**Universidade de Évora - Instituto de Investigação e Formação Avançada**

Programa de Doutoramento em Gestão

Tese de Doutoramento

# Individual values of GenZ in managing their Internet Privacy: a decision analytic assessment

Simran Kaur Dhillon

Regime Especial de Apresentação de Tese

**Universidade de Évora - Instituto de Investigação e Formação Avançada**

Programa de Doutoramento em Gestão

Tese de Doutoramento

# Individual values of GenZ in managing their Internet Privacy: a decision analytic assessment

Simran Kaur Dhillon

Regime Especial de Apresentação de Tese

# Contents

## Index of Figures

## Index of Tables

## Index of Boxes

## Acronyms used

AFT: Alternative Focused Thinking

AHP: Analytic Hierarchy Processing

ERP: enterprise resource planning

GDPR: General Data Protection Regulation

GenZ: Generation Z

GPS: Geo Positioning Satellite

IS: Information Systems

MODA: Multi-Objective Decision Making

RFID: Radio Frequency Identification

US: United States

VFT: Value Focused Thinking

WITI: What is This Important

**Os valores individuais da geração Z na gestão da sua privacidade na internet: uma avaliação analítica da tomada de decisão.**


## Abstract

A nossa investigação coloca a importância dos valores individuais como o centro de qualquer discussão sobre questões de privacidade. Os valores têm um papel essencial no discurso científico. Notamos que o conceito de valores é um dos poucos discutidos e utilizados em várias disciplinas das ciências sociais. Para isso, nesta investigação, apresentamos objetivos baseados em valores para a privacidade na Internet da GenZ. Os objetivos são classificados em duas categorias - os objetivos fundamentais e os meios para os atingir. Em síntese, os nossos seis objetivos fundamentais orientam a gestão das questões de privacidade da Internet da GenZ. Os objetivos são: Aumentar a confiança nas interações online; Maximizar a responsabilidade dos detentores de dados; Maximizar o direito à privacidade; Maximizar a capacidade individual de gerir o controlo da privacidade; Maximizar a percepção da funcionalidade da plataforma; Garantir que os dados pessoais não são alterados.

Coletivamente, os objetivos fundamentais e de meios são uma base valiosa para a GenZ avaliar a sua postura de privacidade. Os objetivos também são úteis para que as empresas de media social e outras plataformas relacionadas elaborem as suas políticas de privacidade de acordo com o que a GenZ deseja. Finalmente, os objetivos são uma ajuda útil para o desenvolvimento de leis e regulamentos.



**Palavras-chave:** Privacidade da informação; Valores individuais; Pensamento focado no valor; Pesquisa qualitativa

**Individual values of GenZ in managing their Internet Privacy: a decision analytic assessment**


## Abstract

Online privacy is a growing concern. As individuals and businesses connect, the problem of privacy continues to remain significant. In this thesis, we address three primary questions - What are the individual values of GenZ concerning online privacy? What are the fundamental objectives of GenZ in terms of protecting their online privacy? What are the means objectives GenZ consider for protecting their online privacy? We argue that online privacy for GenZ is vital to protect. We also argue that protection can be ensured if we understand and know what privacy-related values behold GenZ and define their objectives accordingly.

Our research brings the importance of individual values to be central to any discussion of privacy concerns. Values have an essential place in scientific discourse. We note that the concept of values is one of the very few discussed and employed across several social science disciplines. To that effect, in this research, we present value-based objectives for GenZ internet privacy. The objectives are classified into two categories – the fundamental objectives and the means to achieve them. In a final synthesis, our six fundamental objectives guide the management of GenZ Internet Privacy Concerns. The objectives are: Increase trust in online interactions; Maximize responsibility of data custodians; Maximize right to be left alone; Maximize individual ability to manage privacy controls; Maximize awareness of platform functionality; Ensure that personal data does not change.

Collectively our fundamental and means objectives are a valuable basis for GenZ to evaluate their privacy posture. The objectives are also helpful for the social media companies and other related platforms to design their privacy policies according to the way GenZ wants. Finally, the objectives are a helpful policy aid for developing laws and regulations.

**Keywords**: Information privacy; Individual values; Value focused thinking; Qualitative research

**Dedication**

The thesis is dedicated to my family

# 1
# Introduction

## 1.1 Problem Statement

Online privacy is a growing concern. In 2018 when MyFitnessPal, owned by Under Armor, witnessed a breach of 617 million customers, it sent tremors among the App users. And rightly so because over half of the US populations owns an app-enabled phone and a significant proportion of them had a health-related app (see Krebs and Duncan, 2015). In 2019 Zynga (a gaming company created by Farmville developers) reported that 218 million user accounts were compromised where email addresses, passwords, phone numbers and user IDs for Facebook and Zynga were stolen. The privacy breaches are of a significant concern since various surveys suggest that ninety percent of teenagers (13-17 age group) are active social media users. On an average, teens are active online for nearly nine hours a day[1].

How can, then, we protect individuals from privacy invasion? How can young adults, in particular, be protected? What are the values of young adults regarding online privacy? What objectives should drive companies to design their privacy policies? Research presented in this

[1] Source: AACAP.org (https://bit.ly/34yOtz9)

thesis, addresses all of these questions. We argue that online privacy for GenZ is important to protect. We also argue that protection can be ensured if we understand and know what privacy related values behold GenZ and hence define their objectives accordingly.

## 1.2 Definitions

There are two categories for definitions that lay the foundation of this work – GenZ and Online Privacy. We will discuss each of these below.

**GenZ**. In the literature there is some confusion as to what "GenZ" means. For the purposes of our study, we adopt the definition proposed by Pew Research Center where Demock (1999) discusses the cut-off between Millennial and Generation Z. Today most of the Millennials are well into adulthood, where many of them are turning 38 or 39. In order for the generations to be analytically meaningful, Pew Research notes the following:

> Pew Research Center decided a year ago to use 1996 as the last birth year for Millennials for our future work. Anyone born between 1981 and 1996 (ages 23 to 38 in 2019) is considered a Millennial, and anyone born from 1997 onward is part of a new generation (see Demock, 1999).

Hence, the new generation has been termed Generation Z (GenZ). The oldest of the GenZ people are just turning 22 or 23 (as of 2020). But many of them are as young as teenagers. According to Pew Research, a meaningful cut-off point between Millennials and GenZ is 1996. In 2020, GenZ would be in the 7-22 age group. There are a few interesting points to note about GenZ, and the reason why our study focuses on this age group. iPhone was launched in 2007. The oldest of the GenZers were 10-year-old (now about 23-year-old). By the time this population was in their teens, the primary means of communication for this generation was through mobile devices. Constant connectivity and on-demand entertainment came natural to this generation. In a sense, GenZers are "new technology" natives.

**Online Privacy**. While privacy has been defined as the "right to be left alone", Parent (1983) puts is very succinctly when he notes:

> Defining privacy requires a familiarity with its ordinary usage . . . but this is not enough since our common ways of talking and using language are riddled with inconsistencies, ambiguities, and paradoxes. What we need is a definition which is by and large consistent with ordinary language, so that capable speakers of English will not be genuinely surprised that the term ‘‘privacy’’ should be defined in this way, but which also enables us to talk consistently, clearly, and precisely about the family of concepts to which privacy belongs. (pg. 269)

Addressing the requirements presented by Parent are challenging. Guided by him though, in this thesis we consider privacy protection to be important since it allows individuals to plan their lives in a certain way. Privacy enables sustaining of private situations, which allow for intimacy and a personalized relationship. Privacy also allows for increased control over one's lives, which in effect leads to increased autonomy.

Following on from prior research (e.g see Dhillon, Oliveira and Syed, 2018), we take an individual perspective in defining privacy. In that sense, we consider privacy to be the values that individuals hold regarding their own identity. Implicit in our definition of privacy is the ability of individuals to control their data and information.

## 1.3 Significance

When discussing the significance of the research on privacy and particularly of GenZ, one needs to consider three aspects which are important. These are:

1) Privacy and how it benefits the individual
2) Privacy and benefits to personal relationships
3) Privacy and benefits to society

**Privacy and how it benefits the individual.** This is an important consideration. At a very basic level, privacy protects individuals from overreach in their daily interactions and thus providing time and space for individual relaxation. In an online environment, this aspect is

particularly important since privacy breaches can have a devastating effect on all aspects of relaxation and individual space. Privacy also reinforces the concept of "self-ownership," i.e. the notion that each individual owns their own body and thoughts (e.g. see Reiman, 1976). Self-ownership is important to consider, particularly since privacy violations such as cyber stalking are largely silent. As Charles Fried (1968) notes this is to be the most basic form since privacy serves not just to protect "things" that we share, i.e. online information, but to protect certain thoughts as well.

**Privacy and benefits to personal relationships.** In the literature there are conflicting claims of secrecy and privacy. Scholars have argued in favor of one over the other. Rosen (2000) however notes:

> "even those who claim that society would be better off if people were less embarrassed about discussing their sexual activities in public still manage to feel annoyed and invaded when they are solicited by telemarketers during dinner" (pg. 210).

Rosen's argument is based on the conception that people hold a simplistic view of secrecy and that individuals misrepresent themselves by using "social masks." Privacy therefore offers the conditions for defining different versions of self. Privacy is also considered to support intimacy. When dealing with individuals, Rosen (2000) has argued that people flourish when they have the true knowledge of the other person. This suggests that in cases where individuals need to develop personal relationships, there is a need to have some level of transparency. The requirement for transparency however gets complicated, particularly when we consider online platforms such as dating sites.

**Privacy and benefits to society.** Scholars have argued that privacy supports society's common good. While privacy may result in individual concerns, the common good for society needs appreciation. As Solove (2005) has argued that privacy problems are not just about the harm that is caused to individuals but can also impede individual activities, which may result in a greater good. Researchers have also argued about the impact that privacy has on power

imbalance between individuals and government while also supporting democracy, political activity and service.

Clearly the study of privacy is of significance and what GenZ member consider to be important with respect to privacy, is even more important. In this thesis we explore all these aspects. In particular we address the following research questions:

***Research Question 1:*** What are the individual values of GenZ with respect to online privacy?

***Research Question 2:*** What are the fundamental objectives of GenZ in terms of protecting their online privacy?

***Research Question 3:*** What means objectives GenZ consider for protecting their online privacy?

## 1.4 Structure of the Thesis

The thesis is organized into seven chapters. A brief synopsis of each of the chapters is presented below:

Chapter 1 presents the argument, definitions and research questions for the thesis.

Chapter 2 presents a review of the literature on privacy and the relevance of individual values. The literature is classified into relevant categories and a systematic position is established for the current research.

Chapter 3 presents the methodology used to undertake the research. Details of value-focused thinking and the approach are presented. Study design for this research is also discussed. The chapters also present the theoretical and philosophical foundations of research.

Chapter 4 presents a pilot study. The study was used to practice interview skills and evaluate how values could be interpreted.

Chapter 5 presents the findings of this research. Fundamental objectives for online privacy protection for GenZ are presented and discussed. The means of achieving the objectives are also presented and discussed.

Chapter 6 discusses the significance of the findings. The role of values and GenZ with respect to online privacy protection is discussed.

Chapter 7 concludes the thesis with a discussion of theoretical and practical implications. Limitations and future research directions are also discussed.

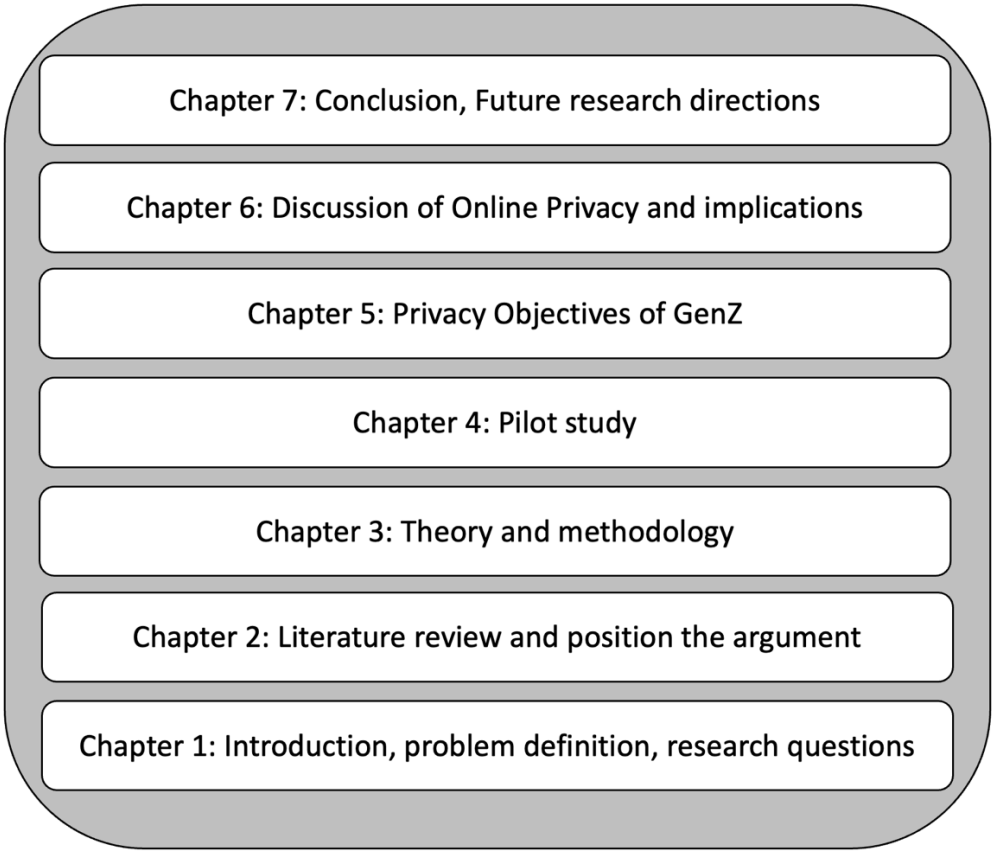


*Figure 1.1, Structure of the thesis*

# 2
# Literature Review

## 2.1 Introduction

In this chapter we present a review of privacy of information literature. Privacy has been studied in great detail in the field of Information Systems (IS). Warren and Laslett (1977) assume that privacy suggests something that is positive and would help individuals take a more proactive decision towards security. Some authors have also described privacy as an elastic concept that has little shared meaning among individuals (Allen, 1988). A different context would perhaps imply a different meaning to the concept of privacy.

With numerous interpretations of privacy as a concept, most of today's privacy research relies on the work of Westin (1967) and Altman (1975). Alan Westin did significant work on consumer data privacy and data protection. *Privacy and Freedom* (1967) and *Databanks in a Free Society* (1972) were among the major books on privacy written by Westin. Irwin Altman (1975) developed the Privacy Regulation Theory which explains why at times people prefer to

stay alone and at other times want to have social interactions. It considered 'privacy' as "a selective control to access to the self or to a group". In the context of sociology, the goal of privacy is to achieve an optimum level of privacy by creating dynamic boundary regulations. Altman's Privacy Regulation Theory has five properties, out of which, desired and actual levels of privacy is of special interest in the domain of Information Systems. The desired level of privacy is the amount of privacy that is essential for a person's own needs and role requirements, whereas, actual levels refer to the amount of privacy a person achieves in the real world. In the domain of Information Systems, this is generally addressed as the privacy paradox, where there is a difference in the stated and actual privacy concerns.

When it comes to information sharing and disclosure, Mason (1986) suggested four major concerns about the use of information, namely privacy, accuracy, property, and accessibility. The online platforms have opened a wide range of opportunities for researchers in IS to explore these main concerns. Culnan (1993), Smith et al. (1996) and Stewart and Segars (2002) explore information privacy as the extent to which individuals are concerned and disturbed about the information collection policies and practices, especially on online platforms and communities. Another aspect of concern among individuals is how the acquired information (financial, healthcare, or general information) will be used.

Information privacy has been studied and explored not only in IS, but also in marketing, law, management, psychology, and many other fields. Researchers across domains have debated the conceptualization of information privacy, antecedents of the concept of information privacy, and have tried to understand how to protect information privacy.

## 2.2 What Is Information Privacy?

Margulis (2003) developed a behavioral perspective of privacy based on Altman's (1977) and Westin's (1967) definitions of privacy. In his analysis of their privacy theories, he was able to identify two important factors of privacy: control over disclosure of personal information

and a notion of vulnerability (Margulis 2003). According to Margulis (2003), privacy involves control over transactions that regulate access to self, such that it reduces vulnerability and increases decisional and behavioral options. While Margulis' conceptualization is valid, the debates over the concept of privacy will continue to vary because its definition will depend on the context and viewpoint from which it is to be examined.

In his earlier work, Margulis (1977) argued that when considering privacy as a psychological concept, it subsumes a range of issues. The relationship between privacy and concepts such as deception, anonymity, and secrecy become debatable since there is little agreement about the boundaries of what is private and what is not. Warren and Laslett (1977) have argued that privacy protects morally neutral behavior or behavior that is valued by society. There are other scholars though who consider privacy neutrally since it can facilitate and support illegitimate activities, including dubious behavior (see Derlega and Chaikin, 1977; Altman, 1977).

Since the psychological concept of privacy emphasizes privacy in terms of control and hence has limitations concerning scrutiny and surveillance, scholars such as Allen (1988) have made calls for considering privacy much more narrowly in terms of limiting access. From a legalistic point of view, particularly the US Fourth Amendment, finding privacy in terms of limited access is appropriate. This is because such a conceptualization of privacy protects individuals from unreasonable searches (e.g., by police during a criminal investigation). Law enforcement, therefore, has to establish 'probable cause' to engage in a search.

The issue of probable cause and access limitation came to light when in late 2015, the US Federal Bureau of Investigation wanted access to the locked iPhone of the San Bernardino shooter. Apple had refused all FBI demands, which resulted in a furious discourse over privacy. Eventually in 2016 a federal judge ordered Apple to assist investigators in gaining access to

the encrypted data[2]. Prosecutors had argued that the iCloud account contained evidence of communication between the victims and the shooter. Another issue that emerged between 2015 and 2017 was the search of electronic devices by the US Customs and Borders Protection agents. Eventually, a ruling came in *Alasaad v. McAleenan* that "suspicionless" searches by border agents violated the Fourth Amendment. The *Alasaad v. McAleenan* suit was filed by the American Civil Liberties Union and the Electronic Frontier Foundation on behalf of 11 travelers[3].

As noted previously, in the literature, there are two informing theories of privacy – Altman (1977) and Westin (1967), which have subsequently been used in the information systems literature. Both theories emphasize the limited access approach, which was evidenced in the *Alasaad v. McAleenan* case. While Westin emphasizes the privacy-secrecy linkage, Altman considers the central relationship between privacy and the environment. Furthermore, Westin focuses on types and functions of privacy, while Altman focuses on the process of regulating social interactions. Consistent with Margulis (1977), Altman (1977) and Westin (1967) personal information privacy, therefore, is the ability of the individuals to control transactions that regulate access to one's personal information, such that it reduces vulnerability and unwanted disclosure.

**Information Privacy**

After Mason's (1986) seminal work identifying privacy as one of the biggest ethical concerns for the information age, information systems researchers increased their focus on the notion of information privacy (Straub and Collins, 1990; Culnan, 1993; Milberg, et al., 1995). Studies have viewed privacy from many different perspectives such as a moral or legal right

[2] https://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701

[3] https://jolt.law.harvard.edu/digest/alasaad-v-mcaleenan-federal-district-court-rules-suspicionless-searches-of-smart-phones-at-u-s-ports-of-entry-unconstitutional

and the ability to control one's personal information (Stone et al., 1983; Bélanger and Crossler, 2011; Clarke 1999; Dhillon, Oliveira, and Syed 2018). A main consideration with respect to information is with the control of information (Katzan, 2010). Straub and Collins (1990) considered the collection and dissemination of information on individuals while respecting individual rights to privacy an important topic of concern. Organizations have typically argued that the enterprise that creates or maintains the information should have control of it. However, individuals typically believe that they should have the ability to control their identity and the release of information about themselves.

Within the information privacy literature, organizational practices, individual perceptions of these practices and societal responsibilities with respect to privacy have been linked in many ways (Smith et al, 1996). Clarke (1999) defines information privacy as "the interest people have in controlling, or at least significantly influencing, the handling of information about themselves". The concept of information privacy has been difficult to quantify with a confirmatory empirical approach. Smith et al. (1996) developed an information privacy concern measurement scale as a proxy for information privacy. They identified the following four data-related dimensions of information privacy concerns: data collection, data errors, secondary use of data and unauthorized access to information. Due to the complexity and difficulty of defining privacy many researchers have opted to use the information privacy concern scale as a proxy for the concept of privacy (Dinev et al., 2009). While this acceptance has allowed for some advancement in the realm of privacy research there still is some concern that the information privacy concern scale is based on a negative notion of privacy and is thus not a true measure of privacy (Dinev et al. 2009).

**Online Privacy**

The ability of online websites or web application to track individual preferences, behaviors, and identity is also a concern for individual's privacy. With the pervasiveness of the Internet,

the research topic of online privacy has been a very popular topic among scholars. Research topics such as information privacy concerns (Son and Kim 2008; Pavlou, Liang and Xue, 2007; Hann, Hui, Lee and Png, 2007; Malhotra, Kim and Agarwal, 2004; Wang, Lee, and Wang, 1998; Smith et al, 1996), trust and privacy relationships (Tang, Hu and Smith, 2008; Dinev, Bellotto, Hart, Russo, Serra, and Colautti, 2006; Hoffman, Novak and Peralta, 1999), and privacy policies (Mai, Menon and Sarkar, 2010; Hann, Hui, Lee and Png, 2007) are similar whether the context is online or in traditional organizational settings. However, new research topic areas such as the effects of privacy seals (Hui, Teo and Lee, 2007; Mai, Menon and Sarkar, 2010), privacy statements (Hui, Teo and Lee, 2007), personalization and privacy tradeoffs (Awad and Krishnan, 2006; Hann, Hui, Lee and Png, 2007) have also emerged as relevant research topics.

As a means to address the question as to why consumers are reluctant to participate in online activities, Pavlou et al. (2007) consider the implications of agency problems of adverse selection and moral hazard. They identified information privacy concern as an antecedent of perceived uncertainty in online buyer-seller relationships. Malhotra et al. (2004) addressed this same issue by drawing upon social contract theory to propose a theoretical framework of Internet users' information privacy concerns. Hann et al. (2007) used expectancy theory in the context of motivated behavior to explore ways to mitigate individuals concern for privacy. Son and Kim (2008) considered individuals' responses to information privacy threats online and classified them into three categories: information provision, private action, and public action. Through their creation of a nomological network the authors were able to show how various customer responses are manifested in ways to protect the privacy of their information. They recommend that Organizations' information practices give proper consideration to customers' potential responses to such organizational practices (Son and Kim, 2008).

Trust is crucial in transactional, buyer-seller relationships, especially those containing an element of risk including interacting with web-based systems (Reichheld and Schefter, 2000). Dinev et al. (2006) adapted Culnan and Armstrong's (1999) privacy calculus model such that if the total effect of trust and control is higher than the total effect of privacy concerns and perceived risk, the user is likely to engage in an online transaction. Research has shown that trust between online business and its customers can be achieved by allowing the balance of power to shift towards a cooperative interaction environment (Hoffman and Novak, 1997). Wang et al. (1998) claim that a consumer-oriented information privacy model will lead to a profitable business model for online transactions. In order to achieve a balance of power in online transactions, businesses need to recognize consumers' rights to data ownership and offer opt-out or opt-in policies regarding information exchanges (Hoffman, Novak and Peralta, 1998). Tang et al., (2008) found that the ability to influence consumers' beliefs about trusting online transactions is a result of how clearly, they communicate their intention to protect customers' privacy. The literature suggests several ways businesses can signal their intentions to protect customers' privacy in online transactions. These include posting privacy statements, establishing privacy policies, and utilizing privacy seals.

Mai et al. (2010) found during their investigation of businesses using privacy seals that vendors' websites with privacy seals could charge a premium for the same products compared to vendors' websites without a privacy seal. Hui et al. (2007) performed a study evaluating the effects of websites displaying a privacy statements or a privacy seal and found that displaying a privacy statement had significant effect on individuals disclosing their personal information where displaying privacy seals did not. Moores and Dhillon (2003) found that privacy seals increased customer confidence in the websites significantly. However, online customers might be unduly placing trust in these websites because they unknowingly think these seals protect against fraud, which they do not. Organizations have the ability to actively manage the privacy

concerns of Internet users by stating their privacy policy more prominently on their website because research has shown that privacy policies are valued by users (Hann et al. 2007).

Internet companies offer to personalize the online shopping experience for their customer as a means to build brand loyalty. The personalization process typically requires the customer to provide their personal and preferences information such that the website can recall their information the next time they visit the site. Organizations that offer personalization need to consider the tradeoff customers make between their value for personalization and concern for privacy (Chellappa and Sin, 2005). A positive aspect of Web-based personalization for Internet companies is that it increases switching costs for its customers and serves as an important means of acquiring valuable customer information. A negative aspect is that customers may not value online personalization if they have privacy concerns about providing the requested information. Chellappa and Sin (2005) found that a customer's intent to use personalization services is positively influenced by their trust in the Internet Company they are doing business with. Awad and Krishnan (2006) examined the relationship between information transparency features and customer willingness to share information for online personalization. They found that customers who require information transparency are less willing to participate in personalization services. Internet organizations should accept the fact that the privacy sensitive consumers are unwilling to participate in personalization, despite additional privacy features and they should not overtly exhaust resources trying to get these customers to buy into the personalization process (Awad and Krishnan, 2006). Research has shown that it is important for online companies to understand and evaluate the values consumers have in the personalization and privacy relationship (Chellappa and Sin, 2005).

**Location based privacy**

The concept of personal privacy refers to keeping confidential those things that an individual does not want known, such as a person's location (Solove, 2006). Ever since George

Orwell penned the novel 1984, citizens of every free society have a fear that their government will track their every movement and invade their privacy with the use of technology. The development of new technologies such as GPS, mobile computing and Radio Frequency Identification (RFID) allows organizations the opportunity to collect ever more information about their customers (Pramatari and Theotokis, 2009). Location based services use these technologies to provide their customers with personalized information however it may cost them their privacy because these technologies track their preferences, behaviors, and identity (Xu, Teo, Tan and Agarwal, 2009).

Research shows that information privacy concern affects the consumer attitude towards RFID-enabled services (Pramatari and Theotokis, 2009). A positive point about RFID technologies is that it allows companies to track products through the entire supply chain from the raw material phase to the point of sale to the end customer and possibly beyond (Kapoor, Zhou and Piramuthu, 2009). This ability to track products through the supply chain allows for organizations to effectively monitor their production processes and ultimately lower their costs and increase profitability. However, the part of concern is the fact that organization can still use some of these tracking technologies after they have sold the product to their customers and analyze information about their customers' habits.

## 2.3 Privacy Ethics and Society

In exploring the ethical implications of the information age, Mason (1986) identified privacy as one of the four primary ethical issues in the information age. Mason (1986) was concerned with "what information about one's self or one's associations must a person reveal to others?" (p. 5). He argued that two aspects of the information age pose a threat to our privacy; the first is the growth of information technology and its capabilities to capture and process information, second is the increased value of information in the decision-making process, particularly because of the increased amount of information being collected by organizations.

Culnan and Williams (2009) argue that organizations have a moral obligation that extends beyond legal compliance to take reasonable precautions with consumer data and to avoid causing personal harm by misuse of their personal information. Research shows that organization's privacy behaviors tend to be reactive and are driven by external pressures such as regulatory factors instead of being proactive with their privacy practices (Goodhue and Straub 1991; Greenaway and Chan, 2005; Smith 1993). Culnan and Williams (2009) suggest that organizations develop principles based on shared moral values by which to guide the creation of privacy practices.

The concept of privacy is dependent on the current privacy values and norms that exist within society. Privacy as social issue has increased for Americans especially since 9/11 and the passage of the USA Patriot Act (Gandy, 2003). Margulis (2003) examines privacy from three distinct positions: high-privacy position, balanced-privacy position and limited privacy position. The high-privacy position wants government to protect privacy rights. The balance-privacy position wants some government intervention along with voluntary organizational programs to encourage individual privacy. The limited-privacy position desires business efficiency and societal protection over individual privacy rights.

The legal aspects of information privacy are very complex. Even though privacy has been argued to be protected by the fourth amendment and several other state and federal privacy statutes such as the constitutional right to information privacy (Solove, 2006), its management remains difficult. Historically, it has been the responsibility of individuals to create contracts with organizations such as healthcare providers for protection of their personal data (Smith, Milberg and Burke, 1996). Privacy contracts are a means to ensure that all parties involved have a clear understanding as to what their responsibility is towards the protection of the individuals' or organization's privacy. A summary of privacy research is presented in table 2.1.

