction, 1*(1), 1-137.
Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.
Jensen, C., & Potts, C. (2004). *Privacy policies as decision-making tools: an evaluation of online privacy notices.* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in Computing Systems.
Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative science quarterly, 24*(4), 602-611.
Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *Mis Quarterly, 23*(1), 67-93.
Kohavi, R. (2001). *Mining e-commerce data: the good, the bad, and the ugly.* Paper presented at the Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining.
Krishnan, S., Sentosa, I., Nurain, S., Amalia, N., Syamim, S., & Hafizah, W. N. (2017). E-commerce Issues on Customer's Awareness in Malaysia. *International Journal of Finance and Accounting, 6*(1), 8-12.

Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the Craft of qualitative research interviewing* (2nd ed.). Thousand Oaks, CA: Sage.

Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011). Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. *Mis Quarterly, 35*(2), 423-444.

Leyden, J. (2003). Office workers give away passwords for a cheap pen. Retrieved from https://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62-71.

Li, N., & Zhang, P. (2002). *Consumer online shopping attitudes and behavior: An assessment of research.* Paper presented at the AMCIS 2002 Proceedings.

Li, S. S., & Karahanna, E. (2015). Online recommendation systems in a B2C E-commerce context: a review and future directions. *Journal of the Association for Information Systems, 16*(2), 72.

Luzak, J. A. (2014). Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy. *Journal of Consumer Policy, 37*(4), 547-559.

Mayer, J. R., & Mitchell, J. C. (2012). *Third-party web tracking: Policy and technology.* Paper presented at the Security and Privacy (SP), 2012 IEEE Symposium on.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research, 13*(3), 334-359.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335-361.

Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Qualitative data analysis* (3rd ed.): Sage.

Milne, G. R. (1997). Consumer participation in mailing lists: A field experiment. *Journal of Public Policy & Marketing, 16*(2), 298-309.

Mittal, A. (2013). E-commerce: It's Impact on consumer Behavior. *Global Journal of Management and Business Studies, 3*(2), 131-138.

Moon, B.-J. (2004). Consumer adoption of the internet as an information search and product purchase channel: some research hypotheses. *International Journal of Internet Marketing and Advertising, 1*(1), 104-118.

Moores, T. T., & Dhillon, G. (2003). Do privacy seals in e-commerce really work? *Communications of the ACM, 46*(12), 265-271.

Mukherjee, A., & Nath, P. (2007). Role of electronic trust in online retailing: A re-examination of the commitment-trust theory. *European Journal of Marketing, 41*(9/10), 1173-1202.

Murdock, K. (2006). Web Analytics: Data Collection Methods. Retrieved from http://www.practicalecommerce.com/articles/196-Web-Analytics-Data-Collection-Methods

Myers, M. D., & Avison, D. (2002). *Qualitative research in information systems: a reader*: Sage.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25*(2), 243-262.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research, 2*(1), 1-28.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536.
Palvia, P. (2009). The role of trust in e-commerce relational exchange: A unified model. *Information & Management, 46*(4), 213-220.
Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), 331-338.
Panda Security Mediacenter. (2014). How do cookies work? - Panda Security Mediacenter. Retrieved from http://www.pandasecurity.com/mediacenter/security/cookies/
Perreault, L. (2015). *Big Data and Privacy: Control and Awareness Aspects.* Paper presented at the CONF-IRM 2015 Proceedings.
Peslak, A. R. (2006). Internet Privacy Policies of the Largest International Companies. *Journal of Electronic Commerce in Organizations (JECO), 4*(3), 46-62.
Petronio, S. (2002). *Boundaries of privacy: dialectics of disclosure*. Albany, NY State University of New York Press.
Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by. *Journal of Family Communication, 4*(3-4), 193-207.
Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*(1), 6-14.
Petronio, S., & Reierson, J. (2009). Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory. In T. Afifi & W. Afifi (Eds.), *Uncertainty, information management, and disclosure decisions: Theories and applications* (pp. 365-383). New York, NY: Routledge.
Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM, 50*(9), 103-108.
Pötzsch, S. (2008). *Privacy awareness: A means to solve the privacy paradox?* Paper presented at the IFIP Summer School on the Future of Identity in the Information Society.
Proctor, R. W., Lien, M.-C., Vu, K.-P. L., Schultz, E. E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, 34*(2), 163-169.
Ramlakhan, N. E. (2011). Ethical Implications of Third-party Cookies. *International Journal of the Humanities, 9*(1), 59-68.
Recker, J. (2013). *Scientific research in information systems* (1st ed.). Berlin: Springer.
Russharvey Consulting. (2017). Passwords: Strategies for Generating and Remembering Effective Passwords | Russ Harvey Consulting. Retrieved from https://www.russharvey.bc.ca/resources/passwords.html
Rust, R. T., Zeithaml, V. A., & Lemon, K. N. (2004). Customer-centered brand management. *Harvard business review, 82*(9), 110-120.
Sarwar, B., Karypis, G., Konstan, J., & Riedl, J. (2000). *Analysis of recommendation algorithms for e-commerce.* Paper presented at the Proceedings of the 2nd ACM conference on Electronic commerce.
Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information, 22*(2), 63-75.
Smith, J. K. (1983). Quantitative versus qualitative research: An attempt to clarify the issue. *Educational researcher, 12*(3), 6-13.
Srinivasan, S. S., Anderson, R., & Ponnavolu, K. (2002). Customer loyalty in e-commerce: an exploration of its antecedents and consequences. *Journal of Retailing, 78*(1), 41-50.

Srivastava, J., Cooley, R., Deshpande, M., & Tan, P.-N. (2000). Web usage mining: Discovery and applications of usage patterns from web data. *Acm Sigkdd Explorations Newsletter, 1*(2), 12-23.

Stanton, J. M., & Stam, K. R. (2002). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance & Society, 1*(2), 152-190.

Turner, E. C., & Dasgupta, S. (2003). Privacy on the Web: an Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. *Information Systems Management, 20*(1), 8-18.

Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: a survey study. *Information Management & Computer Security, 9*(4), 165-174.

Van Teijlingen, E., & Hundley, V. (2002). The importance of pilot studies. *Nursing standard, 16*(40), 33-36.

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757.

Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychological bulletin, 132*(2), 249.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Mis Quarterly, 26*(2), xiii-xxiii.

Weltevreden, J. W., & Rotem-Mindali, O. (2009). Mobility effects of b2c and c2c e-commerce in the Netherlands: a quantitative assessment. *Journal of Transport Geography, 17*(2), 83-92.

Whitman, M. E., Perez, J., & Beise, C. (2001). A study of user attitudes toward persistent cookies. *Journal of Computer Information Systems, 41*(3), 1-7.

Wu, X., & Bolivar, A. (2009). *Predicting the conversion probability for items on C2C ecommerce sites.* Paper presented at the Proceedings of the 18th ACM conference on Information and knowledge management.

Yazdanifard, R., WanYusoff, W. F., Behora, A. C., & Sade, A. B. (2011). Electronic Banking Fraud; The Need To Enhance Security And Customer Trust In Online Banking. *Advances in information Sciences and Service Sciences (AISS), 3*(10), 505-509.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems, 16*(6), 448.