*Table 2.1, A summary of major online privacy research*

| Theme | Author | Context | Method | Major theme |
|---|---|---|---|---|
| Systems Level Data Privacy Protection | Menon et al. (2005) | Data Mining | Analytical Experiment | Item set mining conceals sensitive data patterns at the time of data mining from shared database. |
| | Li et al. (2006) | Data Mining | Optimization | Perturbation method for categorical data preserve the statistical properties of the data based on privacy protection parameters. |
| | Garfinkel et al. (2007) | Health Information | Optimization | Recoding approach protects individual's identifiable data. |
| | Li et al. (2011) | Identity Matching | Analytical Experiment | Data partitioning and data swapping hinder the record linkage of identity matching from identifiable data. |
| | Melville et al. (2012) | Shared Database | Optimization | Hybrid data masking hides sensitive data while preserving the statistical utility. |
| | Li et al. (2017) | Health Information | Analytical Experiment | Algorithmic and systematic approach extract, cluster, and anonymize sensitive data. |
| | Ghoshal et al. (2020) | Shared Database | Analytical Experiment | Machine learning approach to hide sensitive information when sharing distributed transactional data. |
| Privacy and Information Disclosure | Tsai et al. (2011) | Electronic Commerce | Experiment (Causal) | When privacy policy information is clearly stated and accessible, consumers are willing to pay a premium to purchase from privacy protected websites. |
| | Anderson et al. (2011) | Healthcare | Survey | Emotion plays a significant role towards information disclosure decision. |
| | Choi et al. (2015) | Social Networks | Experiment (Causal) | Information dissemination and network commonality jointly influence individual's perceived privacy invasion and perceived relationship bonding. |
| | Cavusoglu et al. (2016) | Social Networks | Natural Experiment | Granular privacy controls lead to an increase in wall posts and decrease in private messages. |
| | Cao et al. (2018) | Social Networks | Analytical Modelling | Any regulation that uniformly control the disclosure of sensitive and nonsensitive information will not reduce privacy harm, not increase social welfare, and not increase information sharing. |
| | Buckman et al. (2019) | Electronic Commerce | Experiment (Causal) | Increased saliency and awareness lead to higher privacy valuation. |
| Privacy Protective Behavior | Xu et al. (2012) | Location-based | Econometrics | Perceived control over personal information is a key factor affecting the decision to opt-in. |
| | Jiang et al. (2013) | Social Networks | Survey | Perceived anonymity increases social media engagement. |
| | Crossler et al. (2019) | Location-based | Econometrics on iPhone users | Personal motivation is one of the strongest determinants of utilizing privacy-protective mobile phone settings. |
| Personalization and Privacy Calculus | Dinev et al. (2006) | Electronic Commerce | Survey | Internet privacy concern inhibit e-comm transactions, personal interest can outweigh privacy risk perceptions of info sharing. |
| | Wattal et al. (2012) | Email Advertising | Econometrics | Product based personalization increases customer response, personal identifiable information based personal increases privacy concern. |
| | Acquisti et al. (2018) | Prospect Theory | Survey | Risk of disclosure, consumer privacy choices, Privacy decision-making |
| | Awad and Krishnan (2006) | Privacy calculus | Survey | Information transparency and consumer willingness in online profiling |
| Other | Gal-or et al. (2018) | Market Competition | Analytical Modelling | Privacy policy strengthening and disclosure can act as a competition mechanism among firms |
| | Kim et al. (2019) | Healthcare | Econometrics | Implementing electronic health record leads to a 3.081 times higher risk of a breach of patient information. |

## 2.4 Emergent issues

In this section we discuss the emergent online privacy issues as identified in the literature. We classify the emergent issues into four categories: System Level Data Privacy Protection; Privacy and Information Disclosure; Privacy Protective Behavior; Personalization and Privacy Calculus.

**Systems Level Data Privacy Protection**

Menon et al (2005) talks about how sharing databases in an organization can increase the possibility of intentional and unintentional sharing of sensitive information. In the context of data mining Mennon et al's research focuses on item sets whose identification is considered as critical. Using the method of analytical and computational experiment the research finds that, item set mining conceals sensitive data patterns at the time of data mining from shared databases.

Organizations are mining their customers' data to identify behavior patterns. However, it is a growing concern that organizations need to protect the customers' data while mining the data. There is a common practice of removing identity related attributes from the customer data. Li et al (2006) investigate effectiveness of this practice. According to the researchers, many records in the data set can be uniquely identified even after the removal of identity attributes. They propose a perturbation method for categorical data to preserve the statistical properties of the data based on privacy protection parameters.

Other than these, system level data privacy protection has been studied in the context of health information. Because of the sensitive nature of health information, it is very important to protect individual's health information. Revealing of individual's health information can impact overall well-being. Garfinkel et al (2007) investigate the security issues in releasing individual level micro data including unique identities. Using the optimization method, the researchers find that recoding approach protects an individual's identifiable data.

Identity matching is another privacy concern in today's world. Identity matching techniques such as record linkage have been used for antiterrorism and in criminal cases. However, such techniques are now being used for identity matching and disclosure of private information. There is no doubt that individuals' privacy is at risk because of such techniques. Li et al (2012) investigate this problem and provide solutions to resolve this conflict between data protection and data utility. Using an analytical and computational experimental method the researchers conclude that data partitioning and data swapping hinder the record linkage of identity matching from identifiable private data.

**Privacy and Information Disclosure**

Extant literature has emphasized a lot on individual's information disclosure behavior in the context of social network, electronic commerce, and healthcare. Tsai et al (2011) investigate the information disclosure behavior in the context of electronic commerce. The problem the researchers identified is, online retailers have information privacy policies, but there still are privacy breaches. The privacy policies remain invisible to the customers who very often do not bother to find and read the policy. The researchers investigate whether a more prominent privacy policy location increases individual's privacy considerations in their online purchasing decisions. Following an experimental method this research identifies when privacy policy information is clearly stated and accessible, consumers are willing to pay a premium to purchase from privacy protected websites.

In another study of electronic commerce Buckman et al (2019) investigated the changes in individual's value that play an important role in information disclosure decisions online. After running three randomized experiments the authors found that increased saliency and awareness lead to higher privacy valuation. Chui et al. (2014) examined privacy risk in the context of intention of repeat online purchases; they found that perceived privacy risk had a weak negative

impact on repeat purchase intentions. Post hoc analysis revealed that perceived privacy risk had a greater effect on customers who purchased fewer than six items (Chui et al., 2014).

In the context of social networking Choi et al (2015) identified that online social network has become a very common socializing platform. The advancement of technology increased bonding among the people. However, sometimes, individuals are being targeted as a part of humor, amusement, or playful teases that include exposing an individual's private embarrassing information of their past. As a result, individuals get offended by involuntary exposure of private information. The paper investigates the impact of information dissemination and the network commonality that shapes their behavior. An experimental method is used to find that information dissemination and network commonality jointly influence an individual's perceived privacy invasion and perceived relationship bonding.

Several papers also examine social networks in regard to privacy and information disclosure. Guo and Yu (2016) examined the interactions between anonymity in an online forum and found that three types of discursive disciplines appear in this context. Liu, Wang, Min, Li (2016) aimed to explore how role conflict impacts privacy risk, control, and disclosure; they found that role conflict positively impacts privacy risk and negatively impacts perceived control, which both in turn impacted information disclosure. Overall, both authors suggest that users of Social Networks should be conscious of the online context, individual attitude and emotion, and anonymity (Liu et al., 2016; Guo and Yo, 2016).

Moreover, in healthcare information disclosure is even more sensitive. Now-a-days there are popular online platforms for health-related information seeking and sharing. These platforms help individuals to receive health related advice from a community. The benefit is that individuals can get an idea of their health problem before visiting a doctor or health consultant. However, the concern here is the privacy of sensitive health information. Therefore, there is a tradeoff between information seeking and privacy information disclosure. Anderson

et al (2011) investigate this tradeoff using a survey research method and find that emotion plays a significant role towards information disclosure decisions.

In addition to individual privacy and information disclosure, Gerlach et al. (2019) examined how companies balance the customers' demands of their information and privacy; they found that there are four tensions that companies may undergo when trying to balance customer information and privacy: trading off data against customers, timing the problem, image-related costs of customer data, and losing customers due to data utilization. By understanding these tensions, the authors argue that companies will be able to reach ambidexterity when managing customers' information.

Posey et al. (2010) and Shih et al., (2017), have both looked at information disclosure but found contradictory results, Posey et al. (2010) found out, that social influence directly affects online self-disclosure; as a positive social influence on to use of an online community increases online community self-disclosure; reciprocity increases self-disclosure. In contrast to this, Shih et al., (2017) found that social identity indirectly affects online self-disclosure intention through constraint-based and dedication-based relationships. Posey et al. (2010) also found that reciprocity and online community trust increase self-disclosure while privacy risk beliefs decrease self-disclosure. Extending the elaboration likelihood theory, Bansal et al., (2015) studied privacy concerns as a moderator of trust and information disclosure. Their results indicated that there are distinct behavioral differences between individuals with high- vs low-privacy concerns when forming their trust to disclose private information.

**Privacy Protection Behavior**

According to Jiang et al. (2013), individual privacy behaviors can be inconsistent with their privacy concern based on their perceived anonymity on social media. Based on the hyper-personal framework and privacy calculus model the authors found that the behavioral strategies

of individuals are more prone to share privacy information in a synchronous online environment. The research also found that perceived anonymity increases social media engagement.

Privacy protection is a natural tendency of human behavior. Crossler et al (2019) investigates the privacy protection behavior of individuals in the context of location-based services. The authors identify the problem that smartphone users always struggle with the protection of information because of the app connection. Moreover, privacy settings are not always easy to manipulate for everyone. Therefore, privacy knowledge and self-efficacy can play a significant role in shaping the privacy protection behavior. Using an econometric model this research finds that personal motivation is one of the strongest determinants of utilizing privacy-protective mobile phone settings.

In other interesting research, Yazdanmehr, Wang, and Yang (2018) and Gwebu, Wang, and Hu (2016) both investigate how social influence impacts privacy protection behavior. Yazdanmehr, Wang, and Yang (2018) review how social influences affect Information Security Policy (ISP) compliance; the authors suggest that "ISP compliance could be a social phenomenon" because they found that social influence, at both the organizational and individual level, moderated employee ISP compliance. Similarly, Gwebu, Wang, and Hu (2016) found that the ethical climate of an organization has an effect on employee ISP noncompliance. So, considering both these studies, employee's protection privacy behavior, specifically relating to ISP compliance, is affected by social and individual factors (Gwebu, Wang, and Hu, 2016; Yazdanmehr, Wang, and Yang, 2018).

Miltgen and Peyrat-Guillard (2014) also had interesting findings with regards to generational difference in information disclosure. Younger people had lower privacy concerns but have very high protective behaviors, which seems to be a reverse of the privacy paradox. This can be associated with several reasons, including the level of exposure of younger people

to online interactions and knowledge on protective behaviors. Generational difference is a factor that needs to be explored further, as there hasn't been much research in that regard, and results of extant literature have been contradictory.

**Personalization and Privacy Calculus**

Privacy calculus is a well-researched topic in the privacy literature. It is not uncommon that in a privacy decision individual make choices where they sacrifice a certain degree of privacy in exchange of perceived benefit or outcome. In the context of e-commerce, Dinev et al (2006) investigate the privacy risk beliefs and confidence that impact the intention to provide personal information in an internet transaction. Using a survey-based SEM the authors find that internet privacy concern inhibits e-commerce transactions, personal interest can outweigh privacy risk perceptions of info sharing.

Greenaway, Chan, and Crossler (2015) developed a framework that aims to describe an organization's information privacy orientation through privacy calculus. Their conceptual framework, called Company Information Privacy Orientation (CIPO), was built using control and justice theory. In total, they found four different types of company profiles: Privacy ignorers, Privacy minimizers, Privacy balancers, and Privacy differentiators. While this framework has been recently developed, the authors urge researchers to view privacy from an organizational level.

The majority of papers about privacy calculus examine it in the mobile technology context (e.g. Kehr, Kowatsch, Wentzel, and Fleisch, 2015 and Keith, Babb, Lowry, Furner, and Abdsullat, 2015). Keith et al. (2015) found a significant impact of mobile-computing self-efficacy on both perceived risks and perceived benefits, which then have an effect on information disclosure; interestingly, this research suggests that those who are early adopters of technology, could underestimate the risks associated with the mobile-computing technology

and thus, could impact their security. Kehr et al. (2015) introduce situational privacy calculus and argue that privacy calculus can be situation specific.

Regardless of the benefits that can be derived by the consumer as a result of personalization, adoption is hindered due to privacy concerns. Li and Unger (2012) studied the effect of a high-quality recommendation service on customers' use of online personalization and found that perceived personalization quality can outweigh the impact of privacy concerns, albeit under certain circumstances. Hence, advocating for high-quality personalization. Researchers have also explored the effects of personal factors such as personality traits on privacy concern of individuals. A study by Junglas et al., (2008), found that agreeableness, conscientiousness, and openness to experience are contributing factors to the formation of privacy concern, while extraversion and emotional stability, in contrast, were found to show no impact.

The influence of culture has also been studied in the extant privacy research. Individualism and collectivism are also the most studied and common cultural dimensions in the IS literature (Shin et al., 2007). This is the same for privacy studies. Miltgen and Peyrat-Guillard (2014) and Posey et al., (2010), all confirm individuals associated with the collectivism culture have a higher tendency of self-disclosure. Dinev et al., (2006), argued that perceived risk and privacy concerns are affected by cultural differences. Based on Hofstede's cultural theory and Fukuyama's theory of trust they found out that culture has an influence on trust, institutional trust, privacy concerns, and higher perceived risk. They studied the case of the US and Italy and even though Italy scored higher on indices of collectivism, the Italian society exhibited lower propensity to trust, institutional trust, privacy concerns, and higher perceived risk.

## 2.5 Discussion

Given the aforementioned, information privacy can be defined as a process by which one can have freedom from unauthorized intrusion hence resulting in seclusion. A key aspect of privacy is the word "unauthorized." While individuals may not like their browsing and

purchasing history to be monitored and stored forever, at least individuals are aware that it's happening. When such tracking and storage take place through unauthorized intrusion, privacy infringement occurs. Various surveys have found that there are increased levels of concerns about privacy. For instance, 40% of people worldwide feel that they don't have control over their personal data[4]. With respect to children, The McAfee survey also found that nearly a third of the parents confessed that they do not monitor their children's connected devices. About the same percentage feel that they are not aware of the risks of the associated danger.

Interestingly the statistics have not changed much. In 1990 and 1992, Equifax had undertaken an opinion poll[5], and that survey found that nearly 79% of Americans were concerned about information privacy (as cited in Culnan, 1993). The study also found that almost 55% suggested that personal information breaches were bound to get worse in the next decade. While the concerns remain, and privacy breaches have been on an increase, awareness, management, and policy initiatives have not made much progress.

As a comparison, a March 1999 Federal Trade Commission (FTC) survey (as cited in Dhillon, 2002), which analyzed 361 websites, found that 92.8% of them were collecting some personally identifiable information. The study also found that 56.8% of them were collecting some demographic information. Over the last two decades, while academia and industry have recognized the issues, not much has been done. To the extent that in 2018 estimates suggest that nearly $19 billion has been spent on analyzing consumer data acquired through the very websites surveyed by the FTC in 1999.

Prior research, some of which have been reviewed above, has critiqued many of the opinion surveys suggesting that information privacy is not a unidimensional construct. The criticism

[4] https://www.mcafee.com/blogs/consumer/key-findings-from-our-survey-on-identity-theft-family-safety-and-home-network-security/ Accessed Feb 3, 2020

[5] https://www.ftc.gov/reports/fiscal-year-1999-second-half. Accessed July 20, 2022

has suggested that a focus on the level of concern is ill-founded, and that the nature of interest should be considered. Addressing the matter, Smith et al. (1996) identify four dimensions of information privacy: collection, unauthorized secondary use, improper access, and errors. Smith et al.'s (1996) research provide a useful instrument to measure individuals' concerns related to privacy. However, privacy concerns related to teenagers are not considered by Smith et al.

There are two reasons for the increased importance of teenage privacy concerns. First, the increasingly competitive business environment is forcing companies to collect a vast amount of personal information, particularly from the younger generations. Many times, there is good intent in doing so, since many businesses may seriously want to customize their products and services for the benefit of the consumer. Or even the intention might be to ensure that the personal details of young adults are not abused. However, the interconnectedness of technology and the resultant abuse, misuse or wrongful use of information raises privacy concerns. Such concerns often result in questioning the intent behind collecting private information. Second, the advances in information technology, social media and the range of available applications, particularly those that are targeted at children (e.g., Tik Tok, Instagram, Snapchat, among others) have not only made it possible to record personal information as the applications are used, but also record location information, patterns of use and their online behavior. In 2014, Snapchat came under fire when it failed to secure it's Find Friend feature, which resulted in a breach where attackers were able to compile a database of 4.6 million Snapchat usernames and phone numbers. The company ended up settling with the Federal Trade Commission after it was found that Snapchat had made multiple misrepresentations to consumers[6].

[6] https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were Accessed Feb 3, 2020.

Concerning the reasons identified above, the issue of fairness in collecting individual information need to be addressed. The extant literature focuses more on issues and concerns related to adults in the western world. In spite of a significant number of privacy breaches and their constant rise, the regulatory bodies in North America and Europe exist and do make a good effort to protect the interests of individuals, may these be children or adults. In other countries in Asia and Africa, however, progress in ensuring privacy and fairness of use of collected data is in its infancy. Not only is there a lack of policy initiatives at the state and at national level, but there have also been virtually no studies to understand the privacy concerns of the population, both young and old.

The concept of fairness is linked to the procedure that might be followed in a particular activity. When it comes to teenage privacy, it is even more important to understand the nature of the outcomes of such procedures. Such an understanding would be a key determinant of the level of privacy concern an individual might have. In Europe, the implementation of GDPR has forced businesses to pay close attention to privacy procedures. Procedural fairness is closely coupled with social contract and trust. When an individual feels the social contract regarding information exchange is not maintained, it results in loss of trust and integrity. In the case of teenage information privacy protection, what constitutes a "fair procedure?" How can "fair procedures" be designed? These are important questions that should inform future research.

**'Privacy' and Popper's Philosophy of Science**

In the early 20th century, scientific discovery was viewed as an extension of the reasoning process through which new insights were articulated to be further developed. Philosophers in those times argued that the logical process of scientific discovery was the 'process of testing'. Karl Popper (2005) challenged the traditional view that science can be distinguished from non-science based on its inductive methodology. He emphasized the importance of critical spirit

and posited that critical thinking was the essence of rationality and only through critical thought could we eliminate false theories. The core ideas of Popper's philosophy of science are the *rejection of induction* and *falsifiability*. According to Popper, scientific theories cannot be inductively inferred from experience and should be falsifiable, i.e., it must be forbidden under certain observations.

*"In so far as a scientific statement speaks about reality, it must be falsifiable; and in so far as it is not falsifiable, it does not speak about reality." --- Karl Popper*

Popper describes a theoretical system as a set of statements that prove or test relationships among different constructs in a defined context. Every theory is specific to its context which is a part of a Universality. The set of statements described in the theoretical system are the axioms of the theory and these axioms must follow four fundamental requirements: a) no contradiction, b) independence, c) sufficiency, and d) necessary.

From the articles analyzed on privacy, the main themes that emerged are:

a) Privacy Calculus, and

b) Privacy Concerns and Privacy Paradox

We also found articles that provided an elaborate literature review in the themes of information privacy research.

Research in privacy calculus focuses on the universality of utility maximization. The objective principle of privacy calculus is based on the expectation theory that an individual's rational behavior is based on maximizing the benefits and minimizing the potential loss from the behavior. Acquisti et al. (2018) use the theoretical axioms of the privacy calculus to view the privacy protection choices while disclosing personal information. The normative factors that dictate privacy behavior apply without any contradictions in the context of the objective and relative risk of disclosure. In the study, the researchers were able to find support for the

theoretical axioms and thus, axioms that held Popper's principle of testability. The theoretical axioms of privacy calculus also were tested in the *consumer willingness in online profiling* by Awad and Krishnan (2006). Their study focused on the axiom that there is a trade-off between the potential positive and potential negative consequences in disseminating personal information. Another interesting theoretical system that has been used in the privacy calculus theme is the Prospect Theory by Kahneman and Tversky (1979). This theory posits that individuals are more risk-seeking when they are faced with a potential loss situation. In both the theoretical systems used to empirically test the privacy calculus, all the four fundamental requirements of Popper's framework were followed.

The theme of privacy concerns and paradox used the Elaboration Likelihood Model theoretical axioms to study concerns of information privacy (Angst and Agarwal, 2009) and the Information boundary theory to explain the personalization-privacy paradox (Sutanto et al., 2013). The Elaboration Likelihood Model explains observed differences in the amount of influence on cognitive energy invested by recipients when exposed to new information. Whereas Information boundary theory explains the psychological processes involved in the sharing of private and valued information by individuals. These two theoretical systems were applied in different problem domains and the axioms of the theories were independent and non-contradictory as required by Popper for scientific discovery.

**Privacy and the Principle of Demarcation**

According to Popper's (2005) philosophy of science, the principle of demarcation helps distinguish between the scientific theories and the theories of pseudo-science. Popper emphasized that only by disapproving a theory or by disconfirmation, can we demonstrate and get closer to scientific truth. In the discipline of IS, with a focus on 'privacy' thematic, this implies that the theoretical systems and theoretical axioms aim to be disapproved. When a

theoretical system is used in a specific context, the theory is demarcated from the universality and thus conforms to Popper's philosophy.

Studies by Awad and Krishnan (2006) and Sutanto et al., (2013) demarcated their research by focusing on personalization. Personalized information was explored using the theoretical lenses of Information boundary theory and privacy calculus.

**Privacy and the Principle of Deduction**

Karl Popper (2005) rejected the concept of induction and emphasized that the deductive method of testing should be preferred for scientific discovery. According to Popper's framework, statements or hypotheses should be put together and conclusions must be drawn by means of logical deductions. The principle of deduction is the way to verify the theory.

All the articles analyzed, used the principle of deduction as posited by Popper (2005). The statements and hypotheses in the studies were drawn from the theoretical axioms that were chosen based on the problem context. The conclusions in the studies were based on logical deduction.

## 2.6 Conclusion

Based on our analysis of the broad 'privacy' thematic in the literature, we studied the sub-themes of privacy calculus and privacy concerns and paradox on the lines of Popper's framework for scientific discovery. The research in IS has focused on the principle of deduction and demarcation as emphasized by Popper (2005). This analysis also gave us insights into the emergent themes in 'privacy' that could be developed in future research.

From the thematic analysis, it was identified that privacy calculus and privacy concerns have been studied in great detail at the individual levels. However, information privacy concerns and privacy calculus trade-off have not been studied at the organizational level, with the exception of Culnan and Williams (2009) who examined organizational privacy and

provided recommendations for organizations to improve their privacy programs. Organizational privacy concerns become important as it included not just the privacy of the organization's information but also the privacy of the customer's information.

The studies primarily focused on the utility maximization concept to study the privacy calculus. However, the field of information privacy has not explored deeply the behavioral and psychological theories to explain the privacy calculus trade-off and privacy concerns. Integrating the cognitive factor as the antecedents for information privacy research would help better understand the 'privacy' thematic.

There is a lack of clarity in organizations as to what individuals consider privacy to be. It is important to understand individual's privacy values, an area that has not been well researched. Individuals seem to have divergent perspectives on the nature and scope of how their personal information is to be kept private in different modes of technologies. Any future work should be concerned with identifying objectives for protecting privacy. We argue that in order to ensure privacy we first have to identify individuals' privacy objectives, which are imbedded in their values towards privacy. Therefore, understanding and identifying individuals' values with respect to privacy is important for the development of privacy objectives and thus protecting privacy.

# 3

# Theoretical Foundation and Methodology

## 3.1 Introduction

In this chapter theoretical and methodological basis of the research on information privacy values for GenZ is presented. Any theoretical foundation and methodological approach must be consistent with the philosophical perspective. Essentially the ontology, epistemology, and methodology should be consistent to qualify as a valid research design. In this chapter we first present a synopsis of research in individual values, particularly as these relate to GenZ. This is followed by a presentation of the extant research on individual values. In the process of doing this, we are cognizant of the research in information systems and the relevant lessons learnt from a technology perspective.

The concept of values is defined as the "wants, preferences, desires; likes and dislikes for particular things, conditions, and situations" (Posner & Munson, 1979). Since the wants and desires change, the values also change with time, particularly as the context changes.

Therefore, defining the concept of values is a kind of a moving target. It can change based on experience, and social expectations (e.g. see Syed, Dhillon, & Merrick, 2018), time, situation, and environmental concerns (e.g. see Keeney, 1993; Merrick, Parnell, Barnett, & Garcia, 2005). Hence studying and defining the concept of values is challenging and an ongoing process.

There is a significant amount of information systems literature addressing the concept of values. Studies have focused on an organizational stakeholders' perspectives (e.g. Posner & Munson, 1979; Slater, 1997). Other studies have explored them from a project implementation perspective (e.g. May, Dhillon, & Caldeira, 2013). Besides, the role of a system, the manager, the rewards program, the platform used, has been explored and evaluated.

Values are grounded in two inter-related concepts, which in a 2003 paper, Daniel Kahneman (2003) enumerates as – thoughts and as they differ in accessibility and intuitive and deliberate thought processes. Kahneman goes on to suggest that decision making has three distinct processes. These cognitive processes are perception, intuition, and reasoning. Several social psychology scholars have recognized this distinction (see Stanovich, 1999; Kahneman and Frederick, 2002; Stanovich and West, 2013). Kahneman (2003) also recognizes that intuitive and perception-based processing is quicker, effortless, implicit, and is often emotionally charged and hence grounded in individual values. Since intuitive reasoning is usually governed by habit, making it difficult to modify. On the opposite scale of intuitive reasoning is perception-based processing. Perception-based processing is slower and requires more mental effort. Hence, it is likely to be consciously monitored. This results in deliberately controlling the perceptions through rules. Furthermore, perception-based processing forms the basis for monitoring and rationalizing decisions, often times originating from intuitive reasoning.

While Kahneman's 2003 works and his other research points towards a cognitive perspective on risk taking and the psychology of preferences (e.g. Kahneman and Lovallo, 1993; Kahneman and Tversky 1982), it does inform the relevance and importance of individual values. Agreeing with Kahneman's line of argumentation, many scholars have argued that deliberative, calculated decision making is an exception. Most decisions are automatic (Bargh and Chartrand, 1999) and are generally experience based or results because of past habits (see instance Louis and Sutton, 1991). Irrespective of the fact that decisions are made based on reasoning or intuition, both are grounded in the values of individuals.

## 3.2 The Concept of Values

Catton (1959) proposes "value theory" as a theory of valuing behaviors. According to this theory, an individual's preferential behavior shows certain regularities, and this pattern can be attributed to some standard or code, which persists through time providing a basis by which people can order their intensities of desiring various desiderata (something desirable. It can be material, object, social relationship or an item of information.). According to Catton, valuing is defined as actions which show a person's intensity of desire for various desiderata or the amount of motivation to pursue them. In context of decision making, preferences must be amongst diverse objects. Observed over a period of time, preferences are not random in nature but show a stable pattern. Hence, according to value theory, it can be assumed that personal preferences of an individual get reflected in the choices made by the person. Such choices are consistent with internal "values" of that person. Values provide a basis by which people can control their intensities of desiring various desiderata (something desirable). Based on available choices, people make preferences or choices which are grounded in their values. In the organizational context, knowledge of such preferences of individuals, provides a context for managerial decision-making.

Catton (1959) argues that "value" is not a property of an object but is a quality of relationship. A person's desire for something under a given situation depends upon the - selective perception of that person. Selective perception directs valuation by interspersing final goals with other intermediary goals i.e. a goal may be pursued in order to attain some higher ultimate goal. Thus, the nature of the major goals accepted by individuals is complimented by their notions of ways in which these goals might be affected by future events. These in turn are the determinants of values of people. Value Theory provides a theoretical platform to affirm that values are important for decision making and incorporating values in developing decision objectives significantly helps individuals accept the results of such decisions. Catton adopts a field concept of values for understanding and predicting human behavior from studying of values. In this approach, the concept of value is perceived as somatic (in brain) which surround the value object. It is assumed to have a correspondence to some postulated external field. The nature of this value field is multi- dimensional. Psychologists have studied values extensively but the popular terminology in this discipline has been motivational (Catton, 1954). The idea behind studying motivations in management, both internal as well as external, has been the same as in the field of sociology i.e. predicting the human behavior from the study of these concepts. Psychologists argue that human nature does not allow the valuation of anything that is readily available and indispensable to their survival. Maslow (1943) shares similar views and argues that when a need is easily fulfilled (or satisfied) there is very little or no motivation. When discussing *A Theory of Human Motivation*, Maslow (1943: p. 374) notes:

> "For the man who is extremely and dangerously hungry, no other interests exist but food. He dreams food, he remembers food, he thinks about food, he emotes only about food, he perceives only food, and he wants only food. The more subtle determinants that ordinarily fuse with the physiological drives in organizing even feeding, drinking or sexual behavior, may now be so completely over- whelmed as to allow us to speak at this time (but *only* at this time) of pure hunger drive and behavior, with the one unqualified aim of relief."

Catton considers the process of valuing as a field of forces since when we observe a person who is valuing something, certain things are apparent from the behavior while others are not. This may generally be true as well, particularly if one witnesses the varying degree of relationships between objects and things (or what Catton refers to as "desideratum.") In his 1954 work, Catton created a comprehensive taxonomy of values and noted that a multiplicative combination of the value measures would help in specifying the worth of its desideratum. According to Catton's Value Theory, the value of a particular object to an individual is specified by the product of the various value dimensions. In a final synthesis Catton (1954: p. 55) notes:

> "On the basis of the three empirical tests of the hypothesis of incommensurability here reported, it can be concluded that human values, including those which are regarded by certain authorities as being of in- finite worth, become measurable relative to each other in exactly the same manner as other verbal stimuli-by application of Thurstone's law of comparative judgment."

Sociologists have studied the social shaping of values for a very long time (Bachika and Schulz, 2011). The formation and operation of values occurs at three levels – micro-, meso- and macro sociological levels. The words formation and operation suggest the manner in which values come into being and get sustained over a period of time. Formation refers to the role played by the human agency. And operation refers the social process by which values get incorporated into a society without necessarily the intentional intervention of the human agency. While quoting Durkheim, Bachika and Schulz, 2011: p. 110) note:

> "As Durkheim suggested, modern society has lost the integrating grip of past hierarchies and uniting world-views and thus depends more on cohesions derived from functional differentiation. Therefore, it should not come as a surprise that the contested nature of values or their interpretations motivate and even urge the scholarly study of values."

Catton's (1959) conceptualization of values took a slightly unconventional route, particularly since it did not conform to Parson's views (for example see Parson, 1951). As

Spates (1983) notes. Catton's construction of "a series of hypotheses for empirical test that still rank among the most interesting in the literature."

Value Focused Thinking, as we know it today, can be traced to the Value Theory of Catton (1959) although Keeney (1992) does not provide an explicit connection. As noted above, in his 1959 paper, William Catton introduces the word "desideratum." The Merriam-Webster dictionary defines *desideratum* as "something that is needed or wanted." Catton uses the term to mean "anything some person desires at some time. It may be a material object, social relationship, an item of information – in general, anything tangible or intangible." In many ways, desideratum is the object of desire. Catton goes on to describe "valuing" as actions or steps to acquire desiderata. The intensity of the desire will, however, vary in proportion to the motivation a person will have to seek desiderata.

Embedded in Catton's conceptualization is the notion of preferences. Given the varying degrees of motivation to seek desiderata, preferences are expressed. These preferences are not random. Preferences have a pattern that are relatively stable, albeit in a given context, society or an environment. Given that preferences have a certain pattern, what individual "value" must be governed by some code of conduct, norms or standards. Catton also notes that values are inferred and are not explicitly linked with the verbal statements. Philosopher Charles Morris, for instance, uses a *semiotic* perspective to attribute meaning to objects and signs (Morris, 1956). In information systems, similar conceptualizations have been presented by Stamper (1973), Liebenau and Backhouse (1990), and Dhillon and May (2006).

In defining Value Theory, Catton (1959) proposes six hypotheses, which are "all related by the value-space concept and a magnetic model to a general theory of valuing" (p. 317). The hypotheses are:

H1: Socially acquired conceptions of the desirable (values), influence human choices among non-symbolic desiderata.

H1a: Significant correlations may be found, at any given time, between values and personal desires.

H1b: Within an isolated social system, such correlations tend to increase through time. That is, there is a strain toward alignment of desiring with socially acquired values.

H1c: The influence of values upon human choices among non-symbolic desiderata is conditioned by socially acquired knowledge of the characteristics of the desiderata.

H2: When values are held constant, desiring varies inversely with the "distance" between the valuer and the desideratum.

H3: When values and desideratum-to valuer distances are held constant, desiring varies with the activation of levels in some prepotency hierarchy.

H4: A valuer's responses to sets of substituted desiderata are more predictable than his response to sets of independent desiderata.

H5: A valuer's responses to sets of congruent desiderata are more predictable than his responses to sets of independent desiderata.

H6: When values are held constant, the order of preferences among a set of desiderata may nevertheless vary from person to person or from group to group as a result of the failure of each person or group to be fully cognizant at all times of all the dimensions of value-space.

## 3.3 Value conflicts

There is a long history of discussions around value conflicts. Karl Marx (1973) in his conflict theory notes that conflicts are a result of mismatched values which don't get resolved. A documented history of the world, which has contained wars, gives credence to the conflict theory. Organizational conflict is well-documented as well. In particular, the information

systems literature has noted research in conflicts arising because of discordance in individual values. For example, Posner and Munson (1979) studied the relationship between organizational behavior and individual values. The Posner and Munson study found a difference in values between managers and students. They also reported differences amongst occupational subgroups. Posner and Munson concluded that understanding individual values is necessary if organizational behavior is to be managed effectively. The study introduces the concept of value conflicts and the necessity of managing values to ensure that an organization's potential is reached.

In a classic case study, Allen (2005) discusses conflicts in the implementation of systems. The case illustrates how conflicting values can have a negative impact on the success of systems. The case titled Value Conflicts in Enterprise Systems explores how an enterprise resource planning (ERP) system was not fully utilized. It happened largely because of lack of cross-functional interaction, which limited the effectiveness of the system. Based on prior work, Allen (2005) makes a case for consideration of social factors, which typically interfere with implementation and subsequently their use. Based on the case, Allen concluded that there are three sources of conflicts:

- Conflict over work priorities
- Conflict over dependency on others
- Conflicts over evaluation fairness

The case is an excellent source of motivation to study values, their conflicts and assess their impact on system implementation and use. Conflicts in values is indeed an enduring theme in organization studies. Conflict impacts firms, their systems, people, processes and structure (Kling, 1996; Allen, 2005). Society and enterprises must evolve. Values must shift. Hence,

new value conflicts will emerge. As researchers, we continue to examine the interplay between technology and the values.

Various researchers have argued that values evolve over time (e.g. see Yankelovich, 1978; Cooper, et al., 1979). In information systems research, values are typically considered in terms of beliefs and preferences that the individuals possess. Additionally, the perceived value derived, particularly when dealing with technology and information systems is considered. Since the information systems that we know of today are not the same as what they were 20 or 30 years ago, the nature and scope of values have significantly evolved – from being rather static to dynamic. For instance, the values purported in the 1980s related more to issues around alignment of business with IT (e.g. see Henderson and Venkatraman, 1999). Today, those values, for instance, have evolved into protecting individual identity (e.g. see Syed et al., 2018). This shifting in focus reflects the evolution of values and how they reshape and influence the design and implementation of IT use.

In order to illustrate this point, an examination of two ERP studies is telling – Allen (2005) and May et al. (2013). Both the studies focus on an examination of ERP implementation and the inherent values of individuals. The May et al study focuses on the strategic aspects while the Allen study is more operations oriented. The two studies show how values evolved from focusing on the system development issues to conflicts amongst stakeholders. The evolution in values suggests the dynamic nature of the values and how values come into play at different levels within an organization.

## 3.4 Value Focused Thinking

As noted earlier, in this study we use the Value-Focused Thinking concepts, as proposed by Keeney (1992). The concepts are used to develop a fresh understanding of Internet Privacy amongst GenZ. Keeney has argued that by identifying values for a particular decision context helps in incorporating concerns of a disparate number of stakeholders. One is able to capture,

very succinctly, what individuals care about. As Keeney (1996) notes, “values are fundamental to all that we do; and thus, values should be the driving force for our decision making (p. 537).” While Keeney does not prescribe an exact number of interviews that should be conducted, it is a function of reaching the saturation point after all. Therefore, the exact number of interviews has significantly varied.

The process used for identifying and organizing values is organized into three steps (see figure 3.1). It helps in identifying key individual stakeholders and their perspectives regarding Internet Privacy. As indicated in figure 3.1, the process is enumerated below:

1. In depth interviews are conducted where individuals are asked to think freely and explicate their values. The interviewer typically asks probing questions so as to bring out the latent values. Probes are used, which could include things like – Why do you think it is important? What makes you think like that?

2. Pertaining to the decision context, the values are converted into a common value format, duplicates are removed, and then the similar sounding values are clustered together. Objectives take the form of a verb and a directional preference.

3. The final set of clustered objectives are then subjected to a WITI test – essentially asking the question, “why is this important?” Systematically responding to the question results in two sets of objectives – fundamental and means. If the objective is important because it leads to another objective, then it is a candidate for a "means" objective. If the objective is important because it simply is important, then it is a candidate for a "fundamental" objective.

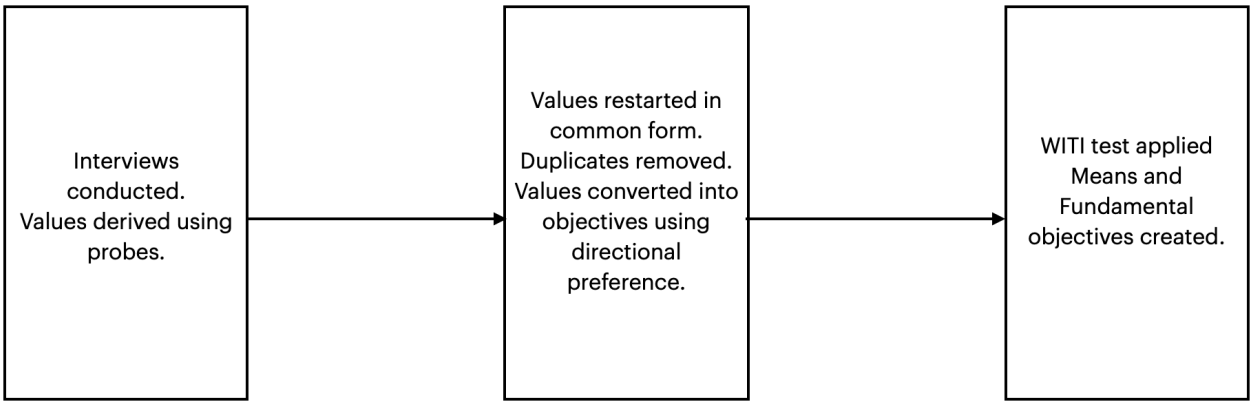


*Figure 3.1, The Research Process*

The Value Focused Thinking approach uses individual perspectives to develop an overall understanding. What individual values, guide how decisions are taken? Consider a situation where a decision has to be taken to buy a new car. Also, assume that the car will be a used vehicle. In the United States, one would probably go to CarMax or Carvana to purchase the vehicle. One will encounter 100s of alternatives. Keeney (1992) argues that the choice or the decision to buy a particular car is a function of your value set. If an individual values the environment, then the choice is perhaps limited to electric vehicles. Alternatively, a different set of values would result in a different set of alternatives. Hence, focusing early on the values will result in more desirable consequences. Therefore, as Keeney suggests, focusing on values allows individuals to focus on issues that really matter. Keeney (1992) highlights the importance of Value Focused Thinking when he notes:

> "In addition, most decision methodologies try to find the best alternatives from a prespecified list. But where does this list come from? In contrast, value-focused thinking does not simply accept prespecified problems or prespecified lists of alternatives. It either creates them or changes them. Value-focused thinking should lead both to more appealing decision problems and to choices among better alternatives than those generated by happenstance or conventional approaches." (p. 8)

Values, therefore, are principles that individuals use for evaluation. People use values to assess actual or potential consequences of their actions or inaction. Following on from our car-

buying example, if an individual really values the environment, then buying a V8 engine gas guzzler SUV should not be one of the alternatives. This suggests, and as Keeney (1992) notes, that the choice of a proposed alternative or a decision can range from an ethical choice to upholding guidelines for preferences among choices. Since Value Focused Thinking is based on the ideal preferred option, it is often labeled as constraint-free thinking. Constraint-free thinking is an essential part of developing strategic objectives – may these be for individual goals or organizations. As Keeney notes:

> "Every individual and every organization has strategic objectives. Although they are often not explicitly written down, these objectives are intended to guide all decision-making. The separate decisions made over time are the means by which strategic objectives are pursued. These same decisions collectively determine how well the individual or organization performs. The strategic objectives should provide common guidance to all decisions and to all decision opportunities. In an organization, they also serve as the mechanism by which management can guide decisions made by different individuals and groups within the organization. If these strategic objectives are not carefully defined and communicated, the guidance is minimal and some separate decisions simply won't make sense in the larger context of the organization's affairs." (p. 41)

An important aspect of Value Focused Thinking is that of a *decision context*. Recall our example of buying a car. In that example, buying a car is our decision context. Going to CarMax and encountering all possible choices is what Keeney (1992) refers to as *alternatives*. Our *value* of being environmentally friendly limits our choice of *what we care about*. The limited set of choices based on our values will allow an individual to formulate very specific value-based objectives, *viz*. "maximize fuel saving;" "minimize exhaust;" "maximize range." These objectives will then allow an individual to limit the alternatives to vehicles such as hybrid and electric cars. The Value Focused Thinking process can be illustrated as in figure 3.2.

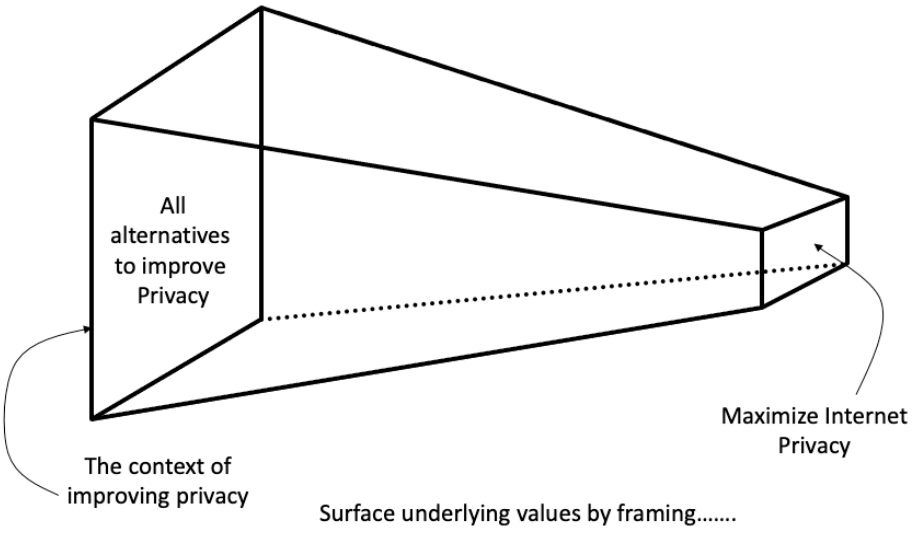


*Figure 3.2, Decision frame and alternatives*

In Value Focused Thinking another aspect that is important to understand is that of *objectives.* Keeney (1992) defines an objective as a statement of what is desired to achieve. It has three constituent elements - a decision context, an object, and a direction of preference. Values for a given decision context and a directional preference results in an objective. Keeney characterizes objectives as *means* or *fundamental*. Fundamental objectives are the ultimate decisions that one might desire. And means objectives help in achieving the fundamental objectives.

## 3.5 Operationalizing Values

Irrespective of the debates and discussions around the concept of values, their operationalization to understand real issues is important. According to Keeney (1999), in order to identify values relevant to solving a particular decision context, one must ask the concerned people, also known as key stakeholders. Keeney (1996) argued that "values are fundamental to all that we do; and thus, values should be the driving force for our decision making (p. 537)."

Keeney (2004) defines decisions "as situations where the decision maker recognizes that a conscious choice can be made". The ultimate goal by following value focused thinking in decision analysis should be to select the best alternative, but that is not always possible due to

the existence of hidden alternatives. The enumeration of values and the creation of objectives serve the principle of eliminating the bad decisions that looked good before, but do not compromise any of the proposed objectives. The unframing of the decision process should be performed as soon as possible by defining the problem at hand and removing the psychological traps that influence our clear judgement in creating new alternatives without the anchoring in the previous alternatives.

Keeney (1994) says that this value focused approach is proactive instead of the reactive basis of alternative focused thinking. He describes values as being "principles for evaluating the desirability of any possible alternatives or consequences." Alternatives are not fundamental; they should be viewed as means to accomplish defined values. Decision makers will align their decision structure by explicating values, thus, discovering hidden objectives which lead to adequate information gathering to support the decision process.

Gregory and Keeney (1994) argue that value focused thinking is a facilitator in a negotiation situation to reach consensus among stakeholders, as the unique list of objectives is part of the values and contributions from all the people involved in the decision process. This list of objectives forms the context to evaluate alternatives that assure the commitment from stakeholders, even if each stakeholder wants to push an alternative, he will have to justify the inclusion of the alternative as a consequence of multiple previously agreed objectives.

There is a significant amount of variance in the number of individuals that should be interviewed within the literature, yet as an example, Hunter (1997) used the interviews of 53 people from two different organizations to do a content analysis to elicit individual conceptions. Phythian and King (1992) used two managers who were experts in assessing tender enquiries to identify key factors and rules that influence tender decisions. Additionally, Keeney (1999) obtained interviews from over 100 individuals to obtain their values to develop

objectives that influenced Internet purchases. More recent work, Dhillon & Smith (2019) have also used the approach to a similar end.

Mishra and Dhillon (2008) develop control objectives based on the values of 54 IT managers using a value focused approach. Sheng et al. (2010) interviewed 33 individuals to study the values of mobile technology and examine how those values adapt to education delivery via a mobile network anytime and anywhere. Dhillon and Chowdhuri (2013) collect individual values for protecting identity in social networks using a value focuses thinking mindset. They interviewed 147 individuals and classified social media objectives. Nunes et al. (2015) interviewed 71 individuals using a value-focused approach to gather and structure information systems risk objectives.

More recent work, such as the work done by Dhillon and Smith (2019) explored the context of cyberstalking from and privacy and security perspective and, similar to Keeney (1999), interviewed over 100 individuals to elicit latent values to develop policy around prevention and protection methods.

The following three-step process is used to identify and organize the values that key individual stakeholders might have (Keeney 1992): First, interviews are conducted which elicit the values that an individual might have within a decision context. Second, individual values and statements are converted into a common value format, such as an objective oriented statement. Then, similar objectives are grouped together in order to form clusters of objectives. Finally, the objectives are then classified as either fundamental to the decision context, resulting in a fundamental objective, or simply a means to achieve the fundamental objectives, which is known as a means objective. Keeney (1988) describes that the structuring of objectives into a hierarchy, with fundamental and means objectives, improves communication among stakeholders thus creating a basis for a common understanding of values leading to a compromise to achieve a consensus. The communication barrier with a specific language that

separates multiple specialties, such as IT as an example, and the business is minimized by the common understanding of values. The involvement of stakeholders, as soon as possible, in the decision process increases their willingness to cooperate to reach a common goal. Thinking of values before looking at alternatives will allow an out of the box design of alternatives, which were not discovered beforehand. The creation of scenarios used to detail objectives will also help as a guide to evaluate the effectiveness of existing alternatives.

One example of this three-step process is the work of Dhillon and Torkzadeh (2006) where they performed an assessment of information systems security in organizations, in which they use a value focused approach with the major objective of maximizing information systems security in organizations. They interviewed 103 managers from multiple organizations and initially identified general values for managing information systems security and recorded them in a wish list. In a second step, values are clustered, labelled and converted into security objectives. The third step consists of the classification of the objectives in the fundamental and means objective group by elaborating the "why is it important?" (WITI) test. The research resulted in 86 objectives that were organized into 25 clusters with 9 fundamental and 16 means objectives.

Another example of this three-step process is the work from Dhillon et al. (2019) where they collected values about Internet Commerce Privacy by conducting 52 interviews. The first step involved gathering values in the form of a wishlist and they gathered 337 values. The second step deals with the conversion from values to a common form and then into objectives with the use of clustering. In this study they were reduced to 225 values in common form and these transformed into 194 objectives.

Studying individual values in an organization in the context of information privacy and security helps in creating a better program. Incorporating values of employees in governance activities helps in reducing the gap between management's expectations from such programs

and employees' interpretations of the requirements. Currently, information privacy and security research does not emphasize the use of individual values in this context. The personal values of employees in an organization play an important role in creating, implementing and monitoring information security and privacy-related policies, practices, and procedures.

## 3.6 Methodological considerations and theory advancement

A theory is the currency of our scholarly realm (Hambrick 2007). Natural scientists see theory as providing explanations and predictions and as being testable. In social sciences, theories are formulated to explain, predict, and understand phenomena and, in many cases, to challenge and extend existing knowledge within the limits of critical bounding assumptions. Some scholars define theory from a positivist approach. For example, Popper (2005) described theory as a scientific universal statement that is testable. He emphasized on falsification. On the other hand, the interpretivist theorists have different views toward theory-building, that is, the primary goal of theory building is not to make it testable. Locke (2007) mentioned that "in reality science has not and could not have progressed by the process of falsification; it progressed only by the process of making positive discoveries" (p. 869). From these definitions we can say that there is very little consensus on what a theory is. From the principles provided by Popper (2005), we develop a preliminary framework for theory advancement as presented in figure 3.3.

A theorical system should have consistency regarding the ontology and epistemology. Moreover, the theoretical advancement is closely tied to the concept of methodology. Ontology defines the theoretical assumptions, epistemology provides guidance regarding how theoretical knowledge can be advanced, and methodology helps the advancement of knowledge by applying different tools such as causal explanation.

Ontology is the philosophical study of existence, dealing with the question of how entities exist. As it relates to philosophy, ontological view can vary from researcher to researcher.

Social scientists examine their area of interest through implicit or explicit assumptions regarding the nature of reality. Two fundamental questions are associated with the ontological position about reality (Ritchie et al. 2013). The questions are– what are the core elements of the world, and how these elements are related to each other? Popper's ontology is based on three perspectives about the world. First, the world is composed of physical objects and events. In this view, objectivity plays a significant role. This view implies very little scope of knowledge discovery for the researcher. Second, the world is composed of mental objects and events. In this view, the researcher has a subjective lens. The reality is framed based on the researcher's interpretation of the phenomena and the world. This view makes knowledge discovery comparatively complex than the objective view. Third, the reality is composed of abstract objects such as theories, social institutions, ethics, math, language, literature, and so on. The reality, in this view, is a result of knowledge discovery processes and continuous research.

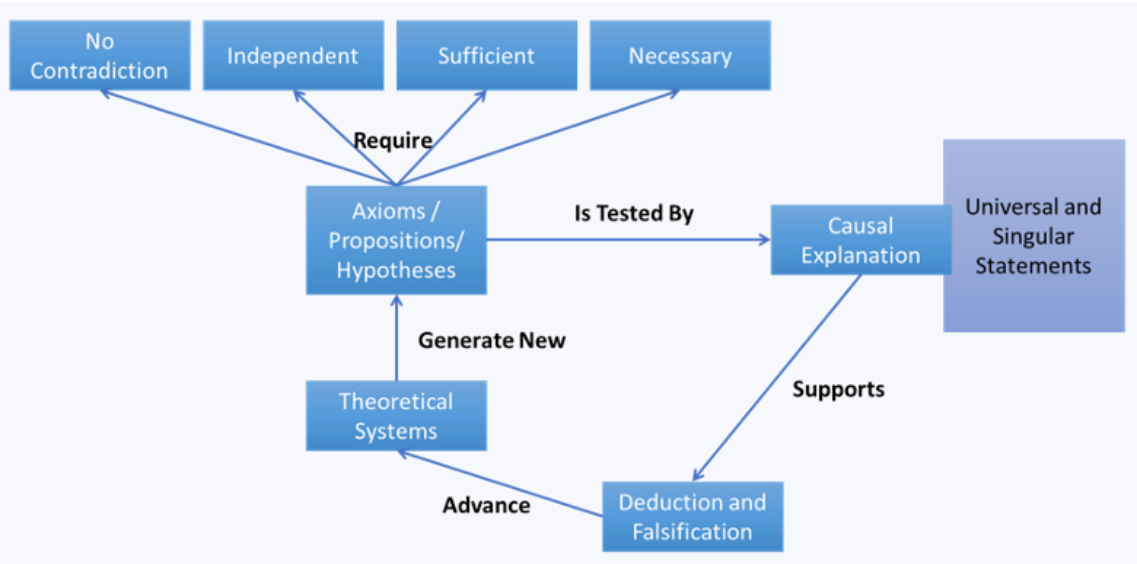


*Figure 3.3, Argument flow*

Morgan and Smircich (1980) provide ontological assumptions debate between the subjective and objective view. Here they provide six ontological assumptions.

- First, reality as a projection of human imagination refers that there is nothing outside oneself: one's mind is one's world. Thus, the knowledge of the social world may be accessible to the human being through phenomenological modes of insight.
- Second, reality as a social construction suggests that the social world is created by individual's impose of meaningful definition about everyday life. Social reality is embedded in the nature and use of symbols created by individuals.
- Third, reality as a symbolic discourse refers that reality exists in the system of meaningful action that renders itself as rule like but not in the rule or in rule following.
- Fourth, reality as contextual field tells that the social world forms based on the transmission of information. In this assumption relationships among the social constructs are relative rather than fixed and real.
- Fifth, reality as a concrete process suggests the social world is concrete in nature but always evolving in detailed form. The world is in part what the individual makes of it.
- Finally, reality as a concrete structure refers that the social world is a hard-real concrete thing that has existence without any influence. The ontological position in a research needs to be explicit for better understanding of the readers.

Epistemology is the study of knowledge about how knowledge is created and how can knowledge be acquired. Answering three questions can justify the epistemological stance of a researcher (Bohman 1991). These questions are— what does knowledge mean, how to get knowledge, and what is the basis for knowledge? Like the ontology, epistemological stance is also based on some assumptions. Morgan and Smircich (1980) provide epistemological assumptions debate between the subjective and objective view. As we pass from subjective

assumption to objective assumptions, the nature of knowledge construction changes. The six assumptions they provide regarding the ontological stance are:

- First, reality as a projection of human imagination is the most subjectivist position among the six assumptions. In this assumption, knowledge is obtained in terms of transcendental form of consciousness. Here phenomenological insight is the key to get knowledge regarding a phenomenon.
- Second, reality as a social construction focuses on analyzing social processes by which the reality is constructed. Knowledge is embedded in an understanding of those processes.
- Third, reality as a realm of symbolic discourse emphasizes on understanding patterns and symbols of social reality. This epistemological position signifies how social situations can be researched to reveal their inner nature.
- Fourth, reality as a contextual field of information emphasizes the importance of understanding contexts in a holistic manner. Knowledge is obtained through the understanding of social contexts.
- Fifth, reality as a concrete process entails the need to understand process. This epistemological position signifies the importance of monitoring process, the way a phenomenon changes over time according to its context.
- Finally, reality as a concrete structure emphasizes particular kinds and forms of knowledge. Using metaphors researchers seek to create knowledge about the world. We can say that; different world views imply different ground for knowledge about the social world. In a research the epistemological position should be aligned with the ontological position.

The methodology is the set of procedures or techniques to identify, collect and analyze data about a phenomenon. Different ontologies, epistemologies, and human nature drive researchers towards different methodologies. There are methodologies for those who view the social world as hard, concrete and real, external to the individual and on the other hand who view the world as dependent and subjective to the individual. Therefore, the methodology depends on the ontology and epistemological position of the researchers. There are two approaches of social science, the subjectivist and the objectivist approach. In the ontology and epistemology portion described above mentioned six assumptions and the first three assumptions are subjectivist and the latter three are objectivist assumptions. The methodology can also vary according to the assumptions of these two broad categories. When the researcher has an extreme subjectivist stance and believes that reality is a projection of human imagination, the exploration of pure subjectivity is the appropriate research method for the subject. With a moderate approach where a researcher assumes reality as a social construction language and text analysis is an appropriate methodology. From the assumption of reality as a realm of symbolic discourse the analysis of symbols associated with that particular social world is the appropriate research method to understand the subject. In the objectivist category the one assumption is reality as a contextual field of information that entails man as an information processor the contextual analysis of Gestalten is the methodology to collect and analyze data. In a more objectivist assumption that entails reality as a concrete process that emphasizes studying systems and processes, the historical analysis of the phenomena fits better in understanding the research area. In the most objectivist assumption where reality is considered as a concrete structure, the research method of lab experiments and surveys are more suitable as the knowledge is assumed hard and real without individual influence.

## 3.7 Theories, Demarcations, and Assumptions

It is evident that in the studies of technology in organizations that researchers have adopted and implemented a number of different approaches reflecting different assumptions about the nature of technology, its role in organizations, and how technology and human can create imbrication. To understand this diverse literature, it is helpful to have a sense of various approaches and the implication of their choices.

Determinism and voluntarism represent the human assumptions of the nature of social science (Burell and Morgan 1979). Determinism holds the objective view of human nature. That means an object can shape human behavior. In our case, we are discussing technology as an object which can shape human behavior to achieve organizations' goals. Hence, we can say, in this case technology has agency. For example, if an organization implements an ERP, the previous manual work procedure changes, which makes the employees change their way of work. Managers who previously signed on the purchase order sheets manually, now must approve online. Thus, ERP implementation changed the work procedure of the organization. On the other hand, Voluntarism holds the subjective view of human nature that shows a person is completely autonomous and free-willed. In short, human has agency. Humans choose their actions depending upon their beliefs, culture, and goals. For example, if the newly implemented ERP system does not comply with the employees' beliefs and goals, they will not accept the technology and will keep avoiding the system.

Materialism holds that matter is the fundamental substance in nature, and that all things, including mental states and consciousness, are results of material interactions. This concept entails, human actions are caused by the physical causes and contexts of a subject matter, and in this case, it is technology. In other words, the feature of technology makes human act in a certain manner. Humans cannot change the materiality of technology or object, they can only

select the material according to their affordance. Different researchers argued imbrication from different angles.

Sassen (2006) suggests that the term imbrication is used to capture the simultaneous interdependence and specificity of each, digital and nondigital. The human and material agencies work on each other to produce imbrication. Technology is deterministic when there is strong material agency, and humans are voluntarists when there is an active human agency.

Giddens (1984), in his structuration theory, suggests that people have goals that motivate them. They can rationalize their goals as acceptable given a set of circumstances, and they can continuously monitor their environment to determine whether or not the goal is being achieved. From these definitions and examples, we can say there should be a balance between human agency and material agency to achieve organizational goals. Otherwise, the organization will not be able to get the optimal value from the investment. In other words, imbrication of human and material agency will result in better optimization of resources.

Affordance theory of Gibson suggests that, technologies have materiality, and those material properties afford different possibilities for action, based on the contexts they are used. On the contrary, idealism holds that norms, values, and spirits constitute human action. Human acts in a particular manner based on their culture, belief, and context. Suchman (2007) states that technology acquires its meaning when embedded in social practice. On the other hand, Orlikowski (2007) argues that "materiality is integral to organizing, positing that the social and material are constitutively entangled in everyday life…. there is no social that is not also material, and no material that is not also social". This entanglement can be an alternative metaphor of imbrication (Leonardi and Rodriguez-Lluesma 2012).

Problematization, a key starting point of theory development, can be defined as "make into or regard as a problem requiring a solution" in general terms. In research, problematization

refers to challenging the inherent assumption of a theory or literature. Alvesson and Sandberg (2011) proposed problematization as a methodology for identifying and challenging assumptions underlying existing literature and, based on that, formulating research questions that are likely to lead to more influential theories. Davis (1971) in his seminal study showed what makes a theory notable and famous, is not only the theory that is proved as true but the theory that challenges the existing theoretical assumptions significantly (see exemplification in Davis, 1986). Therefore, generating research questions through problematization appears to be a central ingredient in the development of interesting theories. However, established ways of developing research questions are through gap-spotting or constructing gaps in existing literature. Gap spotting means identifying the gap or area of improvement in existing literature or theory. Some common examples of gap spotting such as "extending... literature"(Westphal and Khanna 2003), "address this gap in the literature" (Musson and Tietze 2004), to "fill this gap" (Lüscher and Lewis 2008), to point at themes that others "have not paid particular attention to" (Thornborrow and Brown 2009), or to "call for more empirical research" (Ewenstein and Whyte 2009). These examples give a clear idea that gap spotting does not challenge the underlying assumptions in existing literature rather it reinforces the assumptions. Referring to the Alvesson and Sandberg (2011) again, the authors provided a typology of what types of assumptions can be problematized in existing theories and proposed a set of methodological principles of how this can be done. The authors described five types of assumptions that can be problematized— 1) In house, 2) Root metaphor, 3) Paradigm, 4) Ideology, and 5) Field assumption.

In-house assumptions exist within a particular school of thoughts that share and accept the same assumptions without any question. For example, if a group of people define a construct with the same items, we can say they have in-house assumptions. This assumption can be

challenged by saying that the construct can be defined differently from individual's subjective opinion and social context.

Root metaphor assumptions are associated with broader images of a particular subject matter (Morgan 1980; Morgan 1997)). For example, in management studies, the organization is seen as a culture of unitary set of values and beliefs shared by the members of the organization. However, this assumption can be challenged by questioning the assumptions around unity, uniqueness, and consensus (Smircich 1983) also questioning the definition of culture emphasizing differentiation, fragmentation, discontinuity, and ambiguity as critical elements in culture (Martin 1988; Martin 2002)

The paradigm assumption deals with the underlying assumptions of ontology, epistemology, and methodology (Burrell and Morgan 2006; Kuhn 1970). A construct can be defined differently from different ontological stance having different assumptions. Questioning the ontological, epistemological and methodological assumptions provide a chance to investigate a phenomenon or subject matter from different angle which in result provide a multiparadigm view.

Ideology assumptions include moral, political, and gender-related assumptions held about a subject matter of investigation. This assumption can be challenged by asking questions from a different ideological perspective. Field assumptions hold a broader set of assumptions about a specific subject matter that are shared by several different schools of thought within a paradigm, and sometimes across paradigms and disciplines. This assumption can be challenged by arguing from the bounded rationality concept. Bounded rationality refers that a group or individual's decision is based upon their existing availability of knowledge.

Rai (2017) mentioned type III errors occur when a researcher answers the wrong question using the right methods (Mitroff and Silvers 2009; Raiffa 1968). A lot of effort may be

expended, a great deal of rigor may be applied, but coming up with the right answer to the wrong question does not create value. Given the importance of research question and discussing the process of problematization it is very tempting to advocate the problematization methodology as the key ingredient in formulating research questions.

## 3.8 Study Design

We conducted this study in three phases. Phase 1 was the pilot phase where were created a panel of GenZers to gauge awareness of information privacy issues. In the literature the importance of pilot studies in qualitative research has been highlighted. Kim (2010), for instance notes:

> "Although pilot studies may have many useful functions in conducting qualitative research, they have attracted scant attention in research literature. A pilot study is referred to as a feasibility study that comprises 'small-scale versions of the planned study, trial runs of planned methods, or miniature versions of the anticipated research in order to answer a methodological question(s) and to guide the development of the research plan" (p. 191)

We undertook a pilot to test of research protocol and our ability to identify the wishes and feeling of the participants. As noted by Watson et al. (2007), pilot studies are usually not suitable for publication and may not produce any results. Keeping this in mind, our pilot study had the following objectives:

1) To evaluate the practical application of the Value Focused Thinking approach.
2) To test the open-ended protocol for gathering the wishes and values of the individuals.
3) To be aware of any other practical issues and difficulties that we might encounter.

In Phase II of the study, we engaged in the actual Value Focused Thinking exercise. We conducted 88 interviews with GenZ. All interviews were from a boarding school in India. All students were in grade 12. There was an even split between boys and girls. Restricting

interviews to one boarding school in one country allows for generalization to the value theory. Although one can argue that the values identified are not universally applicable. In the literature, this is not considered to be an issue. Findings from case studies typically generalize to the theory rather than to the data (see arguments proposed by Walsham, 1995). Walsham argues that generalizations fall into four distinct categories- the concept development, theory generation, specific implication definition, and rich insight. Walsham cites the work of Orlikowski and Robey (1991) regarding the framework they developed. He notes: "their framework could be used to guide studies in two main areas of information systems research, namely systems development and the organizational consequences of using IT" (p. 80). While conducting the interviews, we took extensive notes. We also asked the participants to list their values in writing. We did this to ensure that we captured the richness of the data. Appendix 1 contains copies of all the had written wishes submitted by the participants.

The interviews produced over 350 unique values, which were re-classified into 217 common form value responses. Common form values allow clustering statements into 105 sub-objectives. The objectives were then grouped into 6 fundamental and 16 means objectives. The explanation of the process used is presented below.

In phase III of the study, we created a panel of experts to discuss the findings. The panelists were individuals who had regular interactions with GenZers or were closely associated with their activities. Our panel of experts included the following:

1. Headmaster of the School
2. Two High School Teachers
3. One social worker
4. One University Professor who worked in the area of security and privacy

The objective of the panel discussion was twofold. First to validate the objectives developed in Phase II. Second, to develop insights for policy recommendations, which would become an input for the Delphi Study. We used the Delphi approach to develop a parsimonious set of objectives.

**Identifying values**

Individual interviews are the central mechanism which allows identification of implicit values for a given decision context. The interview typically begins with the purpose being clarified and the context and scope of the interview clearly stated and established. In our study the core objective of the interview is to define the fundamental objectives for GenZ online privacy. The scope of the interview sets the stage for providing explanations to develop a common understanding of GenZ online privacy. This allows for developing a common understanding of the terminology. The interview progresses by posing four questions about personal values toward online privacy. The questions are:

1. What do you think are your wishes in managing your online privacy?
2. What might lead you to believe data is private and secure when going online?
3. What kinds of protections do you want available in order to manage your Internet Privacy?
4. What personal values do you think may lead people to use this information for their own benefit instead of for its intended purposes?

Suitable probes are used to bring out the latent values. Hence all questions are intentionally kept open-ended. This is because individuals can express values differently. In situations where it seems that the latent values are not emerging, probes challenging the respondent are used. According to Keeney (1992), as probing techniques allow for respondents to think of trade-

offs and consequences thus, making implicit values explicit. The following table (see Table 3.1) demonstrates some examples of the implicit values elicited during the interview process.

*Table 3.1, Examples of Values Elicited During Interviews*

| Values | Common Form | Objective |
|---|---|---|
| "Yes, I do get scared in sharing any personal information on social networking sites because it may be misused by people" | Expressing the raw value in a common form | Adding an object and directional preference to create an objective |
| "Yes it's upon the individuals to be responsible in terms of sharing their information because a company can protect their information within only certain limits" | | |
| "Even some of their friends can use it on some wrong way due to jealousy, envy or any bad feelings regarding anybody" | Expressing the raw value in a common form | |
| "Firstly we should be very careful while sharing any personal information. It is our responsibility to protect our information but if we do so then the social networking sites must have security and then it becomes their responsibility to protect our information" | | |

**Structuring values**

Once all the implicit values of the participants are identified and the interviewer feels that additional probing and questioning is not generating any move values, the process stops. This is when a saturation point has occurred. At this stage, the process of value structuring and objective development can commence. To begin, all statements are restated in a "common form," where duplicates of statements that espouse the same thing (yet stated differently) are condensed. Then, these common form value statements are considered and converted into sub-objectives, which can be clustered based on similarity of intended purpose. According to Keeney (1999), an objective is constituted of the decision context, an object and a direction of preference. Again, within this conversion process it is imperative that the integrity of the original implicit value be retained, which means ensuring that the objective sub-clusters still retain the meaning. When all values have been systematically reviewed and subsequently converted into sub-objectives, it may just be that some sub-objectives may deal with a similar

issue and hence may be redundant. It is therefore necessary to determine if these overlapping objectives and clusters should be merged or left as is. A careful review of the content of the sub-objectives helps in developing clusters. Each cluster of sub-objectives is then labeled by its overall theme (or a common identifier), which then becomes the main objective of the cluster (See Table 3.2).

*Table 3.2, Converting Values to Common Form*

| Values | Common Form | Objective |
|---|---|---|
| "Yes, I do get scared in sharing any personal information on social networking sites because it may be misused by people" | I want to ensure that my personal information remain private | Maximize individual anonymity<br>Ensure discrete social media experience<br>Etc. |
| "Yes it's upon the individuals to be responsible in terms of sharing their information because a company can protect their information within only certain limits" | | |
| "Even some of their friends can use it on some wrong way due to jealousy, envy or any bad feelings regarding anybody". | I want to ensure that people who have access to my information are responsible and accountable | |
| "Firstly we should be very careful while sharing any personal information. It is our responsibility to protect our information but if we do so then the social networking sites must have security and then it becomes their responsibility to protect our information" | | |

### *Organizing objectives*

An important aspect of organizing objectives is to classify them into those that are more important than others. Keeney (1992) proposes the use of a WITI test (Why is this important?). Applying the test systematically helps in seeking objectives that are fundamental to the decision context. The WITI test also helps developing a network of means and fundamental objectives. In describing the operationalization of the WITI test, Keeney (1992) notes:

> Repeatedly tracing ends objectives for specific means objectives should lead to at least one fundamental objective in a given decision situation. For each objective, ask, "Why is this objective important in the decision context?" Two types of answers seem possible. One answer is that the objective is one of the essential reasons for interest in the situation. Such an objective is a candidate for a fundamental objective. The other response is that the objective is important because of its implications for some other objective. In this case, it is a means objective, and the response to the question identifies another objective. The "Why is it important?"

test must be given to this objective in turn to ascertain whether it is a means objective or a candidate for a fundamental objective. (p. 66).

The process of structuring the objectives helps in a good understanding of what one should care about and hence, provides clarity of the decision context. It also leads to a clear distinction of the means of achieving the fundamental objectives. While structured objectives form the basis for quantitative modeling. The resultant means-ends framework forms the basis for any strategic planning that may be necessary, thus offering practical benefits.

## 3.9 Approach taken for the Delphi Study

In this research we use the Delphi method to identify important privacy concerns pertinent to the GenZ. The objective of this study is to develop a comprehensive list of key privacy concerns related to the GenZ. The Delphi method is a suitable way to elicit the opinions of the panels of participants through iterative feedback-based convergence and, identify and rank the concerns in order of importance. The Delphi method has some distinct advantages over other ranking methods, which is discussed by Okoli and Pawloski (2004) who describe the strengths and weaknesses of Delphi method with respect to other ranking approaches. In this study, we applied the Delphi method for the following three reasons: One, the Delphi method allows to inquire and seek the divergent opinions and experiences of different participants affected by privacy violations and translate those into a reliable and validated list concerns for both governments and institutions. Two, we employed a ranking method based on Schmidt's Delphi methodology to elicit opinions of panels of males and females through controlled inquiry and feedback (Schmidt 1997). Delphi study allowed privacy concerns to converge to the ones that are important for males and females. Three, the Delphi method allows understanding of the complex issue of GenZ privacy from the perspectives of both genders.

Participants were selected based on the context of the study, determining the privacy concerns of males and females in India. Since our Value Focused Thinking objectives were

generated in the Indian context, it made senses to contextualize the Delphi study in India as well. Therefore, a sample of both males (N= 12-15) and females (N= 9-12) was selected from the same population as the Value Focused thinking participants. There was however no overlap. All our participants were in the 18-21 age group. We selected our sample carefully as these categories represent the predominant demographics of internet users in India. Rural India does not yet possess the high rates of Internet users and the resulting interpersonal intrusions related to online privacy. Hence, it is important for the purpose of this study to select the person's most likely to be affected by privacy violations. Given that the overall research emphasis in this work is GenZ, the Delphi participants also belonged to this generation. We differentiated the Delphi participants in the males and females since the literature (Cupach & Spitzberg 1998; Cupach & Spitzberg 2001; Spitzberg et al 1998; Spitzberg & Rhea 1999; Spitzberg et al. 2001) suggests that there are gender differences and as such we desired to explore these potential differences based on the literature. Therefore, for a study exploring the privacy and of those most affected by it, our sample selection is appropriate as this was done to have a representative sample of a population, which has knowledge of and context for the decision context. Further, our sample size conforms to the suggestions made by other scholars. For example, Schmidt (1997) suggests these studies limit the number of participants to between 9 and 12, prevent them from being intimidated with feedback generated during ranking rounds. Likewise, Okoli and Pawlowski (2004) recommend a group size of 10 to 11 as the results are dependent on group dynamics rather than group size. Furthermore, the participants in this study represented a typical Indian urban population, which allowed us to focus on the generic privacy concerns in India rather than in global terms.

*Table 3.3, The Delphi Study Process*

| Phase | Round and goal | Participants |
|---|---|---|
| *Phase1*: Discovery of the issues | *Round1:* To detect relevant ways and means of preventing privacy violations. | Males and females together<br>Number: 21-27 |
| | *Round2:* To verify that the terms have been properly mapped and that the respondent's ideas have been fairly represented. | Separately<br>15 males<br>12 females |
| *Phase 2*: Determining the most important issues | *Round 1*: to pare the list of issues so that they can be meaningfully ranked. | Separately<br>12 males<br>10 females |
| *Phase 3*: Ranking the issues | *Round 1*: to rank the most important issues for preventing privacy violations. | Separately<br>12 males<br>9 females |
| | *Round 2*: to rank the most important issues for preventing privacy violations. | Separately<br>15 males<br>11 females |
| | *Round 3*: to rank the most important issues for preventing privacy violations. | Separately<br>13 males<br>9 females |

In line with Schmidt (1997) three distinct phases occurred during the process of the data collection (see table 3.3): First, the discovery of issues where participants were solicited as to their preferences for preventing privacy violations. Second, a review occurred where a determination was made as to the most important issues. Lastly, the issues were ranked by the males and females in the study to ascertain their preferred importance. Within the first and third phase of the study, several rounds were conducted, however the second phase only required one round to achieve the desired results. Additionally, Kendall's coefficient of concordance (W) is used in each round to measure agreement amongst participants. Kendall's method measures current agreement (the ordered list by mean ranks) with a least squares solution and is the most popular method for this purpose, mainly due to its simplicity of application for ranks. It calculates agreements between 3 or more rankers as they rank a number of subjects according to a particular characteristic. The idea is that N subjects/topics are ranked (0 to n-1) by each of the rankers, and then statistics are used to evaluate how much the rankers agree with one another.

The details of the findings and how the approaches are articulated are covered in the subsequent chapters.

**[Disclaimer:** Some parts of this chapter were published in a journal article by the author. Materials included here are with the permission of the publisher. Dhillon, S and Nunes, S (2020). Interpreting individual values for information privacy and security. *Journal of Information System Security.* Vol 16(3): 139-14]

# 4
# Pilot Study

## 4.1 Introduction

A pilot study is a small feasibility study, which is designed to test various aspects of the bigger study. Our bigger study would encompass interviewing nearly a 100 GenZ representatives. While access to the target population had been negotiated, the researcher lacked the experience to undertake a massive number of interviews and draw out the relevant values, which could then be converted into objectives. As Lowe (2019) notes, “The primary purpose of a pilot study is not to answer specific research questions but to prevent researchers from launching a large-scale study without adequate knowledge of the methods proposed; in essence, a pilot study is conducted to prevent the occurrence of a fatal flaw in a study that is costly in time and money” (p. 117).

In the literature, it has been argued that a well-planned and executed pilot study helps researchers to identify potential confounding issues and challenges, not only in the process but

in how the items and constructs are organized. There is much debate, however, about the necessity of pilot studies in qualitative research. As Kim (2011) notes:

> A pilot exercise can be especially useful to novice researchers when they assess and prepare their interview and observation techniques. Likewise, pilot works can also be used to self-evaluate one's readiness, capability, and commitment as a qualitative researcher [….]. A pilot work can be used to train qualitative researchers […] and to enhance the credibility of a qualitative study (p. 193).

Kim (2011) also suggests that pilot studies in qualitative research have the added advantage of identifying and articulating epistemological and methodological issues, which helps sharpen the goals of the proposed study. Similarly, Williams-McBean (2019), enumerate the benefits of a qualitative pilot study as:

1. Developing and refining research instruments
2. Assessing the feasibility of recruitment protocols
3. Designing, assessing and refining research protocols
4. Collecting preliminary data
5. Pre-empting possible challenges in data collection and analysis
6. Increasing training and confidence in conducting qualitative research
7. Securing funding

## 4.2 Pilot Study Design

In this research, we designed the pilot study so that we could actually practice interviewing respondents to identify their values. We also wanted to assess if privacy was indeed an issue for GenZ. Therefore, to conduct the study, we developed a scenario, recruited GenZ participants, conducted interviews and assessed the value of the interviews in drawing interpretations. The pilot study design is illustrated in figure 4.1.

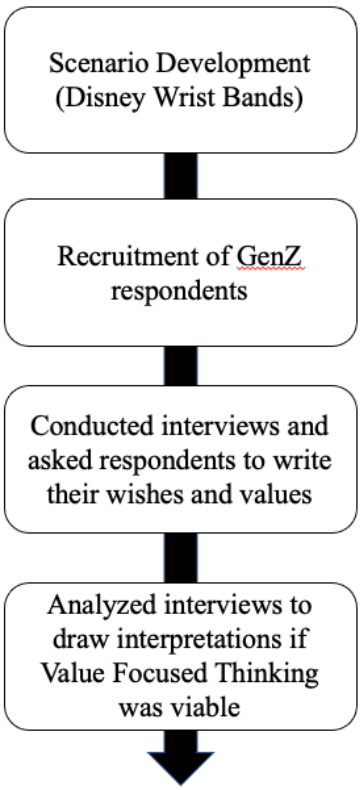


*Figure 4.1, The process followed in conducting the pilot study*

**Scenario Development**

While the main study does not use any scenarios, for the purpose of the pilot, we decided to use a scenario. Box 4.1 describes the scenario.

*Box 4.1, The scenario adopted for the study*

**The Privacy Risks of Disney's Magic Bands**

When you last visited Disney World, did you use a MagicBand as you traveled throughout the parks? Disney hotel guests are automatically given a MagicBand for their visit, but the "old-fashioned" hotel key card is always still an option. MagicBands are marketed as helping visitors have a more magical vacation—from FastPass ride access to facilitating purchases (you can tie your credit card to it) and collecting photos taken by Disney's

photography team. You can even access your hotel room using the bands. As an extra security measure, Disney requires the use of fingerprint or pin code to verify your identity.

We frequently hear of new instances where companies are found to be using personal data in ways individuals never anticipated or didn't know was happening. Disney's MagicBands are governed by six policies on the MagicBand's Privacy + Legal page.

Oh wait, I just realized that those aren't the policies. They are simply the privacy FAQs. I had to look further to find the real Privacy Policy and Terms of Use. Both of these are significantly less user-friendly and make it clear that Disney is tracking users and collecting/sharing data in ways that aren't apparent on those six pages.

The six FAQ pages explain the different features these bands integrate with and provide a different lens to view the FAQ pages through. In an era of privacy where consent and notice is at the forefront (GDPR anyone?), a tangleweb of legal jargon for visitors to navigate does not line up with the visitor-first, "Happiest Place on Earth" mentality that Disney seeks to project.

The FAQ page says that it doesn't track people around the parks via GPS technology, but the wristbands nonetheless interact with RFID readers throughout the properties. The RFID FAQ page specifies that the MagicBands are "used to deliver personalized experiences, as well as provide information that helps us improve the overall experience in our parks." But the Privacy Policy also says generally that they're collecting location data in various ways, including through beacon technologies. Does this mean, then, that Disney isn't tracking their guests via GPS technology but they are doing so at various points throughout the park using RFID readers?

Is Disney storing fingerprint data? I couldn't find anything about fingerprint data in the full Privacy Policy or Terms of Use. The only mention of fingerprint data collected at park entrances to verify the MagicBand wearer's identity is the following language found in the Help Center here: "In order to use Ticket Tag, you simply place your finger on a reader. The system, which utilizes the technology of biometrics, takes an image of your finger, converts the image into a unique numerical value and immediately discards the image. The

numerical value is recalled when you use Ticket Tag with the same ticket to re-enter or visit another Park. Ticket Tag does not store fingerprints." How do they compare the fingerprint to the unique numerical identifier already stored in the system? I don't know how the Ticket Tag system works, but without any sort of mention of it in the formal legal notices, I can't help but wonder if the image deletion works the same way for Disney's Ticket Tag system as it did for Snapchat…in other words, perhaps the images aren't actually deleted.

I know companies frequently try to brush past certain types of data collection or tracking in the hopes that their consumers or visitors never notice, and it's absolutely true that these MagicBands provide visitors with convenience and ease. However, Disney needs to be upfront about how they're using their guests data or they run the risk of tarnishing their perfect reputation.

(Source: https://privacyengle.com/2018/04/14/the-privacy-risks-of-disneys-magic-bands/)

**Recruitment and Interviews**

We recruited 39 students from a local high school to participate in the study. All students were GenZ. The participation was voluntary. We blocked one hour of their schedule, where they were presented the scenario. They were asked to read it and then think freely and then talk about their feeling, wishes, values and opinions. The interviews were spread over 4 days, where the 39 students were brought together. The interviews were open ended. A synopsis of the interviews is presented in paragraphs below.

Disney has developed this wearable technology known at MagicBands that can be used at any of their parks and resorts. This device can be used to unlock hotel rooms, track location, view images, and make purchases when linked to the MyMagic+ app. However, when using technology this advanced, where it has access to your location and payment information, can

cause several privacy concerns. Disney has taken precautions. Disney claims that no personal information is stored within the device, but instead, it contains a code that identifies users. The bands can easily be disabled and replaced if one is stolen or lost. Given this context, we interviewed the first group of respondents asking them two open ended questions - "What are their wishes about protecting their privacy when wearing devices such as Disney's Magic Band."

***Batch 1 interviews***

When asked the question about privacy protection and smart watches. One respondent, Blake, said he does not really have many concerns about privacy protection when using such devices. "Growing up in a world with technology everywhere, being able to purchase items and see someone's location seems normal," said Blake. Blake's only true concern is banking information being stolen, but with technology being so advanced, he said, "I can turn my card to hot mode in a matter of seconds with my Wells Fargo app." Another respondent, Davis, has a different perspective on smart watch technology. Davis mentioned that she did not become familiar with most technology until later in life and never used social media. Her biggest concerns are being tracked and easy access to banking information. "I am not as familiar with technology like many others are, so I do not know how to disable the tracking services or have easy access to turn off my banking information. Davis said, "If my smartwatch or cell phone were to get stolen, the only way I know how to disable my banking information is by calling the bank directly and without a phone on hand it could be a while before I could make that call." She also mentioned that she is starting to learn more about the tracking features because she wants to be able to track her children to make sure they are safe, but she questions that since she can track her children so easily, what would make it hard for a stranger to also be able to track them? These were two interviewees from two very different generations and due to that, they seemed to have different opinions on smartwatch technology.

Similar to the above participants, two more people were interviewed on the wearing of devices such as Disney Magic Bands. Donnelly said that using devices such as the magic bands or fitbits do not concern him since we are already surrounded by so much technology that already gathers our information. “There’s no escaping it. You can’t be worried about your privacy on a smartwatch if you have a smartphone.” He went on to explain that our cell phones basically track our every move and know more about us than we think. “How do you think they know what ads to show us online?” Another person interviewed, Taylor, also did not have any concern about wearing devices such as smart watches. “Our information is already tracked anyway. The only real concern is if these devices were to be hacked, which can happen on any device.” Taylor continued to explain that the risk of your privacy being exposed through technology comes with using any device, and it’s almost unavoidable at this point in time.

Two other subjects that were interviewed had even similar responses. One interviewee stated that they wouldn’t care about the privacy on such devices since the company has already made a reputation for having secure information with their devices. The second interviewee also stated a similar response from those aforementioned; everything else we use is being tracked/recorded/secured. So why not keep using the products from brands I already trust?

Two other interviewees shared contrasting opinions on the matter. Brown, feels that this is an unethical practice that Disney is engaging in. “Disney is designed to be a children's park. Having the need to “identify” someone while storing their information is ridiculous.” He feels like Disney should just use a username basis on the MagicBands instead of saving your personal information on the band. Another respondent, Powell, however, feels similarly to the subjects above and does not care that Disney stores your information. She believes most places already engage in the same behavior.

In another two interviews with John and Jais about how they feel about their security with the watches they wear on their wrist. Jais said that he doesn’t care too much if his FitBit is not

secure, as he doesn't do much with his FitBit anyway, besides checking his heart rate and how many steps he took. John, on the other hand, would worry if something happened to his watch as he texts, calls, and uses his cards with his Apple Watch, so he would worry if his watch was lost or hacked as they could steal his info.

Another respondent, Alexis, goes to Disney every year and she stated when I asked her about her privacy concerns while having a MagicBand that she likes the efficiency and ease it gives using it around the parks but it does make her uncomfortable knowing that Disney is tracking all her purchases and movement around the parks. She told me that she would get Ads then popping up telling her places to go which she knows Disney is doing to help easily navigate her trip but thought it was weird that they knew she was in one park and it was telling her where to go. Another interviewee responded that she has not worn the Disney MagicBand but she wears an Apple watch every day and stated to me that her concern is Apple not requiring a passcode on her watch. She has put a passcode on her watch but if she did not there is the risk that if she were to lose it or if someone were to hack into it, that they would be able to get her credit card information because she uses her watch to pay for things with apple pay.

Another respondent, Nick, found it surprising that Disney is using bands to track certain purchases and where you stay across the resorts that Disney offers. What he thought was, kids can also have this band which can be found as a problem. Kids often lose things which leaves them exposed to losing out on information such as credit card, addresses and room information for personal property to be taken. Another respondent, Drayven, thought it was a wonderful idea to have a band across all parks. It is innovative, nobody has ever done this. The problem with this is he added was, people within Disney can use this information for harm. For a company to have so much access to like this is scary and hopefully no kind of lawsuits would come out.

Another two respondents, Riley and Logan also had another perspective about privacy. Both of them gave me similar answers, being that they wanted to be sure that their personal information was secure. With these devices having access to payments and room keys, their major concern was losing it and having the person who found it have access to their personal information. But as previously stated, Disney has precautions in place to make sure that this does not happen, and once I explained how they protect that information, they were very much on board with the Magic Band system. We all just want to make sure that we are protected in case of technological issues, and if there are safeguards in place to protect us, then there are no downsides to these technological advancements.

***Batch 2 interviews***

In the second round of interviews, we interviewed a significant number of GenZers. One respondent, for instance, was concerned that the Disney band will steal her private information and she would prefer not to wear any device that contains credit card information. She is concerned because of the lack of information about the systems to the public. If there was more information she would feel more at ease. Another interviewee was not as concerned as her, but she wishes there were notices before any devices/applications start to follow your location. She also has had experiences with having information stolen and then having to get rid of her device all together and it was a pain. None of the interview subjects have used Disney Bands but said they would prefer not to if there was another option available.

In our interviews with another two individuals about protecting their privacy when wearing devices such as Disney's magic band or devices such as fitbits. The first respondent said that one of his wishes would be to not have his location enabled or shared with the company. Also, he wants a guarantee that he will have privacy by not being listened to by his device or recorded without his knowledge. The second interviewee said that he wishes to not have his health data tracked, recorded, and sold. He says he does not want the company or a third party to have his

health data or know what current state of health he is in because that is personal to him. He also says that he doesn't want his location to be tracked and shared with the company unless he is made aware of the fact that he is being tracked. Overall, what was gathered from the two respondents was that the main concern regarding privacy has to do with location. Both interview subjects expressed that they do not want their location tracked or seen by the company whose product they are using, nor do they want that information collected and sold or shared to a third party.

In another set of two interviews, we again asked about their concerns of privacy issues with devices such as Disney's Magic Band, and what their wishes are regarding these privacy issues. My first interviewee said that they would feel more at ease if they knew where their data was going as it is being collected, and what exactly it is being used for. My second interviewee would feel at ease with a Disney Magic Band knowing that it can be deactivated. In a place as large as the Disney parks, it can be easy to lose something small like the band. Knowing that it can be deactivated if lost or stolen will help customers feel better about them given all of the data that the bands have access to (credit card information, names, etc.). Luckily Disney has already implemented this feature in order to prevent identity theft from occurring within their parks and Disney having to take responsibility for it.

In another set of three interviews, we asked people for their thoughts about magic bands. The interviews show that most people will forgo privacy if there's a quicker easy option. One person said that they would use a magicband as it makes it easier to access rides and reserve times to ride at the park. It also is stylish and can be counted as a free souvenir. Another participant said they like magic bands just because they like how it's reusable and they would rather give up privacy in order to use less raw materials and have them be thrown away after use. The third interview subject seemed to dislike the lack of privacy but exclaimed that

Disney's track record with user data is solid, so for now, they trust the magic band and its ability to safely be used.

In another set of three interviews about what their wishes are regarding protecting privacy when wearing devices such as Fitbit, different opinions emerged. One respondent stated that he never has trusted technology and never will. He still currently owns a landline and refuses to get a cell phone or any other type of technology. I asked if there were any modifications that could be created that would convince him that technology is okay. He replied by saying, “I do not care about what privacy protection modifications they come up with, because I will never use anything besides my landline, tv, and car. Those three alone are already too much technology for me.” Another respondent, who is much more tech savvy, said that, double security protection would make him feel more secure. For example, not only requiring a password, but also installing a face scan to ensure someone is not trying to steal your information. The third respondent said that he does not trust Fitbits or MagicBands because he thinks it can be hacked too easily. I asked him what innovations would make him feel more secure and he told me nothing, because no matter what comes out, he will not trust it. He said he is fine sticking with his basic technologies and that is it.

In other interviews, a respondent said that he did not see any problem with the privacy of the system. His viewpoint on the system is that the people that sign up and pay for the wristbands are voluntarily giving access to their privacy. So, if someone has no problem with their privacy being invaded then they would pay for the wristbands while others would not. Another respondent had a different point of view that people who pay for the wristbands want a certain level of security and privacy when they use them. Tracking peoples’ locations and connecting to credit cards through Disney wristbands could become dangerous if there was a breach in cyber security or if someone was able to obtain information from scanning the

wristbands without someones knowledge. These different viewpoints challenge how Disney could do business, depending on which is seen to be the more popular.

Another two respondents expressed their wishes about protecting their privacy when wearing devices such as the Disney's Magic Band. Both respondents were very similar in ways. The first stated that they understand the purpose of a device such as a Disney magic band but worry about whether or not their information is protected. A couple of their biggest things were that they "expect my credit card information is protected, that the bands are not able to be hacked into, and once I leave the park the data connected to the band is deleted." I think that these are very good questions to be asked before turning over your information. The second respondent had some similarities, like once you exit the park that the band stops tracking your location. "I understand that products like that are made to make your life easier, but I don't want my information to be shared with anyone." Another example she brought up is the Apple watch and how she does not want any of her exercise, step count and heart rate information to be shared with the company or any of its affiliates. I think that these are all very good points and are something we should take into consideration when it comes to using these devices.

In another two interviews about protecting their privacy when wearing devices like MagicBands, other interesting wishes emerged. One of the respondents explained her concern on how it invades the privacy of her location. She is worried that wearable devices can track her location and hackers could find her location. She wishes that there's precautions of the privacy of her location. The other respondent explained how her concern about her Fitbit is that her personal health information is being shared. She wishes that it could be proven that her personal information is private to only her and her Fitbit.

In two other interviews similar concerns emerged. One respondent said that when she uses the Apple watch, how it gathers her health information, and is concerned of whether that information is being shared with other servers, or sites. The second respondent said that you

know what the risks are, so at the end of the day it is your choice and you have control over it. Having a feature that has a private mode, which will give additional security.

Four other interviews revealed similar values. The first respondent said this "I want to make sure none of my personal data is stolen. My fitbit tracks my location and I don't want that stolen." The second respondent said, "Data protection is my number one worry, I'm pretty sure Disney's magic band has access to photos taken at the park and my credit card information and I can't have that information hacked or taken."

The third respondent said that they didn't really care about their privacy. They just hoped that nothing was recorded that they said or did. But overall felt not worried whatsoever. The fourth respondent said that she was worried about texts or various things like that being observed by outside people and that really worries her for her privacy.

Box 4.2 presents a summary of some other miscellaneous responses from a range of interviews. Overall, there seems to be split between caring and not caring at all. If they did care about the subject it was based upon the idea that if you were wearing this piece of technology on your wrist all the time somebody could potentially have access to your location at all times. It brought up the idea that they could tell things like your patterns and when you were at home or when you were out of the house. The opposite side of the argument from the respondents was the trust and faith in the company to truly protect information like that and not let it fall into the wrong hands. Respondents also doubted that even if the information was leaked about something, like your location, that somebody could actually exploit you somehow with the information. Yet, others wanted the option to control who could see this type of information. What is evident however is that after a while there seems to be a saturation in the content. In our case we felt that after about the twentieth interview there was some repetition in the themes. Yet, it is worthwhile continuing with the interviews since one needs to develop a full perspective.

*Box 4.2, Sampling of interviews and quotes*

**Sampling of interviews**

"My biggest wish is that the devices wouldn't collect, use, track, or share my information. Once you have my information, they can use or share it if they chose and now my right to privacy has been taken from me. Also, there is a real possibility that hackers could access and steal my information. I'm sure they have advanced protection against hacking but it still happens. I know a girl who had her identity stolen in the Equifax leak and had access to her SSN and she couldn't go to college because of it. It's far too much information to be sure that someone is going to take care of it."

"My biggest thing is location tracking. Honestly, there are so many other ways they (hackers) could get my information anyway. It makes me uneasy knowing that someone has the possibility to roll to somewhere I'm at for any reason whatsoever. I don't like that the option is there."

"Personally, I feel that having our cellphones on us is tracking our location constantly anyways so I don't really care if it's like Disney is or my Apple Watch. I kind of signed my life away when I agreed to those Terms & Conditions with Apple so I just try not to think about it, ignorance is bliss."

"I think there are a lot of pros to tracking your location, I think the only con would be like if you're doing something you shouldn't be. Or if like bad people track your location, like sex trafficking. Also, that would be a positive because if your location is constantly tracked then all of these missing people could be found because you know where they are."

"I want to say the same thing [as the above interviewee]. I think that it could also be safer for companies to have our location and if they like it if they went a little more in-depth with it, like maybe it could help kids who like get lost in all of these parks and stuff. I feel like kids do that all of the time and like if somebody gets lost or their kid gets lost, you can just go up to an officer because there's officers there all of the time, and I guess help them find you easily."

"I enjoy how much easier technology like this makes everything, but the data mining of it all concerns me considerably. I do not like companies collecting data on me and I try to avoid it as much as I can. I do have a smartwatch and am aware of the tracking capabilities it has, but those are the capabilities that interest me most. I want to be able to know how many steps I take each day and to be able to monitor my heart rate, but you never do know what the companies collecting that data are doing with it. [My family does] not give out any personal information unless it is required. It is important to protect your personal information as much as possible because it can be sold so easily."

"I think that having constantly our location is scary because if someone wants to rob us or do anything to us they know where we are, but on the other hand I would say that if we lose someone we will know where to find him or her."

"I think it is a very good thing because if you want that kind of deal you know what you are putting yourself into, so I would say that is a positive thing and since there are a lot of people in the parks it's an easy way to prevent dangerous situations."

"The band definitely sounds convenient and useful, but is it (Disney Magic Band) training your location… possibly listening to what you're saying? Who is receiving the data? Is the data received, kept, stored on a secure network? When is it deleted, if at all? Basically, how can I be sure the data isn't used for anything but the bare minimum during my time at Disney World?"

"My biggest concern would be identity theft or unauthorized credit card charges, along with general privacy and "Big Brother" knowing my whereabouts. What happens if it gets in the wrong hands, say through a hack of some kind? I would be skeptical of using the band and very cautious."

"I wouldn't want the band to know in any way that I was by myself... My credit card information I would be worried about… My whole legal name. What if I lose it? (And someone got ahold of it) As for what I "wish" about protecting privacy, I would just hope no one gets the data that doesn't need it, and that park staff would be respectful of me or my family's privacy."

**Paraphrased interviews**

She doesn't want her information to be shared with anyone. She doesn't want someone to be able to take her information and do something reckless with it. When she wore her Magic Band at Disney, she was concerned about it falling off her wrist and someone finding it and charging stuff to her card.

She thinks it is weird to wear a device that will let someone know exactly where she is or where she went. Although she does think that it would be beneficial to Disney to know what rides and other attractions are popular within Disney so if there is something that is not bringing in a lot of visitors then they could make it into something else.

He trusts the device; he just knows what the company will do with the information in a detailed format.

He likes the idea of the device, but he wants his information to stay with the company and not get spread or it to be deleted once the device is removed.

He is afraid of how much information the device can obtain from the user and doesn't fully trust the intentions of many companies with consumer privacy. He says privacy restrictions should be enabled to allow confidential information to remain with the device, and not give permission for the company of the product to save information and sell it.

She believes that the purpose of the device is beneficial for personal use, however understanding how much information gets transmitted to the company cannot be fully trusted, because you are unaware of how much most devices can invade your privacy. She thinks personal devices that contain such personal information should stay private within the company. More security should be added to make sure this information is secure.

## 4.3 Lessons learned

There are several interpretations that can be drawn from our pilot study. We enumerate those lessons learnt below:

1. It became clear that a larger number of interviews are necessary to achieve a saturation point. In the pilot study, we recruited 39 GenZers. While some of the respondents provided detailed responses, others presented a cursory evaluation. Given the prevalent diversity among the GenZ respondents, we believe the in the final set nearly 100 or more interviewees should be recruited.

2. During the pilot, we did not ask the student to write down the wishes. This meant that we were interpreting the GenZ wishes and values after the interviews. While this works in some cases, it poses some challenges in terms of identifying the exact value set of wishes. Based on the pilot study, we decided that besides individual or group interviews, we will ask the respondents to write down their wishes and values with respect to privacy. For this reason, we include the detailed write up of what each respondent said in Appendix 1.

3. We also felt that GenZ were generally knowledgeable about the privacy concerns. Many of the respondents in the pilot study noted that thought interaction over social networks and in interactions with Disney Magic Bands can be beneficial, but if not careful, it can drive numerous unwanted results, such as privacy violations. Especially, it might target young females, including celebrities, GenZ. These matters can take different forms, including scandal, and threats. The targets may be to control or intimidate the victim or to gather information for use in other crimes, like identity theft or offline stalking. While blame shouldn't be placed on victims, the current online view allows itself to create easy targets. For instance, nowadays, many social media users think nothing of publicly posting personal information, sharing their feelings and desires, publishing family photos, and more.

4. We also came up with some simple solutions that would help: To avoid privacy violations as with many things in life, and it's much better to be proactive than reactive when it comes to privacy. Retaining a limited profile in online existence is tough for some people, particularly those who require using online platforms for self-promotion, or business-related activities. However, many users could benefit from toning things down a little. One should always avoid posting personal details such as your address, phone number, and think carefully about revealing real-time information such as where you are and who you are with. Avoid using your full legal real name if one wants to create social online profiles like Facebook, Instagram, or Twitter. Avoid disclosing sensitive information by not sharing personal information about themselves, even outside of social media platforms.

5. Additional key issue, if one is under attack for a privacy violation, one may need to clean up their online presence even further by deleting any old accounts and trying to remove any information or images that pop up in search queries and employing false profiles to act as baits to the stalker. This may sound strange, but it could be a significant help in some circumstances to the victim by adding profiles to social networks that include fake personas using your name or picture. One can provide those profiles with different addresses, jobs, and interests, etc. Also, one can modify some information in real profiles, and use one of the fake accounts as primary for some time. This tactic will help to mislead the perpetrator and create doubts about individual identity. Just be sure, to review the rules and regulations for those platforms before doing this change.GenZ privacy is a big problem, but it is easier to prevent it than to try to solve it and eliminate the consequences.

# 5
# Privacy Objectives of the GenZ

## 5.1 Introduction

This chapter presents fundamental and means objectives for ensuring privacy of the GenZ. The privacy objectives are results of the value focused assessment and are based on a large number of interviews. The details of the interviews were presented in chapter 3. As noted previously, we used Keeney's Value Focused Thinking theoretical and methodological approach to develop objectives for ensuring privacy of the GenZ. In the following sections we present a detailed data analysis and discussion of privacy objectives specific to GenZ. Our discussion focuses in each of the fundamental and means objectives, what they mean, what our respondents said and how the objectives relate to the extant literature.

The research community has long recognized the need to clarify values as a means to develop organizational strategies. Selznick (1984) noted that sound organizational leadership

requires an appropriate ordering of human affairs. This includes establishing order and the determination of public interest such as ensuring the defense of fundamental values. For an organization to achieve a level of excellence, Peters and Waterman (1982) propose that they need to figure out their "value system". This line of reasoning is supported by Keeney's (1994) claim that values define all that you care about in a specific decision context and that they act as guiding principles for evaluating the desirability of any possible alternative or consequences. The process of thinking about values forms the basis for quality decision making by creating alternatives, identifying decision opportunities, guiding strategic thinking, interconnecting decisions, guiding information collection, facilitating involvement in multiple-stakeholder decisions, improving communication, evaluating alternatives, and uncovering hidden objectives (Keeney 1994).

As noted by Keeney (1994), identification of values can only be undertaken if there is a clear and an explicit statement of the overall objective. An objective is grounded in the decision context and hence represents something that an individual aspires for. There are three components of an objective – the decision context, an object and a directional preference. Keeney (1994) noted that the process of interviewing research subjects will typically generate an initial list of raw items, however these items are not solely expressed as objectives. The process of identifying and structuring objectives is a difficult task and the relation between the objectives is easily misconstrued, leading to an unclear understanding of the relationships among objectives. Having clear and well-defined objectives is important to fully understanding problem domain and the contextual aspects of the decision to be made.

For the purpose of classifying objectives, we use the method applied by Dhillon and Torkzadeh (2006) and define objectives at two levels. In order to simplify the organization process of objectives, Dhillon and Torkzadeh (2006) restates values in a common form structure. Converting the raw values into common form values allows for duplicates to be

removed. The common form values are then converted into objectives. The objectives are then clustered into thematics and given a common identifier. As we progress from values to common form values to objectives and clustering, duplicates are systematically removed. The process also allows for themes to emerge, this makes it easier to perform the WITI test discussed earlier.

## 5.2 Fundamental Objectives for GenZ Online Privacy

Our research establishes six fundamental objectives. These are: Increase trust in online interactions; Maximize responsibility of data custodians; Maximize right to be left alone; Maximize individual ability to manage privacy controls; Maximize awareness of platform functionality; Ensure that personal data does not change. In paragraphs below we discuss each of these in more detail.

**Increase trust in online interactions**

Social media users need to have an ability to increase their trust that their personal information is not being compromised. The trust not only needs to be amongst the users, but also between the users and the platform. *Trust in online interactions* is the extent to which individuals can rely on what is being said by the other party. If an individual cannot rely on the other party, there is bound to be a lack of uptake of the platform or of the information that is shared. Lack of trust, therefore, leads to underutilization of the systems and platforms. Businesses and online platforms constantly classify content and user patterns to ensure they are targeting the right kind of information. While this may be important from a business perspective, there are challenges in how the users perceive such actions. As Lyon (2019) notes:

> "… Facebook "connects" users with other acquaintances, family members, groups and so on, as heavily advertised from the beginning. But it also connects users with unseen others – the data brokers, developers, advertisers, political campaigners and snake-oil vendors that pay Facebook for data about these valuable connections. This is Facebook's business model, which falls squarely into the surveillance capitalism

category. People are attracted to the site and encouraged to spend more and more time there so that their attention, their interests, the details of their daily lives, may be sold to the highest bidders. As data are donated, unwittingly, or at least only vaguely perceived, by users, so the data are used to profile those users and their friends and acquaintances, including those with no Facebook account. As with all social media, these interactions with the site are the source of value. And their aim is not merely to predict but also to shape lives and lifestyles." (p.66)

When occurrences such as surveillance take place, it becomes challenging for the users to build trusting relationships. Therefore, establishing a trusting relationship between different parties is the primary goal. One of the respondents in our study noted:

"I am always concerned when I don't know what is happening behind the scenes. When I use Tik Tok, how come I only see materials around the topic area I had seen before. I have no control in changing my settings or being exposed to a broader range of information. I always feel that the *machine* is watching me."

Another responded commented on platform trustworthiness:

"I want to deal and work with people and platforms I trust. I am certainly not going to add my personally identifiable information on a platform I don't trust. In some cases, I just put in fake information. Or I use private windows to browse."

The concepts of trust and privacy are interlinked. Wang, Lee and Wang, (1998) found trust and privacy to be the most critical issue that leads to fear and distrust among people. Scholars who have used the social exchange theory to study trust suggest that trust is the single most essential asset that needs to be nurtured and protected (see Zucker, 1986; Benassi, 1999, among others). There is a rich tradition of research in this area and over the years scholars have worked on identifying antecedents of trust. As Chen and Dhillon (2003) note:

"As suggested in the literature overall trust of a consumer in an Internet vendor is determined along three dimensions. These are competence, integrity and benevolence of the firm. Detailed description of the constructs has been presented in previous sections. It is worth noting however that an idiosyncratic

combination of competence, integrity and benevolence results in an intention to purchase or not purchase online. If we argue that trust in an Internet vendor is a key driver to realize a sale, as has been suggested by Torkzadeh and Dhillon (2002), then it is of paramount importance to focus attention on abilities necessary to deliver a product or a service, benevolence and the general integrity of the business." (p. 314)

**Maximize Responsibility of Data Custodians**

Responsibility and custodianship has been an ongoing issue. While in our study the GenZ identify it as an issue of concern, the origins of such concerns can however be traced to the medical field. In an editorial of the *British Medical Journal*, Peto, Fletcher and Gilham (2004) note:

"At a public meeting in November 2002, organized by the Parliamentary Group on Cancer and opened by Alan Milburn, then secretary of state for health, the audience were provided with an electronic voting facility. After a discussion of the restrictions on access to medical records that British epidemiologists now face and their effects on our work, the audience were invited to vote for or against the following proposed law: Consent is not required for access to medical records for non-commercial medical research that has no effect on the individuals being studied and has been approved by an accredited research ethics committee." (p. 1030)

No doubt there are nuances when it comes to medical data and other data in general but given the emergence of social media firms and what Zuboff (2019) terms as surveillance capitalism, the issues related to data custodianship have come to the centerfold. Zuboff (2015) argues:

"Data about the behaviors of bodies, minds, and things take their place in a universal real-time dynamic index of smart objects within an infinite global domain of wired things. This new phenomenon produces the possibility of modifying the behaviors of persons and things for profit and control. In the logic of surveillance capitalism there are no individuals, only the world-spanning organism and all the tiniest elements within it." (p 85)

While the notion of data custodians is not new, it has always been closely intertwined with the information privacy domain. Privacy breaches in recent years have only reinforced the need

for data stewards. Table 5.1 summarizes some of the information privacy breaches, which have directly called for the need of data stewards.

Good data custodianship is defined as the ability to comprehend the data flows between different components of a system and have individuals responsible for the safe custody of the data (Pym and Sadle, 2010). Given the distributed nature of computing and how social networks and data flows works, attributing responsibility and data custodians is a challenging task. Nevertheless, companies are cognizant of the need largely because of their fiduciary responsibility (see Rosenbaum, 2010).

*Table 5.1, Major information privacy breaches (compiled by the author)*

| Information Privacy Breach | Records | Call for Data Custodians |
|---|---|---|
| CAM4 – adult live streaming owned by Granity Entertainment (Irish)[*] | 10.88 billion | no |
| Keepnet Labs – UK based security company[+] | 5 billion | yes |
| Whisper – a "secret sharing" app[#] | 900 million | no |
| Estée Lauder[@] | 440 million | yes |
| Microsoft[**] | 250 million | yes |

[*]https://www.helpnetsecurity.com/2020/05/06/cam4-leaking-data/
[+]https://www.verdict.co.uk/keepnet-labs-data-breach/
[#]https://www.infosecurity-magazine.com/news/fetishes-exposed-by-secretsharing/
[@]https://threatpost.com/estee-lauder-440m-records-email-network-info/152789/
[**]https://www.itgovernance.eu/blog/en/250-million-microsoft-customer-records-exposed-in-latest-breach

In our research, GenZ participants expressed concern of possible breaches and how the platform or the responsible company could ensure their protection. One participant stated noted:

> "If my information gets hacked or is disclosed accidently, someone needs to be responsible. Recently I suspected that someone had unauthorized access to my Instagram account. I tried contacting them and finding a means to reach to the company but had no luck. This has to be simpler than it is now."

So there clearly is a concern that individuals are worried about their personal information and want responsible individuals to ensure their security and privacy.

**Maximize right to be left alone**

Recent privacy scandals have brought the age-old privacy call, the right to be left alone, to the fore. In some cases, the authorities have arrested and persecuted the perpetrators, but it has not deterred other folks to engage in criminal acts. Recently profile accounts of Elon Musk and former President Barrack Obama were used to commit privacy violations. As reported by *Vox*, the perpetrators were eventually arrested[7]:

> "A teenager in Florida allegedly played a major role in the massive Twitter hack earlier this month that commandeered some of the platform's highest profile accounts, including Elon Musk's and former President Barack Obama's, to scam people out of about $120,000 in bitcoin.
>
> Graham Ivan Clark, 17, was charged with 30 felonies related to the hack, according to a local news station in Tampa, Florida, where he lives. Though federal authorities led the investigation, Clark was charged by the state's attorney because, state attorney Andrew H. Warren said, Florida law makes it easier for Clark to be tried as an adult."

Information Systems scholars have argued that increased use of information and communication technologies have resulted in privacy challenges (e.g. see Mason, 1986; Straub and Collins, 1990). In a seminal article, Mason (1986) argues:

> "Two forces threaten our privacy. One is the growth of information technology, with its enhanced capacity for surveillance, communication, computation, storage, and retrieval. A second, and more insidious threat, is the in- creased value of information in decision-making. Information is increasingly valuable to policy makers; they covet it even if acquiring it invades another's privacy" (p. 5).

What Mason wrote over 35 years ago is still valid and more recently Zuboff (2019) has made similar arguments when discussing surveillance capitalism. The right to privacy is an important ethical issue and, in the literature, it continues to be discussed. Several international

[7] https://www.vox.com/recode/2020/7/16/21327474/florida-teen-arrested-twitter-hack-joe-biden-election-2020-security . Accessed Dec 25, 2020

institutions (UN, EU) have declared privacy to be a fundamental right. However, in the US there is still contention regarding the fine balance of what is private and what is not.

Our respondents were very much sensitized to the notion of privacy as a right and how they felt various platforms should address the issue. One respondent noted:

> "I, as an individual, should have the exclusive right as to how my information is collected, stored and saved. I should also own my personal information."

The respondent clearly seeks to preserve the right to know all aspects of the information that is collected and saved. In a study by Freedman (1982), the "right of information privacy" is highlighted and considered as something that individuals control regarding collection, storage, use and dissemination. Another respondent for our study noted:

> "I need to have the right to access my personal information. For me that is the fundamental right to privacy."

The literature has addressed this issue as an ethical concern. Parrish (2010) for instance, uses Facebook as an example to point out issues around information ownership. In 2009, facebook had changed the terms of its contract to retain user information indefinitely, even after their accounts ceased to exist, only to revert back to the original policy three days later. In this regard, Parrish notes:

> "Despite the fact that Facebook retreated on their changes to their terms-of-service contract, users should still consider carefully the content they wish to share on SNS if they don't want to lose control of the information forever. This has nothing to do with the site. Rather, it has to do with search engines and their ability to cache content. Say, for example, a user posts an image on a social networking site and then thinks better of it a few days later. If it was cached by a search engine, it will still be accessible regardless of whether or not it is removed from the site" (p. 191).

It is therefore important that organization define their privacy agreements correctly and remain cognizant of the rights of individuals. At the same time, establishing custodians and proper responsibility and accountability structures are also important.

**Maximize individual ability to manage privacy controls**

Today, mankind has increasingly become dependent on technology. For example, at the beginning of the 20th century, there were a variety of different ways in which people could be entertained. This may have involved attending dances, live events, amusement parks, or playing a game with neighborhood friends. Over the years, such active entertainment has gotten converted into "passive" entertainment. Binge-watching Netflix, for instance, dominates most GenZ people. The consequences of technological reliance have its ill effects. A recent survey[8] found that about 37% of young people between the ages of 12 and 17 have been bullied online. And for some 30%, it happened more than once. The survey also revealed that girls are more likely than boys to be both victims and perpetrators of cyber bullying. 15% of teen girls have been the target of at least four different kinds of abusive online behaviors, compared with 6% of boys. All our respondents were in the age group of this survey and findings from our interviews resonated with them. One respondent noted:

> "I have just learned to ignore all the unsolicited Snapchat messages I get from people I don't even know. And some of them are not nice. At times I get a feeling they know an awful lot about me and what I do. This is to a point where I feel that they know me or have been stalking me."

Another issue that was identified is that of identity. While the inherent complexity of online environments requires stronger identity controls (Gopalakrishman, 2009), but systems and platforms do not necessarily consider such controls proactively. Often what the users want and

[8] https://www.dosomething.org/us/facts/11-facts-about-cyber-bullying Accesses January 1, 2021

what social media site might offer is not in sync. Syed, Dhillon and Merrick (2019) term this the *value gap* and note:

> "Given the problems of identity threats on social media, it is prudent to understand the gap between what users wish to protect and what social media sites provide via the current security and privacy controls. We term this as a *value gap*. [Hence] any effort to manage online identities will require a comprehensive analysis of individual values and how social media sites espouse these values" (p. 500)

A respondent for this study also noted:

> "I am pretty careful with my identity. But, sometime there is a mismatch between how I want to protect myself and the options that a given site provides. I have many a time "walked away" from a site just because I was uncomfortable with how they thought of my identity and how they aspired to protect it."

Another respondent noted:

> "Protection of my identity is important to me. I am always concerned of the scams and spams that we receive and somehow giving up vital information. For this reason, I try not to sign up for receiving emails or for sites that I am uncomfortable with."

An underlying assertion in our interviews and as evidenced in the above statements is that while people understand the necessity of providing information, they are uncomfortable and troubled by the ill effects. Such ill effects may range from cyberstalking and cyberbullying to identity theft. Many of these outcomes are because of lack of controls and ethical standards that the platform and the social media companies should have in place. As Angin et al (2010) argue that there is a strong need for a strong and an efficient privacy-preserving mechanism.

**Maximize awareness of platform functionality**

Developing awareness of platform functionality and an understanding of how technology works ensures that individuals will have less negative feelings. This assertion has been made by many scholars over the years, particularly Bandura (1986) and his theoretical assertions in Social Cognitive Theory. As noted in our literature review, there are two conceptions of privacy

– privacy of personal sphere and privacy of personal data. In the context of privacy of personal sphere, privacy is understood as solitude and non-intrusion. In that sense, privacy refers to an individual's thoughts, properties and actions remaining secret. Such a conceptualization was afforded by Warren and Brandeis (1890). Privacy of personal data on the other hand refers to "the right to select what personal information about me is known to what people" (Westin, 1967). This conceptualization stresses an element of control. If we are to take these two perspectives and make individuals aware, then we would in many way be achieving this fundamental objective. As Pötzsch (2009) notes:

> "Taking into account the two views on privacy presented above, privacy awareness
>
> of an individual encompasses the attention, perception and cognition of:
>
> - *whether* others receive or have received personal information about him/her,
>
>  his/her presence and activities,
>
> - *which* personal information others receive or have received in detail,
> - *how* these pieces of information are or may be processed and used, and
> - *what amount* of information about the presence and activities of others might reach and/or interrupt the individual" (p. 228).

During our interviews several respondents explicitly stated that if there was increased transparency of how their data was used and if they were aware of the process, they would be more willing to share the information. One respondent noted:

> "My wish is the platform provided me with more information as to what they do with my data, where it is stored and what impact it has on me individually. There are so many unknowns in the process and this is perhaps the reason why the level of trust in service providers is low."

Another respondent said:

> "The more I am aware of how a given platform handles my information, the more confidence I will have in not only providing information but also in the platform as such."

As is evident, various platforms have historically not provided much information about the technology, their platform, and data handling practices. This has caused some frustration and unease amongst users. While there is an argument that platforms will not disclose their practices because of loss of competitive advantage, but there is a fine line between staying ahead, privacy and keeping the customers happy.

**Ensure personal data does not change**

One of the primary considerations in *data integrity* is the notion of "discipline-crossing foundation of credible science" (Kleppner et al, 2009). The term integrity implies the notion of "trust," "fitness of use," and "consensual understanding." In our context GenZ do have a desire to maintain all the characteristics of integrity in their dealings with various platforms. One respondent, for instance noted:

> I am really troubled because every time I interact with Snapchat or Instagram, I implicitly feel that I don't trust the platform. I don't think that my understanding of trust and fairness of use of my data and that of Snapchat is the same. A part of me feels that these platforms take advantage of us because they provide a free service. If the model would have been similar to newspapers where revenue is generated through subscriotions and advertising, I would be okay. Not the new media has crossed all ethical limits of advertising and personal data use.

As Lagoze (2014) notes:

> "Taking a cue from archival science then, we should look at the role of *control* (and *unbroken provenance*) as a necessary (but not necessarily sufficient) factor in data integrity. Traditional data origination, sharing, and reuse were based on the reality of containable and concrete physical data (e.g. written by hand or stored on magnetic devices that are kept in drawers or file cabinets) and data sharing practices based on physical handoff to known colleagues. The physicality of both the data and the transfer of data amounted to a well-defined *control zone* resulting in a provenance chain that was documented and witnessed" (p. 6).

The concern we are witnessing with the proliferation of various platforms and services is that Lagoze's *control zone* and its boundaries have vanished. From a user's perspective a better understanding of the online provider's technology infrastructure allows them to be proactive in protecting their information on their end. One of our respondents noted:

> "I am always concerned about my identifiable information getting changed because there is no clarity in how the Facebook manages my data, how they combine it with other sources and publicly available data."

Another respondent resonated with the opinion to note:

> "I believe providers should clearly communicate the mechanism and transformations they use. While the services may be free, but it is my data."

The concerns expressed by the respondents are symptomatic of a bigger problem – trust of user in how their data is managed and its integrity. The concerns with data integrity certainly deserve more attention. Kennedy, Elgesem and Miguel (2017), put it very succinctly when they say:

> "…we found that a number of factors influence how users view social media data mining and thus throw some light on the variation that can be seen when quantitative studies in related fields are considered together. Characteristics such as age, nationality, occupation, extent of social media use and prior knowledge of social media data mining seemed to play a role, given the differences among participants that we identified. The type of data tracked and gathered, the purpose of the monitoring activity, the extent to which social media activity and data gathered are perceived to be public or private, and views about transparency and informed consent also appeared to inform participants' responses. We argue that there is an urgent need to acknowledge this variation because to date, there has not been sufficient differentiation of social media data mining practices in theorizations of them, which have tended to highlight their similarities rather than their differences" (p. 285).

A summary of fundamental objectives is presented in table 5.2.

*Table 5.2 Fundamental Objectives*

| ***Fundamental Objectives*** |
|---|
| ***Overall Objective: Maximize GenZ Online Privacy*** |
| **1. Increase trust in online interactions** |
| Ensure transparency in what information is collected |
| Maximize use of guarantees in information exchange |
| Ensure reputation scores are accessible |
| Maximize use of platforms that have existed for a while |
| **2. Maximize responsibility of data custodians** |
| Ensure people have responsibility for protecting personal data |
| Ensure people have accountability for protecting personal data |
| Maximize integrity of data custodians |
| **3. Maximize right to be left alone** |
| Maximize efforts to preserve individual privacy |
| Ensure that service providers follow privacy laws |
| Maximize uniformity of privacy laws. |
| Maximize control over personal information |
| **4. Maximize individual ability to manage privacy controls** |
| Maximize my ability to control my own information |
| Maximize democratization of privacy controls |
| Ensure clarity of where personal information is stored |
| Maximize individual control of identity |
| Maximize protection of my personal identity |
| **5. Maximize awareness of platform functionality** |
| Ensure users are aware of platform functionality |
| Maximize awareness of how data flows in the platform |
| Maximize clarity of how different aspects of the platform come together |
| **6. Ensure that personal data does not change** |
| Maximize use of encryption technologies |
| Maximize use of new cryptographic advances |
| Maximize use of blockchains |

## 5.3 Means Objectives for Ensuring Online Privacy

In this section we present a discussion of the 16 means objectives that help in achieving the fundamental privacy objectives of GenZ.

### Maximize security of data transfers

Security of data that moves between a platform and those using the service is essential. At some point in time this data will traverse the Internet and is subject to loss or compromise. One of the respondents for this study noted:

> "Online providers should follow a strct protocol to protect the data, particularly when it traverses from their systems to the user."

It is now common practice to encrypt data in transit. But many a times even these simple steps are not taken. One of the most prominent security breaches where the company failed to encrypt the data was Anthem. The *Wall Street Journal* reported[9]:

> The risks became clear last week, when Anthem discovered that hackers had broken into the database and made off with information on tens of millions of consumers, likely making it the largest computer breach disclosed by a health-care company.
>
> Because the data wasn't encrypted, it would be easily readable by hackers. The company believes a hacker group used a stolen employee password to access the database.
>
> That storage decision has made the country's second-largest health insurer the latest poster child for a continuing debate in executive suites: Is turning a corporate network into an electronic Fort Knox worth the potential cost?

Our respondents had similar concerns, one noted:

> "Any data that is transmitted between different parties should be encrypted."

Another respondent said:

> "I just home that my data does not get changed or corrupted when it being transmitted."

A challenge in encrypting data and then transmitting poses many challenges, let alone to storing it. In the Anthem case discussed above, the electronic record system, while allowing encryption of data, prevented it from getting queried. This means that the database would have reduced functionality. Such limitations force companies to adopt a method that compromises the confidentiality, integrity and availability of data.

[9] https://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560 Accessed Jan 1, 2021

**Maximize competence of users**

With increased reliance on technology, protection of data and its privacy have become challenging as has the protection of critical infrastructures. (Pearson and Charlesworth, 2009: Dhillon and Kolkowska, 2011). The ambiguousness of devices and cloud computing has added to the complexity. Coupled with this, the rapid changes in technology have created a competence void. As one of the respondents noted:

> "Each time my applications get updated, I just don't know what to expect. It is as if I have relearn some of the things".

The need to build security competence is very succinctly noted by Thomson and von Solms (2006) when they note:

> One of the most significant vulnerabilities in information security, the human factor, is often overlooked in organizations. Accordingly, employees who understand the benefit of protecting the information assets, as well as their roles and responsibilities, and adhere to the correct behavior, could be the strongest link in the information security infrastructure. Therefore, senior management of organizations should ideally want its employees to become Unconsciously Competent in information security practices (p. 14).

Similarly, a review by Tsohou and Holtkamp (2018) found that even in the extant literature there was a gap in the understanding of competencies and the role they played in successfully managing security and privacy. They note:

> Our findings indicate the existence of a research and practice gap: on the one hand, ISP compliance research implies that IS users perform activities that require certain competencies, but on the other hand competency frameworks in various professions do not promote those ISP compliance competencies. IS literature also lacks studies explaining what are the information security competencies that non-IT personnel should acquire (p. 1057).

Pearson and Charlesworth (2009) have also argued that technical solutions cannot just be implemented. These have to be co-designed, which will not only ensure buy-in, but also ensure

accountability. Scholars have argued that the technical tools alone do not solve the problem. Privacy is best ensured if the users are fully in tune with the developments. Unfortunately, social media companies have fallen short of involving the users in their developmental activities. (Dhillon and Kolkowska, 2011).

**Maximize technological standardization**

The rapid evolution of technology and the innovative manner in which organizations have been using it has resulted in a disconnect with standardization and regulation. If a technology is standardized, it can be regulated. Google, for instance, while being a search engine, has back end integration to optimizing advertising revenue, cloud services, etc. It becomes hard to delineate each of the technologies. Similarly, Amazon, which collects significant amount of data and consumer purchasing behavioral data has other allied businesses, which become virtually impossible to segregate. Resent calls by law makers to curtail the power of big tech is not without other emergent challenges. As Zuboff (2019) says, it is easier to manage and regulate one big tech rather than multiple ones in case these are broken up. Various scholars have argued in favor of standards for online computing. In research conducted by Marston et al. (2011) the author notes that online environments raise significant privacy concerns. Hence establishing clear standards and custodianship is extremely important. Marston et al also caution that standardization needs to be in the context of existing laws and regulations. As one of our respondents noted:

> "Online platforms should have some degree of standardization which allow consumers to be aware how their data is being transmitted and transferred."

Several authors have suggested that there should be government-enforced self-regulations. Such an approach is realized through a partnership between the industry and the government. There are many instances where such partnerships have been useful (e.g. see some of the debates and concerns in Bowie and Jamal, 2006). During the early days of information security

standardization, such a partnership was established in the UK, which resulted in a best practice information security guide. The then Department of Trade and Industry took the guidelines and working with the British Standards Institute, established the BS7799 standard.

**Ensure vulnerability management is effective**

While most systems have built in mechanisms that ensure that vulnerabilities are minimal, it is even more important in the case of social media. Any vulnerability in a platform has the chance of millions of records getting exploited. Platforms and service providers typically look at Annualized Loss Expectancy as a measure of risk. While this may work in most cases, but from a consumer perspective it is not entirely correct. In 2012 a LinkedIn breach exposed 6.5 million hashed passwords and impacted 117 million accounts. LinkedIn's response was to force password resets. Cory Scott wrote on the company blogpost:

> "Yesterday, we became aware of an additional set of data that had just been released that claims to be email and hashed password combinations of more than 100 million LinkedIn members from that same theft in 2012."

Our respondents are equally concerned of such breaches. As one respondent noted:

> "I am generally okay with sharing things on Instagram, Snapchat and other platforms. Sometimes I wonder though what if there were a breach. And criminals had access to my photos and somehow figured out who I was."

**Maximize effectiveness of practices**

Online users of platforms should be kept informed of all privacy policies and practices. A study by Gartner Group found that any time 50% of the companies revise their privacy policy in light of changing regulation, changing business practices, etc. While many of the changes get communicated to the users, there are many a times when they are not. Subashini and Kavitha (2010) have argued that from an individual perspective, risks to privacy depends on the policies established by the online provider. In order for the policies to be effective, however,

as Pearson and Benameur (2010) notes, there should be combination of rules established in privacy policies and some contractual elements that bring about accountability. One of the main reasons why individuals get exposed to privacy threats is because of lack of comprehension of the policy, or the shear fact that they did not read it.

As Cranor (2003) has noted, the manner in which privacy policies are written, they are cumbersome to read and comprehend. In most cases college level education is required, particularly in terms of reading skills. Cranor also found that consumers get frustrated when companies change the policies ever so often. One of respondents noted:

> "In my opinion the privacy policies pop up at the wrong time – just when you are trying to do something important. It forces me to just accept it. And it is so difficult to read all the legal stuff."

While good policies are important for establishing practices for data collection and storage (Karjoth, Schunter and Waidner, 2002), it is equally important for companies to provide proper access to the data. A clear and comprehendible statement of the polices will increase the confidence and trust of the users in a given platform.

**Maximize independent oversight**

When a third party verifies that the privacy practices of an organization are adequate, we refer to it as an independent oversight. Independent oversight also helps in building trust and transparency. During the early days of eCommerce, such trust was gained through the use of web assurance seals. Moores and Dhillon (2003) note:

> The relative success of the privacy seals suggests that many sites recognize the issue of privacy and strive to uphold the highest standards. These sites are not the problem. The problem is with those sites that violate their stated obligations, those sites that make no commitment, and those sites that actively seek to exploit the data they collect. With each new case of fraud that hits the headlines, the perception by online consumers will continue to be that Internet thieves lurk in the shadows of cyberspace, widening the trust gap and

constraining the legitimate commerce being carried out online. As such, it seems to be in the interest of all concerned that legislation is enacted to define the basic principles of data privacy (p. 271).

Our respondents also had a similar view, as one noted:

"I wish there was a way of figuring out that the service provider has some oversight and ensured that all privacy controls were in place. We need to have a system similar to consumer credit ratings."

There is no doubt that the need for an independent oversight is critical. While researchers have echoed the need (e.g., see Wang et al. 2010), other scholars such as Probst et al. (2012) have made calls for setting up an agency such as a "public penetration-testing agency," which will help in increasing consumer trust.

**Maximize segregation of information**

Segregation of information is not a new concept. It is an age-old practice to ensure that integrity of the data and processes is maintained. Smith (1993) had identified errors as a primary cause of privacy concern. This early call by Smith had led many scholars to suggest that separating data in different databases would help in not only reducing errors but also ensure privacy. With increased reliance on cloud computing, the importance of data segregation has reemerged. A study by Gartner Group found that data segregation was among the top ten privacy concerns[10]. One of our respondents touched upon this aspect when he noted:

"It feel it is important to segregate information. I feel that my personal information should be separated from family, friends, academic, professional and so on."

Another respondent said:

[10] https://www.gartner.com/en/documents/3393518

> "I want my personal information to be compartmentalized. It should only be available to me and I should have the authority to present it the way I want."

While online system typically is built around the concept of multi-tenancy, particularly in a cloud setting (this is when many users can store data in the same location). However, public infrastructures are typically not designed to ensure proper segregation and compartmentalization. The infrastructure is also prone to several vulnerabilities that can increase the chances of a privacy breach. It is therefore producent to invest resources in data segregation practices and thereby increase the confidence of consumers.

**Minimize Individual Liability**

Any user of online platform needs to be cognizant of legal and regulatory risks associated with the use of services. Cloud providers and for that matter most of the social media service providers pool resources and use shared infrastructure, which typically results in process and store data. A significant concern is where the data resides. It is virtually impossible to determine the jurisdictional boundaries and the applicable laws. The uncertainty about the location calls into question the jurisdictional concerns and how privacy is handled (Sotto et al., 2010). As one of the respondents noted:

> "One time I thought my facebook account had been compromised. I contacted Facebook but had no clue where my data would be and who I should reach out to. I don't live in the US, and no number to call."

The concern for online data storage is not specific to the U.S. alone. It is equally relevant in Europe. The new GDPR limits where and how personal data is stored and how it is transmitted. Individuals however are not conversant and aware of all the laws and regulations and how they need to protect themselves.

**Minimize accessibility of online resources**

One of the major concerns in privacy is improper access (Smith et al., 1996). We need to ensure that an individual's personal information remain protected. Research has found that nearly 85 percent of surveyed adults thought it was extremely important to control access to personal information (Madden et al. 2007). While technologically it has been debated as to how access to information should be granted, it is also organizationally important to define constraints around how access is granted to information (Smith et al., 1996). Respondents in our study echoed these concerns, as is noted here:

> "I want clarity as to who has access to my data, who can change it, who can use it and who can sell it. If someone is going to make money from my data, then I need to know."

> "I want to have the ability to control my information. Rather than the platform giving access, I want that control."

Scholars have identified ways and means that allow for inappropriate and unauthorized access to be granted (Pearson and Charelesworth, 2009). As (Kaufman, 2009) has argued, stringent access control practices must be enforced. Leavitt (2009) has suggested audits of capabilities so as to demonstrate access to data. It can therefore be suggested that limiting access to data is desirable and a necessary condition for success of privacy controls.

**Optimize online technology use**

Ease of use as a concept has been well researched in the literature (e.g. see Rogers, 1995; Eriksson et al, 2005; Venkatesh and Davis, 1996; Venkatesh and Morris, 2000; Hernandez and Mazzon, 2007). Ease of use is defined as an understanding of the technology that leads to adoption. Ease of use and security are often considered opposite sides of the same coin. As Dhillon et al. (2016) notes:

> "Bruce Schneier's cynical slogan, "The more secure you make something, the less usable it becomes" sums up the current state of security and usability. As we make systems more secure, genuine users try and find hacks and work around, which result in compromising security. Research in information security and usability has recognized this problem, however, not much has been accomplished, largely because of two reasons. First, the requirement for security and usability of systems has always been considered as an afterthought. Two, security and usability issues have not been considered strategically and integrated into the strategic plans for developing systems. These two reasons have resulted in systems that are often not aligned in terms of security and usability. Therefore, the need is to identify objectives for both security and usability, collectively, that will help with proactively balancing security and usability" (p.656).

One of our respondents noted:

> "I would like to remove old information easily. The platforms do not provide any easy way to do so."

Stronger privacy can only be there if the controls are balanced in terms of ease of use and usability. In order to facilitate stronger privacy controls for the ease of use technology, it is best to develop privacy-enhancing tools, which can be easily adopted by online users.

**Minimize unnecessary access**

Unnecessary access to information has long been a challenge. Over the years various models have been proposed. As Lu et al (2015) describe:

> "As opposed to the permission-based access control mechanism, which assigns permissions required to perform tasks to users directly, the role-based access control (RBAC) mechanism defines a role set by associating permissions to roles and then assigns roles, rather than a number of permissions, to users. RBAC has been regarded as a de facto access control model. Its many advantages include the convenience of authorization allocation and the reduction of the system administrative workload. To benefit from those advantages, enterprises still employing their old access control systems need to migrate to RBAC. To accomplish the migration, the first phase is to define a good role set. While the role defining problem is seemingly straightforward, it has been recognized as one of the costliest phases in the implementation of

RBAC and poses a great challenge to the system engineers. The difficulty comes from the fact that a RBAC system engineer usually has little knowledge on the semantic meanings of user responsibilities and business processes within an enterprise" (p. 107).

A similar frustration was expressed by one of the respondents, who while acknowledging the the cost issues, notes:

"I am concerned how the online platforms define roles and responsibilities of the consumers. All consumers are bundled into one stakeholder group. They need to be a little more granular than that and link the roles with business activities."

As Sandhu & Samarti (1996) have argued, optimization of tools that authenticate and manage access and audit are the foundation for protecting personal data. Identity of one party to the other is established through the authentication process. To ensure proper access, verification is important. There are four main authentication methods. Idrus et al (2013) summarize the authentication methods and added a fifth one to the list:

"1. Something the user knows: a password, a passphrase, a PIN code, the mother's maiden name. . .

2. Something the user owns: a USB token, a phone, a smartcard, a software token, a navigator cookie. . .

3. Something that qualifies the user: a fingerprint, DNA fragment, voice pattern, hand geometry. . .

4. Something the user can do: a signature, a gesture. . .

But now, perhaps we could include a 'fifth' authentication factor:

5. Somewhere the user is: a current location/position, a current time information. . . "

**Ensure privacy policy governance**

Policy governance came into prominence following the Enron fiasco and the passing of the Sarbanes Oxley law. There are significant failures and businesses suffer losses because of data loss. And more often than not, consumers are put at direct risk. In an ICIS 2010 panel discussion (see Gillon et al (2011), one of the panelists noted:

> "Dhillon suggested that the success of governance measures and laws depended on the specific context and contrasted two scenarios which had seen very different results due to the solidity of underlying principles. On the one hand, there were state-level security and privacy policies that were based on ill-conceived standards, leading to weak foundations and inability of the agencies to comply. On the other hand there were instances of well grounded policies, particularly in the Las Vegas Casino industry, thus making positive strides in anti-money laundering efforts. Dhillon noted that it really boils down to how well conceived a given set of governance measures is and how well the measures reflect the ground realities" (p. 565).

In a similar vein, one of our respondents said:

> "I think there is a disconnect between what the governance laws are and how these are implemented."

Nissenbaum (2004) has termed this problem as "contextual integrity." Nissenbaum argues that privacy is a function of appropriate flow of information, which conform to the prevalent norms. The contextual norms relate to the data subject, senser, recipient, information type and transmission principle. When dealing with governance issues all contextual norm issues need to be evaluated and appropriately managed.

**Minimize information disclosure**

There is a concern among individuals as to how control over information should be established. Following the classic definition of Westen (1967), the ability to self-select as to when, how and with whom the information is communicated forms the basis of information disclosure practices. In an extensive literature review Kolotylo-Kulkarni et al (2021) note:

> "Our findings also inform consumers about the mechanisms they undertake when choosing to share their private information and different means that merchants adopt to influence them to do so, potentially assisting them in making more educated and carefully considered decisions. It also cautions consumers on how their decisions to disclose their personal information can contribute to their spending. Unless online platforms are designed to support informed choices, consumers must be aware of their limitations and the possible impact of online tools" (p. 235).

Our respondents had a similar view and resonated with what has been noted in the literature. As one of them noted:

> "Prior to signing up on a platform, I would like to know what the platforms historical position has been? How often have they been hacked? What their practices are for information disclosure? These are important isses that require consideration."

The threat of information disclosure is real. An evaluation of risks of personal information is essential and exposure should be limited. Under all circumstance, users should have a choice as to their information is collected, used and disclosed. In essence, users need to give consent. Moreover, personal information should only be stored for limited period of time determined by necessary and sufficiency conditions.

**Minimize government access to personal information**

The topic of government access to personal information has been a topic of significant discussion. May this have been in light of the breaches or in terms of the surveillance. The ongoing debate related to supercookies (aka the surveillance state) is interesting. As Connor and Doan (2021) argue:

> "Our findings suggest that the public and media companies do not deem supercookies as important or interesting as government surveillance of citizens and foreign countries. If media organizations and the public find this topic less interesting, then to some degree they may not find it as offensive to their values. It may not offend the democratic code and it may be normalized in the economic sphere, where the democratic code

> is not hegemonic. The media discourse that was present was much less critical in terms of their characterization of Verizon. There were relatively few narratives placing Verizon as a serious antagonist that threatens the democratic code. Instead, many outlets criticized them in what amounts to a public wrist slapping. Verizon violated customers' privacy rights, but they paid a fine and made the policy opt-in. These actions more or less quelled strongly negative discourse on Verizon's use of supercookies. It can be argued that the public was less critical of Verizon because they did not perceive them as significantly threatening sacred codes of the economic sphere" (p. 64).

While the authors use the example of Verizon, the problem and the concern persist. As one of the respondents noted, they are concerned, at times of posting their opinion online, for the fear of being victimized by the government. This can be a real concern if there is a situation of a "big brother watching over you." A respondent noted:

> "I am always concerned with my online posts. My dad got into trouble in his youth when he expressed opinions in favor of the protests in India. It cost him his job. What I have learned is that the State is always watching you!"

**Minimize third-party access to personal information**

The very core of the definition of information privacy is the limiting of access to personal information, particularly for third parties. In the literature, personal information privacy is defined as an ability of a person to control information about themselves (see Stone, et al, 1983; Milburg, Burke, and Smith, 1995). Respondents in our study explicitly expressed their desire of not sharing personal information with third party vendors. As one respondent noted:

> "I do not want online providers to disclose my information to third parties. I need to know who is given this access."

While the prevalent business model encourages sharing of information with third parties, which generates subsequent traffic to the websites, the consumers think otherwise (Dhillon and

Kolkowska, 2011). In many ways consumers feel that they are being used for someone else to profit from their information.

**Maximize awareness of data ownership**

Where the data resides (data residency) and who owns the data (data ownership) is an evolving concept. However, with the distributed and ubiquitous nature of computing, it brought a new meaning to data residency and data ownership (Marston et al., 2011). When the data has been shared online or shared on a public forum, there is much debate as to who owns the data. While some may argue that the data is owned by the company where it is stored, others argue that is still owned by the individual who placed it there in the first place. As Katzan (2010) has argued, it is important to evaluate the data ownership issue prior to an organization venturing into an online presence. One of our respondents noted:

> "I think users should have control of their data and if someone else is going to use it, then there should be proper accountability structures."

Another respondent said:

> "I wish I had control over my data."

As Hoffman et al. (1997) note, first step to establishing data ownership structures and trust is the recognition that there is a need to do so. Any online privacy is a function of the level of trust that an individual has in the service provider. Trust comes about through the balance of power shifting towards more cooperative processes (Hoffman and Novak, 1997). As part of the cooperation is the process of opt-in and opt-out that needs clarification.

In this section we have presented the details of all the means objectives. A summary of these is presented in table 5.3.

*Table 5.3 Means Objective*

| ***Means Objectives*** |
|---|
| **1. Maximize security of data transfer** |
| Maximize end to end security of user experience |
| Maximize security of services provided on the platform |
| Maximize compartmentalization of data |
| **2. Maximize competence of users** |
| Maximize availability of privacy protection training |
| Minimize reliance on automated warning |
| Maximize reliance on Artificial Intelligence to ensure privacy protection |
| **3. Maximize technological standardization** |
| Ensure all engagement technologies are standardized across platforms |
| Ensure data exchange protocols are standardized |
| Ensure latest standards are effectively communicated to users |
| **4. Ensure vulnerability management is effective** |
| Ensure that platform risk management is undertaken regularly |
| Ensure that vulnerabilities are effectively made known |
| Ensure users are aware of the vulnerabilities |
| Maximize efforts to communicate vulnerabilities with users |
| **5 Maximize effectiveness of practices** |
| Maximize security/privacy of employee training |
| Ensure employees are conversant with privacy challenges |
| Maximize awareness of laws and regulations |
| Maximize compliance with regulations |
| **6. Maximize independent oversight** |
| Maximize technical audit of platform |
| Maximize privacy audit of platform |
| Ensure vulnerability audit is conducted on a regular basis |
| **7. Maximize segregation of information** |
| Maximize segregation into specific identity groups |
| Maximize compartmentalization of personal information |
| Ensure confidential information is segregated |
| Maximize confidentiality of personal information |
| **8. Minimize individual liability** |
| Ensure that individuals are not held responsible for loss of data |
| Maximize protection from litigations |
| Minimize individual harm because of mistakes by the platform |
| Minimize legal responsibility and risk |
| **9. Minimize accessibility of online resources** |
| Maximize accessibility of personal information |
| Maximize availability of personal information as required |
| Minimize down time of online platforms |
| Maximize reliability of platforms |
| Maximize offline availability of personal information stored online |
| **10. Optimize online technology use** |
| Maximize convenience of online access to personal information |
| Minimize difficulty in use of online platforms |
| Minimize use of multiple platforms and complexity |
| **11. Minimize unnecessary access** |
| Maximize control over who has access to personal information |
| Ensure individual profile monitoring is in place |
| Maximize ability to provide authorizations to others |
| Ensure a balance between opt-in and opt-out |
| **12. Ensure privacy policy governance** |
| Maximize control over who has access to personal information |
| Ensure individual profile monitoring is in place |
| Maximize ability to provide authorizations to others |

| | |
|---|---|
| | Ensure a balance between opt-in and opt-out |
| **13.** | **Minimize information disclosure** |
| | Minimize information collection |
| | Minimize individual identification |
| | Maximize communication of security and privacy breaches |
| | Increase ability to manage personal information |
| **14.** | **Minimize government access to personal information** |
| | Minimize government access to personal information |
| | Minimize government ability to seize personal information |
| | Minimize government surveillance |
| **15.** | **Minimize third-party access to personal information** |
| | Minimize sharing of personal information with third parties |
| | Minimize collection of information by platform providers |
| | Minimize third-party access to personal information |
| **16.** | **Maximize awareness of data ownership** |
| | Maximize clarity of data ownership |
| | Maximize clarity of intellectual property rights |
| | Ensure responsibility of data owners |
| | Ensure accountability of data owners |

## 5.4 Conclusion

It is important to evaluate the fundamental and means objectives we have identified in this study to ensure their validity. As described in chapter 3 we utilized experts to validate the objectives for ensuring privacy as recommended by Dhillon and Torkzadeh (2006). An audit team that consisted of 6 individuals with an expertise in auditing information systems performed the evaluation process. These experts were utilized to evaluate the validity of the ensuing objectives. They reviewed the 22 identified privacy objectives (6 Fundamental and 16 Means objectives) during the data analysis of VFT phase of this study. Each member of the audit team reviewed the 22 main objectives and the clusters of sub-objectives individually to determine if they considered them to be valid objectives for ensuring privacy in online computing. During this process, they also evaluated the relationship between each main objective and its corresponding sub-objectives and determined if they were accurately grouped together in their professional opinion. Once each member had reviewed the objectives, we had a focus group meeting, and they shared their opinions on the validity of the objectives. After this discussion, the group decided one objective, “Maximize awareness of data ownership,” initially classified as a fundamental objective should be classified as a means objective. Also,

the group determined that the following two additional objectives needed to be included in the list of means objectives, “Minimize information disclosure” and “Ensure privacy policy governance.” This resulted in a total of 22 main objectives being identified, 6 fundamental objectives and 16 means objectives.

This chapter has presented the fundamental and means objectives that ensure privacy on online platforms. The study presents a unique and a thorough presentation of Value Focused Thinking as originally presented by Keeney (1992). The objectives for privacy in online computing were derived from a large number of interviews with a wide range of personal experience in online interactions. We discussed in detail the process of how we performed the analysis of the rich data resulting from the interviews in this study. The results of the analysis are presented in tables 5.2 and 5.3 that resulted in 6 fundamental and 19 means objectives. We provided a detailed discussion on the relevance of the objectives as per the extant literature. Our discussion also establishes the relevance of the overall aim of ensuring online privacy.

# 6

# Discussion of Online Privacy, Individual Values and Implications

## 6.1 Understanding values

Values are, rarely, perfectly aligned with behavior. Fundamentally, values have been found to guide behavior and can be breached to move from one value to another (Kennedy et al. 2009). Consumers can have many beliefs about sustainability issues concerning subjects from recycling and reuse of products to electric consumption reductions. Other beliefs may center on environmental benefits that result from shifting demand against the value of feeling cooler and turning down thermostats on hot summer afternoons. Overall, value represents those things which individuals or groups deem important (Burrows et al. 2014) and can be starkly different

from beliefs. Values can be self-chosen or imparted from family, be circumstance driven (in which justification for specific decisions are sought), or may be a combination of both. Coughlan (2005) developed and initiated codes surrounding value systems where justification by individuals (namely employees) were sought based on choices and decisions.

Normative structures of organizational codes of ethics were found to be a basis for justification when individuals reacted to certain beliefs and could be most useful when clear, comprehensive and enforceable actions were taken which either upheld or differed from one individual's value system (Coughlan 2005; Raiborn and Payne 1990). Once enforceable actions are codified, and justification maintained, normative structures can shape individual values and beliefs. Developing information systems to provide enforceable actions based on individual values allow for the development of value-based alternatives and long-salting sustainable action.

Various stakeholders within information systems embody a range of social and organizational value factors (Tan and Hunter 2002). Social and organizational norms can shape and influence an individual's value assumptions pertaining to normative structures (Dhillon and Torkzadeh 2006; Orlikowski and Gash 1994). Four normative structures that can be utilized to shape individual values include: justice, competence, integrity, and utility (Coughlan 2005; Raiborn and Payne 1990). Each structure can be utilized through organizations to define organizational codes and shape individual values of those who work or operate within the corporate system. Justice concerns interpersonal dealings and an individual's consideration of others, competence signals the maintenance of high personal standards, integrity is the consistent use to values based on moral principles such as honesty, sincerity, and candor, while utility accounts for the utilitarian ethical framework which considers consequences based on outcomes (Coughlan 2005; Raiborn and Payne 1990). Kennedy et al. (2009) moved beyond organizational constraints to more personal social systems of normative structures to

investigate environmental values. Cost of enacting sustainable measures, support from family members, time investments, decision control about sustainable policies and the accessibility to recycling and reuse program were found to help shape individual value systems.

Individuals have central values, which can be delivered from biologic sources, cultural patterns, and social preferences to available alternatives for decision making. Micro and Macro alternatives have been identified, which provide individuals with value systems to make decisions (macro) or meet overall individual objectives (micro). Rokeach (1973) indicated social decisions based on 'macro' alternatives concerned values created by governments or socialized enterprises. Values of objects or outcomes are stipulated by the macro environment and include such things as paychecks and/or tax incentives, and are associated with the expectancy model of motivation (Vroom 1964). Decisions based on a specific social end are associated with 'micro' alternatives and can be associated with descriptive states of individuals consisting of instrumental and terminal values. Terminal values are self-sufficient "end-states of existence" in which a person attempts to achieve (Rokeach 1973) and can be associated with individual motivations for sustainable actions or cost reductions related to selfish actions. Instrumental values are specific modes of behavior coupled to central or core values of individuals that are difficult to alter or modify and allow for terminal values to become established.

How the macro and micro alternatives compare is a naturally occurring process for individuals, and allows for investigations of alternative activities (Rokeach and Ball-Rokeach 1989). Individual ethics and justifications for making specific decisions, can present difficulty when individuals attempt to identify true value preferences (Meglino et al. 1989). Decision structures of this nature become equal and are difficult for individuals to differentiate between alternatives and make value-based choices. "Enlightened self-interest" assumes all individuals have similar social objectives (Arrow et al. 1996; Keim 1978) however, differences of opinion

arise on social issues from information asymmetries and a general lack of knowledge about social outcomes. The means of meeting the ultimate values of individuals, and exactly which ultimate value choice alternatives have dependence to certain combinations of macro and micro preferences, can become dependent on if too little or too much information (or too many choices) is conveyed to the individual. How social decisions and social ends are manipulated and coupled with available knowledge and self-interest is relatable to individual generation and determination of value-based objectives and their means.

## 6.2 Theoretical Framing and Implications

The Theory of Action was developed to implement change from individual or organizational viewpoints and provides the basis which can lead to long-term goal setting such as environmental sustainable actions (Coleman 1986). Parsons and Shils (1951) and Warner (1978) describes individual actors who make choices to achieve a means of action which are limited by objective conditions and governed by culture (normative structure). Parsons and Shils (1951) define values as "an element of a shared symbolic system which serves as a criterion or standard for selection among the alternatives of orientation which are intrinsically open in a situation" which leads to an overall value orientation. Culture affects human action through values (not beliefs) and generally direct decisions on one social end over another.

Coleman (1986) describes the ability to enact change as requiring a social action on the ability to act but as an active participant in the action. This requires individuals to make transitions between macro and micro alternatives into an overall system of action to reach some mean associated with core values. Additionally, Coleman (1986) associated the Theory of Action to economic utility functions where values of individuals could be identified as courses of action where selfish actors attempt to maximize their own utility and benefit. This is in contrast to social science where action analysis is measured to affect changes in behavior.

Overall, this theory allows for utility of individuals to affect values among identified alternatives.

Therefore, the system of action can then be utilized to link individual action (micro actions) to macro level influences such as social norms or information asymmetries (or overload) to identify values of individuals within specific cultures and normative structures to move beyond a limited belief system and base substantive action for sustainable outcomes on core values.

Overall, many decisions begin with identification of alternatives or to develop strategies to reach our objectives (Keeney 1992). Keeney (1992, p.1) believes this is counterproductive to what is in the best interests of decision makers stating, "values are more fundamental to a decision situation than are alternatives." With that in mind, values, then, should be the first step in determining what decision will be made and not be 'boxed in' by the limited alternatives known and describes this methodology as value-focused thinking. Once you have internalized the values associated with a decision, only then should alternatives be analyzed to reach desired objectives. Keeney (1992) also believes value is associated with "ethics, desired traits, characteristics of consequences that matter, guidelines for action, priorities, value trade-offs, or attitudes for risk."

Application of value-based thinking is not universal and can be operationalized through various means which are not always equal. Merrick and Garcia (2004) utilize a multi-objective decision analysis (MODA) framework which provides an intentionally logical process for making decisions by applying value-focused thinking principles, which can "including the direct benefit of creating better alternatives." Where some approaches to make better decisions involving multiple stakeholders can take an adversarial approach where stakeholders defend their own positions which leads to a lack of trust and implementation of identified solutions, MODA models can turn the discussion from defensive to collaborative analysis (Merrick and Garcia, 2004). Five stages have been developed for MODA models and include: 1) Defining

overall objectives 2) Defining fundamental objectives through hierarchy lists (as opposed to means objectives) 3) Choosing how to evaluate measures of achievement for the lowest level objectives 4) Transforming those evaluations into units of value and 5) Weighing the objectives to reflect the value to the overall decision maker. MODA models can be used to generate and evaluate alternatives, indicate gaps where improvement will have the greatest effect, and build alternatives around those needs. In the case of social media and artificial agents, this method will allow investigations that identify and organize values associated with individuals when targeted with misinformation, and how that targeting originated through third-party information dissemination.

Quantitative and qualitative value modeling can be applied to determine how decisions are attacked through problem definition and requirements of the system. Systems analysts create both quantitative and qualitative models to select possible paths after the selection of a possible decision from among the created outcomes of each choice. (Lee 2004) does not specifically talk to this setup, but generally describes a similar situation as a process where an "emergent result of the mutually and iteratively transformational interactions among the social system, the technical system and the knowledge system." Qualitative value models have been regarded as more important than quantitative models because of the reflection of key stakeholder values when examining the decision system (Parnell et al. 2011). Value measures provide a weight to rate alternatives against the ideal system desired, where initial functional analysis assign objectives and measures the overall model. Quantitative value models are then turned into qualitative models to identify how well identified solutions to the problem meet what the stakeholder desires. See figure 6.1 for our conceptualization.

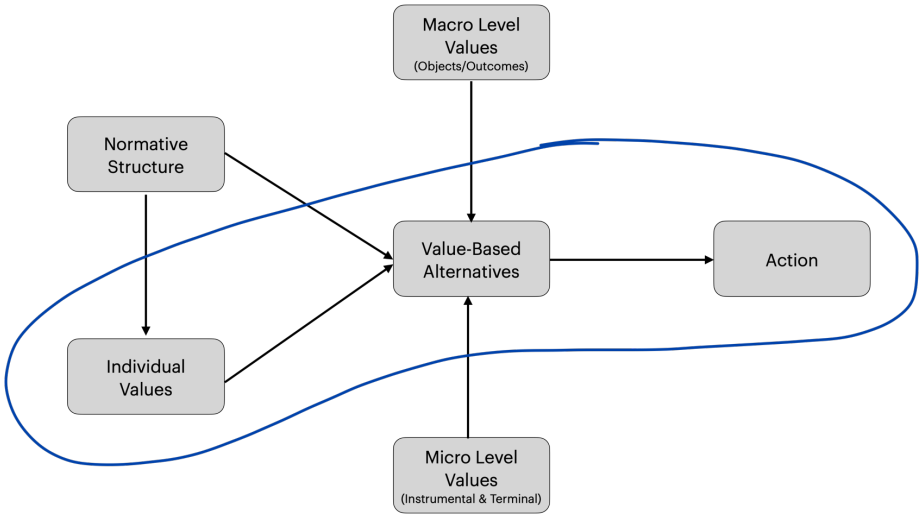


*Figure 6.1, Overall view of how information privacy objectives for GenZ are shaped*

## 6.3 Information Privacy Values

Most of the research and discussion in IS privacy has been focused on finding out the immediate reasons which lead to the erosion of privacy in the age of information technologies and what to do to protect and conserve the privacy. Less attention has been directed toward the fundamental question of what the values are underneath that privacy. Furthermore, out of all the theories adopted, IS privacy researchers fail to address the issue from decision theory and value-focused thinking perspective. Based on value-focused thinking, this section addresses the gaps.

As noted in the literature review chapter, the famous judicial definition of privacy by Warren and Brandeis (1890) is widely regarded as the first publication in the United States to advocate a right to privacy, articulating that right primarily as a "right to be let alone." Since the 1960s, serious interests to define and understand privacy have been developed (Marguilis 1974). Research conducted in the 1970s established the theoretical foundation for privacy. The classic definition of privacy from a legal view is "*the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others*" (Westin 1967).

The basic idea of privacy conveyed in these classical works before and in 70s is that individuals should be allowed to define themselves, and to decide how much of themselves to reveal or to conceal in different situations (Rosen, 2000). These arguments indicate three important aspects of privacy from an individual's perspective. First, privacy is a decision-making process. Second, the definition of privacy reflects the judgement with regard to how people define who they are, a critical question of self-identity on the core value sense of oneself. Third, privacy is context-based. The earliest examination of privacy originates from a behavioral perspective in a work by Georg Simmel in 1906 (Marguilis 1974). According to a literature survey conducted on IS senior basket journal of eight by the author of this essay, research on privacy in the information system discipline started about 2000, rooted in the 1970's legal theoretical foundation, which studies privacy behaviors in information technologies.

IS privacy research in the past two decades has produced fruitful results, indicating the maturity in developing, testing, and citing its own measurements and theory. The majority IS privacy studies are under the umbrella of APCO (Antecedents -> Privacy Concerns -> Outcomes) (Smith et al. 2011), a framework that studies antecedent, moderating/mediating forces, and outcomes (i.e. reveal or conceal personal information, and other privacy protection behaviors). Guided by APCO model, IS privacy research is dedicated to the understanding of the immediate economic, psychological, and social reasons which lead to the privacy erosion.

Despite achievements, there is room for future IS privacy research to improve. The APCO model is largely problem-solving oriented. Each paper and theory in IS privacy research implies but rarely applies decision-making perspective. According to Keeney (1992), the standard problem-solving approach reacts to rising problems. Typically, this approach places the emphasis on problem solving mechanics and tools, and on identifying fixed problem-solving alternatives rather than on the purpose of problem-solving. This is a "symptom control"

problem-solving approach. For example, over-the-counter drugs can be effective on controlling or relieving symptoms for the time being and curing minor illnesses. However, a serious disease requires doctor's diagnosis to understand the pathology for finding proper cures and eradicating the causes of a disease. This essay argues for a holistic "pathology" approach to understand how people make privacy related decisions.

In order to protect privacy, people need to first define what privacy is. As this essay points out at the beginning, one of the important aspects of privacy in classical research is that defining privacy reflects the judgement of people regarding who they are. This is a critical question of self-identity on the core value sense of oneself. Based on the two dominant theories of self: identity theory (Stryker, 1980) and social identity theory (Tajfel 1981; Tajfel and Turner 1979, 1986), Hilton (2003) argues for a personal identity, he defines it as identity that is experienced by individuals as "core" or "unique" to themselves and formed by individuals' value-structures.

The empirical study (Hilton, 2003) proves that values lead to conceptualization of personal identity, which in turn leads to reflexive constructions of various role, group, and social identities. These latter identities are tied more directly and closely into concrete behaviors. Following Hilton's personal identity theory, unique values of each individual decide how a person define himself or herself. This internalized personal identity aids developing other perceived role, group, and social identities which further affect privacy protection behaviors chosen by individuals. However, according to a literature survey conducted by the author of this essay, the value thinking is missing in current IS privacy research.

Privacy protection talks about behaviors, or actions. Behavior is the manifestation of a particular decision-making process. In the last three decades, the field of classical decision theory has witnessed two conceptual shifts which have become mainstream in the 90s with the publication of two corresponding milestone books: "The Adaptive Decision Maker" by Payne et al. (1993) and "Value-Focused Thinking" by Keeney (1992) (Carenini and Poole, 2002).

The first conceptual shift has occurred in the field of behavioral decision making, where a large number of studies have shown that human decision is inherently adaptive and constructive (Carenini and Poole, 2002). Individuals, in their behavioral decision-making process, are adaptive to both the task on which decisions are made and the context in which decision are made.

The assumption is that decision makers have several decision strategies at their disposal. Therefore, when making a decision, decision makers select a strategy depending on a variety of factors related to the task, the context, and individual differences. Studies investigating the contingent nature of decision-making show that individuals often do not possess well-defined preferences on many objects and situations but construct decisions in a highly context dependent fashion during the decision-making process (Carenini and Poole, 2002). This stream of theoretical idea has been reflected in the extant IS privacy research. In 2008, Xu et al. propose formally in their paper that information privacy is dependent on context and also varies with a person's life experiences. Therefore, the third aspect of the basic ideas of privacy is recognized and captured. This is the “good” part in the IS privacy research.

The second conceptual shift in decision theory has occurred in the field of prescriptive decision-making and it is called value-focused thinking (Carenini and Poole, 2002). The prescriptive decision-making focus on how people actually make decisions in practices, assuming that humans may not always be perfectly rational agents. Before discussing about the value-focused thinking prescriptive decision-making, one notion that needs to be pointed out here is the normative (traditional) decision-making. The normative decision makers make decisions based on set of rules and algorithms. In this traditional view, humans calculate decisions with respect to the logic, math, and rationality so that judgment and decision making are the results of rational choices.

The difference between the normative and value-focused thinking lies in the decision-making process. According to Ralph Keeney (1992), the normative decision-making process consists of three steps. The first step is to identify a set of plausible alternatives, the second, to specify the values relevant to evaluate the alternatives, and the last, to apply these values to choose the best alternative. Value-focused thinking turns the decision process upside down. Once a decision problem is recognized, full specification of fundamental and relevant values is the next step. After that, the identified values are used to creatively identify possible alternatives, to carefully assess their desirability, and to make choices. Therefore, value-focused thinking is a proactive approach. As a matter of fact, the alternative-focused thinking is at the center of critique from value-focused thinking.

Dominant IS research is normative decision-making oriented and mainstream IS privacy research model APCO reflects this traditional decision-making conceptualization in privacy protection. Despite that, IS researchers try to model the opportunist (paradox) behaviors by developing risk–benefit privacy calculus theory (Culnan and Bies, 2003), they are keen on empirical testing, modeling, and quantifying the relationship between antecedents and behavioral outcomes of privacy. The striking commonality found in the survey is that more than 80% of articles utilize the structural equation modeling (SEM) analysis. Additionally, 12% take mixed research method approaches including SEM, and only 7% uses interpretive methodologies. The APCO model is the very product of the normative decision-making thinking in IS privacy researchers. Clearly, the current IS privacy research is trapped in positivist methodological approach which hinders the research potential to develop holistic and proactive privacy theories.

## 6.4 Defining information privacy values for GenZ

Value-focused thinking research enables researchers to identify values of constructs of interest as well as determine relationships among these values. It is fundamentally about

deciding what is important and how to achieve it (Sheng et al, 2005). Value-Focused Thinking (VFT) approach can be used to conduct the interviews, where qualitative data is gathered, and to articulate and organize the data from the interviews. VFT is a systematic methodology which enhances the reliability and validity of research results (Sheng et al, 2005). People participating in structured value focused thinking research are typically able to make better informed, more thoughtful and higher quality decisions (Arvai et al, 2001).

Selart and Johansen (2011) assert that VFT in itself is not a sufficient condition for the rich production of solutions or ideas, as has been suggested by Keeney (1992, 1994). They attributed this to decision makers generally not being more effective when using techniques that they have long been accustomed to in their everyday lives. On the other hand, new and unfamiliar methods might require more cognitive effort and result in a lower degree of decision effectiveness and productivity. In the VFT approach, one starts with the best potential outcome and then works to achieve it. This can constrain fun, experimental, explanatory thinking that so often characterizes truly creative thinking (Visscher and Fisscher, 2009). Also, VFT may sometimes be potentially more convergent than divergent to the disadvantage of idea fluency because it imposed greater demands on peoples' information processing capacity (Selart and Johansen, 2011).

Even though values may constrain on ideation fluency, research suggests that they have a positive effect on idea quality. Hence VFT offers a great opportunity, to researchers and practitioners (Girotra, Terwiesch and Ulrich, 2010) to the stimulate high-quality ideas. VFT has a greater potential to trigger creative ideas, however, certain preconditions such as motivation must be met for VFT to realize its potential (León, 1999).

The value of privacy is a question intertwined in philosophy, sociology, psychology, and other perspectives. As the APCO model itself and the variables in the IS studies indicate, despite efforts of IS privacy researchers to include antecedents selected from psychology,

sociology, and economics disciplines to study privacy, they have failed to give the problem a decision-making thinking, and they have missed to address the roots of privacy which represents the values of privacy decision makers.

Following the theoretical perspective of value-focused thinking, this essay argues, while there are many alternatives to solve privacy problems on the sight, understanding the fundamental values of the privacy is the right approach. Addressing the problem at its roots not only help identifying decision opportunities but also assist creating better alternatives.

Although value-focused thinking is overlooked by the mainstream of IS privacy research, it is encouraging to learn that another stream of IS security and privacy research is applying it. In preliminary research regarding artificial intelligence (AI) on preference elicitation, Carenini and Poole (2002) propose and discuss the implications of value-focused thinking in decision-making. Dhillon and Torkzadeh (2006) follows value-focused thinking and elicits and builds a set of constructs (objectives) to comprehend IS security in organizations. Following the same theory, Dhillon et al. (2018) identifies the values attributes of individual privacy in e-commerce and establishes the mean objectives to protect privacy in e-commerce. Smith et al. (2018) uses value-focused thinking to define electronic identity management objectives related to security.

Proven by these exemplar papers, the value-focused thinking is an effective approach to advance IS privacy research in identifying and building theory constructs. For IS research, one of the unique challenges is to define some elusive concepts such as privacy. Different researchers can have different aspects of these concepts, which makes comparisons between studies and knowledge accumulation difficult. Only by equipping with the accurate constructs and measurements, the latter research using positivist methodology can generate meaningful research results. This is the greatest contribution that value-focused thinking can make in the future of IS privacy research.

## 6.5 Delphi Study of GenZ Privacy Concerns

While defining value-based objectives is an important task, it is equally important to operationalize the objectives for strategic decision making – for the companies and policy makers. The problem, however, is that the objectives generated through Value-Focused Thinking are significant in number and hence, difficult to articulate. Therefore, it is important to prioritize and rank order them in terms of their importance. For this purpose, the Delphi approach is the most suitable. In this section we describe, present and discuss the results of the Delphi study.

**Phase 1: Discovery of the issues**

In this phase we generated a list of objectives that are critical for ensuring privacy of GenZ. Our starting point were the six Fundamental Objectives. We did not include the Means objectives since those are the mechanisms for achieving the fundamental objectives and hence, are important in terms of realizing the outcomes. Our panelists, however, felt that there were other sub-objectives in the Fundamental objectives group that should be included in the initial list.

The following five additional sub-objectives were included for consideration:

- Maximize uniformity of privacy laws
- Ensure transparency in what information is collected
- Maximize awareness of how data flows in the platform
- Maximize control over personal information
- Ensure clarity of where personal information is stored

The complete list of objectives included appears in Table 6.1. The table also provides a brief description of each of the objectives.

After the initial discovery of the items, all respondents were given an opportunity to comment on the gathered issues and/or the explanations and provide any additional clarity as necessary. They were also provided the opportunity to add any new issues that they considered to be missing in the current list.

*Table 6.1, List of all objectives included in the Delphi Study*

| No | Issues (unranked) |
|---|---|
| 1 | *Maximize awareness of platform functionality*: Ensure users are aware of platform functionality; Maximize awareness of how data flows in the platform; Maximize clarity of how different aspects of the platform come together. |
| 2 | *Maximize responsibility of data custodians*: Ensure people have responsibility for protecting personal data; Ensure people have accountability for protecting personal data; Maximize integrity of data custodians. |
| 3 | *Maximize individual ability to manage privacy controls*: Maximize my ability to control my own information; Maximize democratization of privacy controls; Ensure clarity of where personal information is stored; Maximize individual control of identity; Maximize protection of my personal identity. |
| 4 | *Maximize that personal data does not change*: Maximize use of encryption technologies; Maximize use of new cryptographic advances; Maximize use of blockchains. |
| 5 | *Increase trust in online interactions*: Ensure transparency in what information is collected; Maximize use of guarantees in information exchange; Ensure reputation scores are accessible; Maximize use of platforms that have existed for a while. |
| 6 | *Maximize right to be left alone*: Maximize efforts to preserve individual privacy; Ensure that service providers follow privacy laws; Maximize uniformity of privacy laws; Maximize control over personal information. |
| 7 | *Maximize uniformity of privacy laws*: Ensure all laws are the same; Ensure that laws related to the jurisdiction; Maximize applicability of same law to all. |
| 8 | *Ensure transparency in what information is collected*: Make transparent upfront the information that will be collected; Communicate the purpose of collecting pertinent information. |
| 9 | *Maximize awareness of how data flows in the platform*: Make all aware of how the data flows through the platform; Communicate where the data is manipulated; Maximize privacy during data flow. |
| 10 | *Maximize control over personal information*: Allow individuals to control their data; Ensure that individual has a choice how their data is used; Maximize individual control of their data. |

| | |
|---|---|
| 11 | *Ensure clarity of where personal information is stored*: Communicate where personal information is stored; Ensure that location of stored data is known to individuals; Maximize individual choice for storing individual data. |

**Phase 2: Determining the most important issues**

The goal in phase two was to pare down the list of issues so that they can be meaningfully ranked by the respondents (Schmidt 1997). To accomplish this, all the participants were asked to choose from the list, which currently encompassed all issues they had considered, only the most important privacy objectives of GenZ. To do this, a randomly ordered and consolidated list from the first phase was sent to each participant. From this list, the respondents independently selected the issues they considered as the most important in privacy objectives of GenZ. All issues that were not selected by a majority of the respondents were eliminated from the list. This resulted in a list of 11 total issues selected as most important privacy objectives of GenZ by men and 14 total issues selected as most important by women. Schmidt (1997) suggests that this phase be repeated until the list include less than 20 issues, therefore only one round was necessary as both men and women produced lists under 20 items.

*Table 6.2, Results of phase 2 - Male participants*

| No | Issues (Rank Ordered) |
|---|---|
| 1 | Maximize control over personal information |
| 2 | Maximize uniformity of privacy laws |
| 3 | Maximize that personal data does not change |
| 4 | Maximize individual ability to manage privacy controls |
| 5 | Maximize awareness of platform functionality |
| 6 | Maximize responsibility of data custodians |
| 7 | Increase trust in online interactions |
| 8 | Maximize right to be left alone |
| 9 | Ensure transparency in what information is collected |
| 10 | Maximize awareness of how data flows in the platform |
| 11 | Ensure clarity of where personal information is stored |

According to Schmidt (1997) a list of fewer than twenty issues can be meaningfully ranked and thus, researchers can continue with phase three, which is aimed at ranking the issues in

order of importance. Table 6.2 and 6.3 show results from phase two according to men and women with respect to the issues the majority found important privacy objectives of GenZ.

*Table 6.3, Results of phase 2 - female participants*

| No | Issues (Rank Ordered) |
|---|---|
| 1 | Maximize right to be left alone |
| 2 | Maximize awareness of how data flows in the platform |
| 3 | Ensure clarity of where personal information is stored |
| 4 | Maximize individual ability to manage privacy controls |
| 5 | Maximize that personal data does not change |
| 6 | Maximize control over personal information |
| 7 | Ensure transparency in what information is collected |
| 8 | Maximize awareness of platform functionality |
| 9 | Maximize responsibility of data custodians |
| 10 | Maximize uniformity of privacy laws |
| 11 | Increase trust in online interactions |

**Phase 3: Ranking the issues**

Phase three was conducted to rank the most important privacy objectives of GenZ by men and women. Lists were provided separately to men and women, which detailed the issues they had chosen in phase 2 as the most important privacy objectives of GenZ. The separate lists were distributed via survey to the male and female respondents groups and in the survey, they were instructed to rank the issues in the lists in descending order from the most important to the least important to them. Each group, male and female, were analyzed where the following were calculated: means ranks for each issue, Kendall's Coefficient of Concordance, and percentage of respondents placing the item in the top half of the list. This process was repeated for three rounds. At the conclusion of each ranking round, issues ranked lowest (higher rank-means), were removed from the list and not presented in subsequent rounds. This was done consistent with the Ranking Delphi method in order to facilitate movement towards consensus. Tables 6.4 and 6.5 show results from our analysis for women and men respectively. No issues were dropped between round two and three as the mean-ranks were near equal for all ranked

issues for both male and female groups. The first number for each rank is the rank-mean and the second is the percentage of respondents placing the item in the top half of their list.

*Table 6.4, Mean rank for male participants*

| **Issues: men** | **R1** | **R2** | **R3** |
|---|---|---|---|
| Maximize control over personal information | 4.83<br>67% | 2.60<br>80% | 2.38<br>77% |
| Maximize uniformity of privacy laws | 3.75<br>75% | 4.40<br>40% | 3.31<br>54% |
| Maximize awareness of platform functionality | 4.00<br>67% | 4.20<br>40% | 3.85<br>54% |
| Maximize individual ability to manage privacy controls | 5.00<br>58% | 3.73<br>33% | 4.15<br>46% |
| Increase trust in online interactions | 5.25<br>67% | 3.87<br>40% | 3.62<br>38% |
| Increase awareness about people accessing your profile | 8.33<br>17% | N/A | N/A |
| Maximize responsibility of data custodians | 6.00<br>50% | 5.07<br>37% | 5.15<br>31% |
| Maximize that personal data does not change | 6.08<br>42% | 4.13<br>40% | 5.54<br>8% |
| Maximize right to be left alone | 8.00<br>8% | N/A | N/A |
| Maximize awareness of how data flows in the platform | 7.08<br>25% | N/A | N/A |
| Ensure clarity of where personal information is stored | 7.67<br>25% | N/A | N/A |

*Table 6.5, Mean rank for female participants*

| **Issues: females** | **R1** | **R2** | **R3** |
|---|---|---|---|
| Maximize responsibility of data custodians | 7.67<br>33% | 5.64<br>45% | 6.86<br>29% |
| Maximize individual ability to manage privacy controls | 5.56<br>79% | 4.82<br>45% | 4.57<br>43% |
| Maximize awareness of platform functionality | 6.33<br>67% | 5.00<br>45% | 6.57<br>14% |
| Maximize control over personal information | 6.56<br>56% | 5.55<br>36% | 5.29<br>29% |

| | | | |
|---|---|---|---|
| Ensure transparency in what information is collected | 6.67<br>67% | 4.64<br>55% | 6.14<br>0% |
| Maximize awareness of how data flows in the platform | 6.33<br>67% | 4.64<br>45% | 3.86<br>43% |
| Maximize that personal data does not change | 4.11<br>100% | 5.00<br>36% | 5.29<br>43% |
| Maximize uniformity of privacy laws | 9.33<br>33% | N/A | N/A |
| Maximize right to be left alone | 7.00<br>56% | 4.82<br>45% | 2.00<br>100% |
| Maximize uniformity of privacy laws | 8.22<br>44% | N/A | N/A |
| Increase trust in online interactions | 9.67<br>22% | N/A | N/A |
| Protect your account by logging out | 10.33<br>11% | N/A | N/A |
| Ensure clarity of where personal information is stored | 7.22<br>44% | 4.91<br>45% | 4.43<br>71% |
| Managing spam and phishing emails | 10.00<br>22% | N/A | N/A |

In this section, we discuss the findings pertaining to the two research questions of this phase of the study. A synopsis of the findings is presented by the research question and conclusions are drawn with respect to each. The table below (Table 6.6) shows the final results of our study.

*Table 6.6, Most important issues: comparison between men and women. Most to least*

| | **Females** | **Males** |
|---|---|---|
| 1 | Maximize right to be left alone | Maximize control over personal information |
| 2 | Maximize awareness of how data flows in the platform | Maximize uniformity of privacy laws |
| 3 | Ensure clarity of where personal information is stored | Increase trust in online interactions |
| 4 | Maximize individual ability to manage privacy controls | Maximize awareness of platform functionality |
| 5 | Maximize that personal data does not change | Maximize individual ability to manage privacy controls |
| 6 | Maximize control over personal information | Maximize responsibility of data custodians |
| 7 | Ensure transparency in what information is collected | Maximize that personal data does not change |

| | |
|---|---|
| 8 | Maximize awareness of platform functionality |
| 9 | Maximize responsibility of data custodians |

**Gender differences and privacy objectives of GenZ**

The main finding from this study is that while from a similar background; men tend to focus (rank highest) on technical control for privacy objectives of GenZ, while women focus (rank highest) on their right to be left alone and awareness solutions (see table 6.6). This is important as it draws a distinct conclusion for the need for varied solutions and privacy objectives of GenZ that addresses these differing concerns amicably. For example, men emphasize the uniformity of privacy laws and maximizing control over personal information. Women, on the other hand tended to emphasize the additional responsibility of platforms to show how data flows through them, this emphasizing clarity of objectives by responsible authorities. To the point: women in the study stated that besides platforms, individuals should have responsibility of what information they make available and what is kept private. Results show the females are more inclined for taking personal responsibility and clarity. Males on the other had tend to suggest that there should be more uniformity in regulations and emphasis should be placed on establishing trust.

**Gender convergence**

The convergence between men and women occurred first in phase two and then in phase three in different ways. In phase two both men and women chose similar issues, however male respondents selected 11 and female respondents 14 total issues as most important. The same 11 issues selected by men were also selected by women. This is important to note as men and women selected 11 of the total 14 overall, most important objectives for privacy of GenZ in a similar fashion. In this phase, we saw a high degree of convergence amongst selected measures

in terms of overall preferences. However, once the study moved into phase 3, the most interesting points of convergence for men and women occurred in all three rounds.

After the first round of the ranking process in phase 3 of the study, 4 of the issues ranked lowest by female respondents and 4 of the issues ranked lowest by male respondents were removed from the respective list and not considered in the subsequent rounds. The table below (Table 6.7) shows the issues ranked lowest by women and men. None of the lowest ranked objectives were similar. This is important to note even though the study is focused on finding the most important prevention measures, understanding which concerns are least important to both groups and can be safely set aside is also important knowledge which can save time and expedite the policy creation process aimed at creating effective prevention measures.

*Table 6.7, Lowest Ranked issues for Males and Females in Round one of Phase three*

| **Issues ranked lowest by females** | **Issues ranked lowest by males** |
|---|---|
| Maximize uniformity of privacy laws | Increase awareness about people accessing your profile |
| Increase trust in online interactions | Maximize right to be left alone |
| Protect your account by logging out | Maximize awareness of how data flows in the platform |
| Managing spam and phishing emails | Ensure clarity of where personal information is stored |

After the second round in phase three both men and women place only one issue in the top half of the list. On an interesting note, there were some differences between mean ranks for the remaining issues for both female list and male list of privacy objectives for GenZ. However, none of the groups achieved consensus based on their respective Kendall's Coefficient of Concordance (Table 6.8), but the purpose of this study was not to achieve agreement. Instead, the purpose was to understand preferences and whether any convergence in those preferences occurred between the male and female groups with respect to privacy objectives of GenZ.

Finally, after the third round, in phase three, both groups did achieve weak agreement based on their respective Kendall's Coefficient of Concordance. Five of the privacy issues included in both lists were similar, though not identical. Of interest here is females emphasized their right to be left alone, while males emphasized the importance of control over personal information. Females wanted more awareness of how data flows, while males waned uniformity in privacy laws. Females wanted clarity of where their personal data was stored and males wanted to increase trust in online interactions.

*Table 6.8, Kendall's Coefficient of Concordance by round for Males and Females*

| Round | Men | Women |
|---|---|---|
| 1 | 0.231 | 0.188 |
| 2 | 0.121 | 0.017 |
| 3 | 0.249 | 0.303 |

In order to solve a problem as complex as GenZ privacy, it is important to understand the interplay between the information itself and the decision-making framework employed by an individual or organization. To contextualize this assertion, we note that research in decision-making has long recognized that no simple connection exists between ‘‘more information’’ and ‘‘better decisions’’ (Sarewitz et al., 2000; Sarewitz & Pielke 2007). Therefore, simply adding more information with the implication being a greater understanding of the decision context, in this case privacy, cannot be said to either solve the problem or demonstrate the shortcomings given a decision maker (Sarewitz & Pielke 2007). Many reasons exist as to why only adding more information alone to the discussion may not improve decision outcomes or outright solve the problem. For example; the information is not relevant to user needs; it is not appropriate for the decision context; it is not sufficiently reliable or trusted; it conflicts with users' values or interests; it is unavailable at the time it would be useful; it is poorly communicated (Sarewitz & Pielke 2007). Further yet, those who stand to benefit or be adversely affected the most, will have a greater stake in the outcome of such decisions

(Sarewitz & Pielke 2007). This is highly relevant to our study in that the Delphi methodology seeks to address several of these concerns, namely; relevance, appropriateness to decision context and, perhaps, most important of all it seeks to involve the most affected stakeholders in the decision process.

To this end, the information necessary in the context of decision making related to the prevention of cyberstalking can be said to be strongly influenced by complex and important factors, which influence to a high degree the types of information that decision makers need and use in attempting to solve the problem of GenZ privacy (Sarewitz & Pielke 2007). Therefore, this research involved the most affected stakeholders in the decision-making process to elicit and embed as many important factors as possible in the decision-making process for those who create policy. This grounds decisions, based on this study, firmly in the values and interests of the vested stakeholders (those most affected). Hence, academics who seek to understand the behavior of scientific information in complex decision contexts such as GenZ privacy must then converge on the recognition that the utility of this information depends on the dynamics of the decision context and the broader social setting (Jasanoff and Wynne, 1998; Pielke et al., 2000). In the context of India's most affected stakeholders with respect to GenZ privacy, it is clear that men and women prioritize objectives differently and align only in one place for their top 5 objectives (See Figure 6.2). From this study, it can be clearly stated even with objectives derived directly from involved stakeholders, overly general policy will fail to adequately address societal GenZ privacy concerns. With a misalignment of priorities between men and women and low levels of overlap in perceived issues it would be difficult, if not impossible, to adequately address the issue of GenZ privacy. To this end, our research highlights both the need for additional research to better understand this complex phenomenon and that important issues do indeed exist, which require redress such that the problem of GenZ

privacy can be eliminated. This is then to say the following: the presentation of knowledge for its own sake does not provide utility, and thus it is important to recognize that the contribution of this research in that it contributes knowledge by providing application utility to the decision maker. This is done by providing useful objectives, derived directly from affected stakeholders, to be incorporated into the decision-making process when formulating policy.

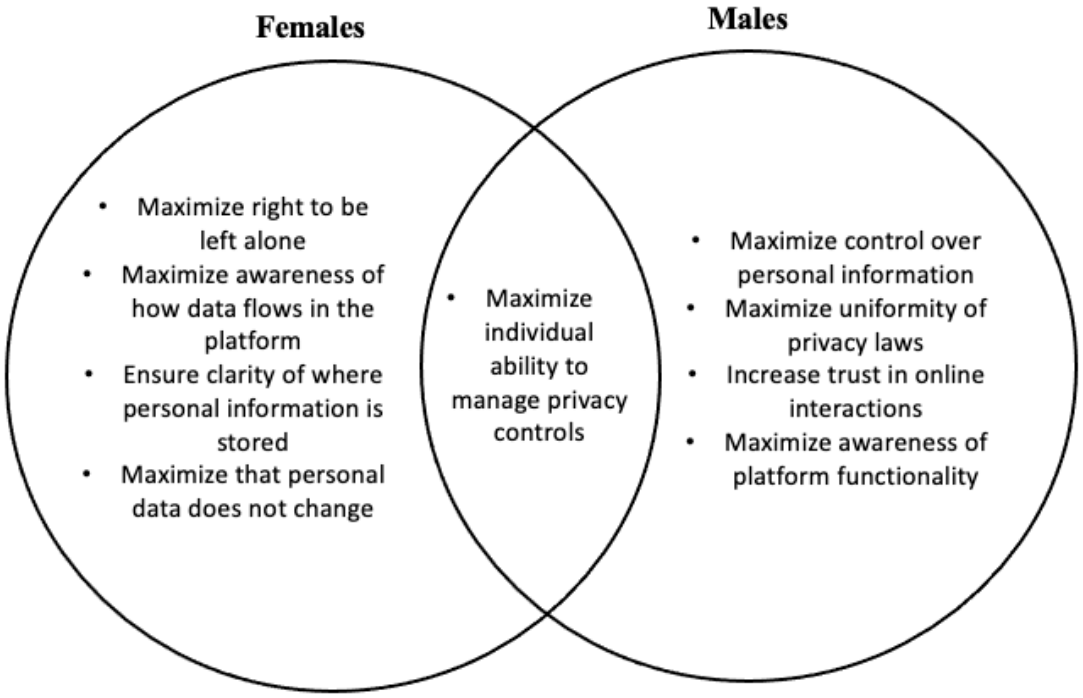


*Figure 6.2, Venn Diagram for Females and Male Top 5 Issues*

This chapter and the Delphi study systematically identified the key privacy concerns that men and women consider important with respect to the GenZ privacy. To date, this is perhaps one of the few studies that conducts an explicit analysis of these concerns in the context of GenZ privacy in India. Methodologically, the use of the Delphi study in a cultural examination of privacy concerns in India allows us to develop unique insights into the subject matter. Our conceptualization of the decision context does not necessarily focus on gaining consensus as to the core prevention mechanisms for GenZ privacy. Rather the study has developed insights based on the top concerns of men and women and looked to determine to what degree a

convergence of those concerns exists. This perspective allows us to identify the overall top concerns amongst men and women as the central concepts to ensure privacy.

The study itself is not without limitations, inheriting the methodological limitations known to the Delphi method. Considerable effort is required to get buy-in from the participants and is time consuming to identify male and female members and obtain agreement from the participants to be involved and continue throughout all phases. Further, the sample size varied from phase to phases and by round, however it was always within the specified ranges for a proper Delphi study. The sample size was also relatively small compared to larger sized studies. As a consequence, one might question representativeness of participants, however, our study was solely focused on male and female members of GenZ. It will be useful to extend the study to other parts of the world and incorporate other perspectives for comparative purposes, allowing comparison of male and female perceptions on a global scale and differences between societies. This would add a great deal to the generalizability of the study and the contribution to cyberstalking prevention as a whole.

# 7
# Conclusions

In this chapter, we conclude the research presented in this thesis. First, we discuss the theoretical contributions of this research. Second, we discuss practical contributions that will help in enhancing privacy policies for GenZ. Third, we discuss the limitations of this research. Fourth we present future research directions

## 7.1 Contributions

In this thesis, we set out to answer the following three research questions: 1) What are the individual values of GenZ concerning online privacy? 2) What are the fundamental objectives of GenZ in terms of protecting their online privacy? 3) What means objectives GenZ considers for protecting their online privacy? In this section, we will discuss the contributions for each of the research questions.

**What are the individual values of GenZ concerning online privacy?** As noted in the literature review section, dominant information privacy research falls into two categories – privacy concerns and privacy calculus. While the specifics of the *privacy concerns* literature have been discussed in this thesis, this body of work's overall contribution has been to identify

individual concerns relative to sharing personally identifiable information. While it is essential to identify the privacy concerns, the concerns themselves emerge from nowhere. Privacy concerns are grounded in the context, the nature of use, and the culture. In this thesis, we have argued that while privacy concerns may be significant, individuals' values are equally essential. Steps that people will take to address the privacy concerns are a function of individual values.

The second body of literature concerns privacy calculus. In such cases, individuals calculate, based on a range of constraints, worth sharing their private information. Again, while different situations warrant different responses regarding the value that individuals place on privacy, individual values play an important role in deciding an individual's willingness to disclose. Our theoretical contribution rests in bringing individual values central to our understanding of information privacy. While our study focuses specifically on GenZ, the findings are generalizable for a broader application.

**What are the individual values of GenZ with respect to online privacy?** Values have an important place in scientific discourse. Scholars have noted that the concept of values is one of the very few topics that have been discussed and employed across several social science disciplines (see Rokeach and Ball-Rokeach, 1989). Despite widespread use, what constitutes values has not been well understood. Differentiation of values as motivations, goals, utilities, attitudes, interests, among others is significantly noted. In this thesis we have followed the understanding of values as these describe a person as opposed to an object. Following the work of Ralph Keeney, we have considered values in terms of "outghtness." Oughtness suggests how an individual should or ought to behave. Hence, any concern an individual has is grounded on ougthness and partially, the context and the culture. As indicated in figure 7.1, privacy concerns get shaped by the privacy values. If individual privacy values are not understood, the privacy concerns are ill-founded. Individual values are also context dependent. Our research brings the importance of individual values to be central to any discussion of privacy concerns.

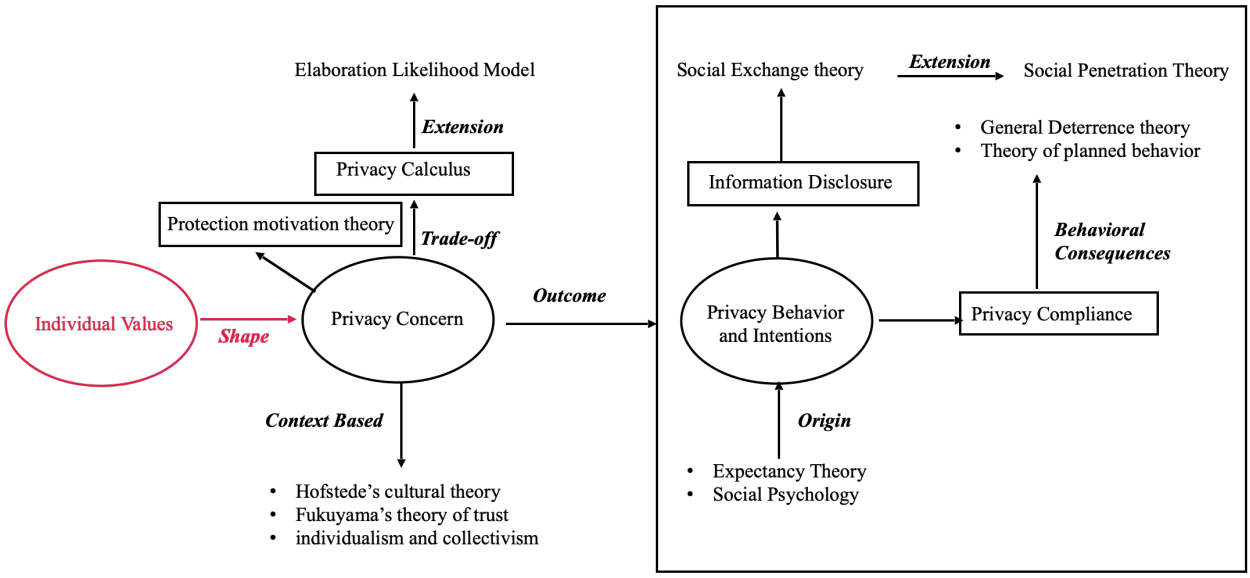


*Figure 7.1, Theoretical contribution of this research*

**What means objectives GenZ considers for protecting their online privacy?** Ever since the time of Aristotle, the concept of values has often been discussed. Values that individuals hold, imbibe in themselves the morals and beliefs, conduct and qualities that are desired. The values can be divided into two sets, ones that are terminal and the ones that are instrumental. Keeney (1992), argued that adding a directional preference to a value (or value sets) results in a value becoming an objective. Objectives then help in deciding the direction in which an individual, organization or a society needs to evolve into. There is an ordered relationship between values and the resultant objectives and hence, the measures. We present the hierarchical relationship in Figure 7.2. In this paper we have developed two sets of objectives –fundamental and means, which correspond to the terminal and instrumental values. Our objectives bring structure to the privacy concerns literature by providing tangible things that individuals, organizations and societies can work on.


*Figure 7.2, Hierarchical structure of value and objectives*

## 7.2 Decision Model to Maximize Privacy Amongst GenZ

Fundamental objectives for maximizing information privacy that were created in this study used the original ideas from Keeney's (1992) value-focused thinking approach. As noted earlier in this thesis, the value-focused thinking approach has its roots in Operations Research and the approach offers a means for decision-making (Clemen, 1996). Keeney (1992) has summarized the two dominant methods for decisions – AFT (Alternative Focused Thinking) and VFT (Value Focused Thinking). Table 7.1 summarizes the difference between the two approaches.

*Table 7.1, Comparison of AFT and VFT*

| AFT | VFT |
|---|---|
| A decision problem is recognized<br>Alternatives are identified<br>Alternatives are evaluated<br>An alternative is selected | • A decision problem is recognized<br>• Values are specified<br>• Alternatives are created<br>• Alternatives are evaluated<br>• An alternative is selected |

**Step 1 – Defining Strategic Objectives**

As indicated in Table 7.1, the AFT techniques are the classic approach to decision-making. It essentially entails the listing and identification of alternatives. AFT is critiqued by Keeney in that the approach constrains a decision maker. He argues that the generated set of alternatives often do not necessarily represent and reflect what is important for a decision. As Kahneman (2003) argues, the decision maker often remains "anchored" to the domain, thus, limiting of their context. VFT, in contrast, begins with individual values that are inherent to any decision context. The approach then works through to propose alternatives, which can help address the individual values.

If a decision maker is tasked with determining what the best way to maximize information privacy for GenZ is, a list of alternatives might include things like prevent GenZ from going online, ensure that they follow a strict protocol, etc. If one were to use the AFT approach, a decision maker would proceed to identify which of the alternatives work best for GenZ. This would then result in implementing the alternatives, without much consideration of the underlying values inherent in the decision context. Therefore, any implemented solution would therefore be artificially bounded by the constraints inherent in the alternative. In contrast, if a VFT approach is chosen, it will ensure that the decision maker first works with individuals to identify what do they care about and what their values are. This will then determine the appropriate alternatives. Such alternatives truly address these needs. VFT therefore recognizes that alternatives that would become the means to achieve the more fundamental value-based objectives, which often are hidden in any decision context.

What we have presented in this research (see Table 5.2 in chapter 5) instantiates the first 2 steps of the VFT process shown, which are shown in table 7.2. What we have in tables 7.1 and 7.2, provides researchers with a framework for addressing information privacy issues. However, there is a need for a methodology, which will help in creating, evaluating and

selecting these alternatives. Such alternatives are the practical basis for decision-makers to make informed decisions. The research presented in this thesis is a theoretical grounding for a methodological approach and sound techniques for creating, evaluating and selecting the best alternatives, particularly in the context of maximizing information privacy amongst GenZ.

*Table 7.2, A step wise VFT method for information privacy decision making*

| Step | Activity | The Process | Reference/Notes |
|---|---|---|---|
| 1 | Define a Strategic objective | Recognize Decision Problem | As in Keeney (1999); Dhillon & Smith (2019) |
| 2 | Create Value Hierarchy | Specify Values | As in Keeney (1999); Dhillon & Smith (2019) |
| 3 | Develop Evaluation Measures | Evaluate Alternatives | Typically through a Case Study |
| 4 | Create Value Hierarchy | Evaluate Alternatives | Typically through a Case Study |
| 5 | Weight the value Hierarchy | Evaluate Alternatives | Typically through a Case Study |
| 6 | Generate Alternatives | Create Alternatives | Typically through a Case Study |
| 7 | Score Alternatives | Evaluate Alternatives | Typically through a Case Study |
| 8 | Rank Alternatives | Evaluate Alternatives | Researcher |
| 9 | Perform Sensitivity Analysis | Evaluate Alternatives | Researcher |
| 10 | Recommendations | Select Alternatives | Researcher |

While VFT is one technique to generate informed alternatives, there are a number of others, both qualitative and quantitative. Analytic Hierarchy Processing (AHP), is one such technique, which was developed for these types of problems (Saaty, 1980). AHP is a mathematical decision-making technique. It takes into consideration both qualitative and quantitative aspects of a decision. Complex decisions are reduced to a series of pairwise (one-on-one) comparisons, which are then used to synthesize the results. AHP is not without criticism, particularly because of consistency and rank reversals problems. As Chambal et al. (2003) note, it is hard to implement it in the context of a large number of alternatives.

As a future research direction, in this thesis we propose using a 10-step approach (Table 7.2). The approach uses a combination of qualitative and quantitative techniques. The concepts

are derived from the literature, particularly (Keeney, 1992; Keeney and Raiffa, 1993; Kirkwood, 1997; Chambal et al., 2003) and presents a multi-objective decision analysis perspective. Various other scholars have used similar steps to provide guidance in decision-making. For instance, Chambal et al. (2003) applies concepts in the context of choosing a new municipal solid waste management strategy. Merrick and Garcia (2004) use the approach to define best alternatives for improving a watershed.

As noted in Table 7.2, Keeney (1999) and Dhillon & Smith (2019) have elaborated on how to address steps 1 and 2. However, as a future research direction, we propose steps 3-10 as a basis for developing a multi-criteria decision-making approach. For the purposes of sketching out the future research direction, we situate the problem in GenZ and maximizing information privacy. Many of the quantitative numbers are hypothetical and for illustrative purposes only. The process, however, sketches out a typical progression of a decision-makers approach. There is no doubt however, that our proposed approach needs to be empirically validated.

**Step 2 - Create a Value Hierarchy**

Decision makers use a value hierarchy as a conceptual model that helps in generating alternatives. A value hierarchy helps in structuring individual values. The process begins with the strategic objective and ends up in developing lower-level objectives that are used in the evaluation process. As noted previously, fundamental objectives are the ones that decision maker desires in a given decision context. Fundamental objectives can be presented as a tree where the lower tier objectives become the basis for the more detailed means presented by the higher tier objectives. As Kirkwood (1997) notes, a value hierarch defines how fundamental objectives are appropriately related to the strategic objective. The hierarchy in turn helps in identifying if any values are missing or if other additional values are required.

In the research presented in this thesis, we closely followed the process of eliciting values and organizing the objectives. As noted previously, the process has been spelled out by Keeney (1992) and used by various other scholars, including Dhillon and Torkzadeh (2006) and Dhillon and Smith (2019). There are several desirable properties for an objective hierarchy. Kirkwood (1997) identifies these properties to include completeness, non-redundancy, decomposability, operability, and small size. The definitions of the properties are:

- *Completeness* refers to the "collectively exhaustive." It is the notion that the objectives should cover all the necessary concerns. The property assures that alternatives are adequately evaluated, which would then subsequently be ranked.
- *Non-redundancy* refers to "mutually exclusivity." It is the property that implies that no two objectives at any tier should mean the same.
- *Decomposability* is a property that refers a way in which it is possible to measure each objective such that it is possible to determine overall desirability of the alternatives.
- *Operability* is a property that suggests the objective hierarchy should mean the same thing to all concerned.
- *Small size* is property that suggests that the hierarchy should not be larger that is absolutely necessary. This minimizes the time that will be spent on subsequent steps as presented in table 7.2

**Step 3 - Develop Evaluation Measures**

Following the value hierarchy, evaluation measures for each objective need to be defined. Evaluation measures help in specifying unambiguous rating, particularly in terms of performance of alternatives. As Kirkwood (1997) notes, an evaluation measure can either be a

natural scale or it can be measured using a constructed scale. Keeney (1992) states that a natural scale, which is measured directly, is less controversial since it has a common interpretation for everyone. As an example, survey questions that use a 5-point Likert scale are considered to be a constructed scale.

In this thesis we presented the fundamental objectives Table 5.2. Given the qualitative nature of the sub-objectives, there can be issues with natural measurement. Hence, constructed scales are the best option. As a future research direction, we propose developing a list of generic questions to measure each of the sub-tier objectives in Table 5.2 and 5.3. The questions are then presented to a decision maker for a more accurate wording and scales that relate to the specific context. The process also allows the decision maker to see first-hand, the value hierarchy. The questions so created should be administered to all GenZ participants.

**Step 4 - Develop Value Functions**

One of the problems of measures from the previous steps is that they are all in different scales, this makes it difficult to obtain a summated score. Keeney (1992) and Kirkwood (1997) propose a solution where value functions are transformed into "value units." And a scale of 0 to 1 is adopted. For our future research, we propose using a 5-point Likert scale. Input from a decision maker is necessary to evaluate the differences between each point on the Likert scale and what the differences might be. If the difference in each point on the Likert scale are the same, then the assignments of values can be as per Table 7.3. Alternative techniques can be evaluated if the various questions do not have an equal change in value.

*Table 7.3, Evaluation Measures Assuming Equal Change*

| Score | Meaning | Value |
|---|---|---|
| 1 | Strongly disagree | 0 |
| 2 | Disagree | 0.25 |
| 3 | Neither agree not disagree | 0.5 |
| 4 | Agree | 0.75 |
| 5 | Strongly agree | 1 |

For example, consider the question "You and your team want to increase trust in online environments." Following discussions with decision makers, it might be the case that there is a bigger difference between a score of 3 and 4 and 3 and 2 than the score of 4 and 5 and for 1 and 2. This means that the value function would probably be more like an S-curve as represented in Figure 7.3, otherwise it would be a straight line. Moreover, in any value model, value functions are generally preferred to be either monotonically increasing or monotonically decreasing. As Chambal et al., (2003) argues, it helps in establishing consistency. A monotonically increasing value function, for instance, will have a score along the x-axis that increases as the value along the y-axis also increases. A value model that has functions that have monotonically increase, helps in scoring alternatives because of "more is always better" notion.

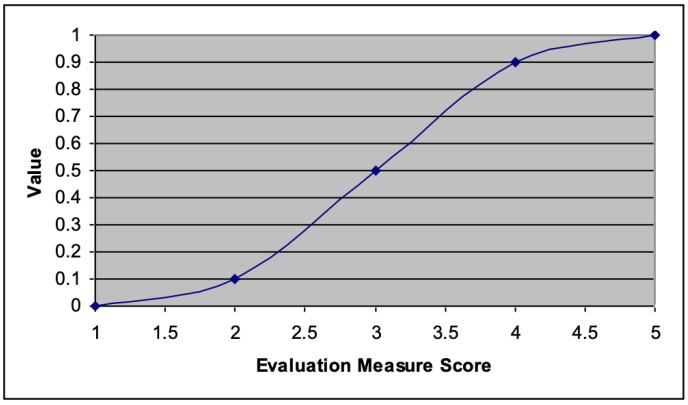


*Figure 7.3, Evaluation Measures with Non-Equal Changes*

Kirkwood (1997) details the process for determining non-linear value functions (p.62). The process consists of the following:

- Set the lowest and highest evaluation measure scores to values of 0 and 1, respectively.
- The decision maker is asked to consider if there is a difference in values when moving from 1 to 2, 2 to 3, 3 to 4, and 4 to 5.
- The decision maker, then, might indicate that the difference in going from 5 to 4 is less than going from 4 to 3 for and evaluation measure and that it might be 4 times greater.
- The decision maker may indicate that the same situation is true at the lower end.
- The researcher then sets the lowest increments from 1 to 2 and 4 to 5 to $\boldsymbol{x}$. Increments from 2 to 3 and 3 to 4 are set to $4\boldsymbol{x}$. The value of $\boldsymbol{x}$ is then solved by recognizing that $\boldsymbol{x} + 4\boldsymbol{x} + 4\boldsymbol{x} + \boldsymbol{x} = 1$; or $\boldsymbol{x} = 0.1$. The values for each evaluation measure is determined as is shown in Figure 7.2 and generated as:

$$V(5) = \boldsymbol{x} + 4\boldsymbol{x} + 4\boldsymbol{x} + \boldsymbol{x} = 1.0;\ \boldsymbol{x} = 0.1$$
$$V(1) = 0$$
$$V(2) = \boldsymbol{x} = 0.1$$
$$V(3) = \boldsymbol{x} + 4\boldsymbol{x} = 0.5$$
$$V(4) = \boldsymbol{x} + 4\boldsymbol{x} + 4\boldsymbol{x} = 0.9$$

**Step 5 – Weight the Value Hierarchy**

A value hierarchy has multiple objectives, which should all be considered in the decision-making process. However, all the objectives do not have same level of importance for a given decision context. To account for the variance and differences in the level of importance, weights must be assigned to each value hierarchy while being cognizant of the

decision context. While assigning weights the total for each branch of the hierarchy must sum to 1.0.

In the literature (e.g., Borcherding et al., 2003), various weighting techniques have been proposed - the ratio method, the swing weighting, the trade-off approach, pricing out method, among others. As a future research direction, we propose using the swing weighting technique. Swing weights method has been preferred because of significant convergent validity. Swing weights approach is operationalized by asking the decision maker to consider the lowest tier objectives for each branch. And then, also, consider the worst possible levels in terms of value. Decision maker is also asked to determine the objective in a group that they would like to swing to the best possible level. This is followed by asking the decision maker to compare the two most important objectives and assess the relative importance of the full swing for each objective. The process proceeds iteratively with due consideration of increments between each objective. The results are sequentially ordered by value. At each increment a factor of importance is assigned relative to the smallest increment. After the process is completed, the total of all the increments needs to equal 1. The system of equations in step 4 are used to solve exact manner in which the weights are assigned. If there is more than one decision maker, their weights can be averaged, and agreement sought amongst the decision makers.

**Step 6 - Generate Alternatives**

One of the primary advantages of the Value Focused Thinking approach is that beyond the fundamental objectives, the means of achieving them through alternatives is also developed. The alternatives take the form of a value hierarchy. The value hierarchy drives the right kind of questions to be asked, such that, alternatives emerge. When administering the questionnaire (as discussed in Step 3), each question is followed up by seeking respondents to provide alternatives thus, in turn, improving the objectives. Following the development of the

alternatives, these are then discussed with the decision maker to determine if there are any additional objectives that could be added.

**Step 7 – Score the Alternatives**

The output of step 6 must be scored in order to generate a value model. The scoring is undertaken relative to each objective. To determine the scores, typically a panel of decision makers (and at times outside experts) is assembled. The panel evaluates the measure for each objective. Ideally, the panel should arrive at a consensus. A consensus adds defensibility to the output, this helps in removing uncertainty. If an objective has a negative impact, then negative scores can also be attributed.

**Step 8 - Perform Deterministic Analysis**

In table 5.1 we have defined a range of objectives. A question that arises is which of these alternatives would have maximum impact on ensuring GenZ privacy. This is where deterministic analysis plays a role. Deterministic analysis allows ranking of the various alternatives in order of importance. This provides for an informed and quantifiable means for selecting the outcome.

Table 7.4 presents an illustrative example of deterministic analysis. In this example, we use fictitious numbers for objective number 6 of the value hierarchy. As stated in Step 5, the 3 weight columns are generated using swing weighting. The task is completed via interviews with decision makers. The Adjusted Weight columns is also referred to as the global weight and is calculated as W1 * W2 * W3. The measure column has a list of evaluation measures that are generated via a survey. The Average-Adjusted-Score column represents the average value, which is the combined scores of all respondents. It is adjusted through the value function scheme that was shown in Step 4. This column shows how group or organization, or individuals (depending on the situation) performed with respect to a given evaluation measure.

The Scaling Factor column represents the importance of a given measure. It is calculated as one minus Average-Adjusted-Score. So, higher the Scaling Factor, the more scope there is for improvement for an objective.

The alternatives column, which is labeled as "Alt," represents the actual alternatives that are generated through the survey and the subsequent interviews with decision makers. The score column represents the actual score for each of the alternatives relative to each measure. This was discussed in Step 7. Finally, the Value Adjusted Score column is the score adjusted through the value functions that were created in Step 4.

The calculations below represent the final step where the best alternatives are determined using Equation 1. Thus, as represented in the equations the alternatives $A_2$ and $A_3$ are recommended since these have the greatest impact.

(Equation 1): $V(A_i) = 1000 * \text{å}\ AW_j * SF_j * VAAS_j$

$\therefore$ $V(A_1) = (0.025)(0.33)(0.9) = \mathbf{7.4}$
$V(A_2) = (0.025)(0.33)(1.0) + (0.025)(0.67)(0.5) + (0.075)(0.11)(0.5) = \mathbf{20.8}$
$V(A_3) = (0.025)(0.67)(0.9) + (0.075)(0.77)(0.1) = \mathbf{20.\ 9}$
$V(A_4) = (0.075)(0.11)(0.75) = \mathbf{6.2}$

*Table 7.4, Table for Deterministic Analysis*

| **1st level evaluation** | | **2nd level evaluation** | | **3rd level evaluation** | | | | | **Alternatives** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Objective | Weight (W1) | Objective | Weight (W2) | Measure | Weight (W3) | Adj. Weight | Avg. Adj. Score | Scaling Factor | Alt | Score | Value Adj. Score |
| Steps | | | | | | | | | | | |
| 2 | 5 | 2 | 5 | 3 | 5 | 5 | 8 | 8 | 6 | 7 | 8 |
| 6 | 0.2 | 6.1 | 0.25 | Q 6.1.1 | 0.5 | 0.025. | 0.67 | 0.33 | A1 | 4 | 0.9 |
| | | | | | | | | | A2 | 5 | 1 |
| | | | | Q 6.1.2 | 0.5 | 0.025 | 0.33 | 0.67 | A2 | 3 | 0.5 |
| | | | | | | | | | A3 | 4 | 0.9 |
| | | 6.2 | 0.75 | Q 6.2.1 | 0.5 | 0.075 | 0.23 | 0.77 | A3 | 2 | 0.1 |
| | | | | Q 6.2.2 | 0.5 | 0.075 | 0.89 | 0.11 | A2 | 3 | 0.5 |
| | | | | | | | | | A4 | 4 | 0.75 |

**Steps 9 and 10 - Sensitivity Analysis and Final Recommendations**

The deterministic analysis forms the basis to perform the sensitivity analysis. Sensitivity analysis examines the validity of the findings since it removes subjectivity associated with the weights. It also provides insights to a decision maker. The process is undertaken by systematically altering the weights of each value and the subsequent impact on the final alternative scores and rankings are evaluated and tracked. As the individual weight change, other weights are adjusted accordingly. This ensures that the sum of the column or section does not change. As the weights are adjusted, the proportionality of the other weights is maintained.

On completion of sensitivity analysis, final recommendations are compiled and presented to the decision makers. The recommendations include the insights gained during the process. The recommendations are guidelines for the decision maker rather than being replacing individual discretion and judgement of the decision maker.

## 7.3 Limitations

As with any project, this research had several limitations. The limitations were constraints that prevented us from expanding the scope of this work. First, we focused on just GenZ participants. While we recognize that privacy values vary with age, restricting our study to GenZ prevented us from comparing it with other generations. Future research should consider a cross sectional study where different generations and their values are considered, evaluated, compared and then the relevant objectives are formed. This limitation, however, does not stop us from advancing theory. We are still able to make contributions to the body of literature, as has been discussed in the previous section.

Second, we adopted a rather focused approach in our inquiry. As Dhillon (1995) points out, our study was at a more micro-substantive level. Not only did we go in-depth into one setting,

we conducted in depth interviews with a large number of individuals. Doing so, allowed us to develop deep insights. While a micro-substantive investigation does not allow for a broad generalization, the generalization is limited to the theory and the axioms therein. Future research should use our objectives to engage in a more macro-objective study and develop a more parsimonious set of objectives.

## 7.4 Final words

Our study is one of the few that brings the concept of values to the center fold and systematically positions its relevance and scope in the extant literature. The study is well formed and addresses an important gap in the literature. Going forward, we hope that our identified values and objectives form the basis for more work that investigates information privacy in a range of settings. Our privacy objectives are a starting point and a reminder to policy makers who strive to develop meaningful regulations to protect what we have and who we are. By focusing on the values, we bring the concept of morals and ethics to the centerfold

# 8
# References


Adjerid, I., Peer, E., & Acquisti, A. (2016). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly,* 42(2), *465-488*

Adler, F. (1956). The value concept in sociology. *American Journal of Sociology*. 62(3), 272-79

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield Pub Incorporated.

Allen, J. P. (2005). Value conflicts in enterprise systems. *Information Technology and People*, 18(1), 33–49.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA: Brooks/Cole Publishing.

Altman, I., (1977). Privacy Regulation: Culturally Universal or Cultural Specific? *Journal of Social Issues*. 33(3), 66-84.

Alvesson, M., and Sandberg, J. 2011. Generating Research Questions through Problematization, *Academy of Management Review*. 36(2), 247-271.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490.

Angin, P., Bhargava, B., Ranchal, R., Singh, N., Othmane, L.B., Lilien, L. and Linderman, M. (2010) An Entity-centric Approach for Privacy and Identity Management in Cloud Computing, 2010 29th IEEE Symposium on Reliable Distributed Systems, Oct 31-Nov 3 New Delhi, India.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339-370.

Arrow, K. J., Sen, A., and Suzumura, K. (1996). *Social Choice Re-Examined*. Springer.

Arvai, J. L., Gregory, R., and McDaniels, T. L. (2001). Testing a structured decision approach: value-focused thinking for deliberative risk communication. *Risk Analysis*, 21(6), 1065-1076.

Awad, N.F., and Krishnan, M.S., (2006), The personalization privacy paradox: an empirical evaluation transparency and the willingness to be profiled online for personalization, *MIS Quarterly*, 30(1), 13-28.

Bachika, R., & Schulz, M. S. (2011). Values and culture in the social shaping of the future. *Current Sociology.* 59(2), 107-118.

Bandura, A. (1986). *Social Foundation of Thought and Action: A Social Cognitive Theory*. Prentice-Hall.

Bansal, G., Zahedi, F. 'Mariam,' & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, 24(6), 624–644.

Bargh, J. A., & Chartrand, T. L. (1999). The unbearable automaticity of being. *American Psychologist*, 54(7), 462.

Barth, A., Datta, A., Mitchell, J. C., and Nissenbaum, H. (2006). Privacy and Contextual Integrity: Framework and Applications, Security and Privacy, 2006 IEEE Symposium on: IEEE, pp. 15 pp.-198.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1041.

Bélanger, F., & James, T. L. (2020). A Theory of Multilevel Information Privacy Management for the Digital Era. *Information Systems Research*, 31(2), 510-536.

Bélanger, F., and Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1042.

Benassi P. (1999). TRUSTe: an online privacy seal program, *Communications of the ACM.* 42(2), 56 - 59

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*, 30(6), 1010-1042.

Bohman, J. 1991. *New Philosophy of Social Science: Problems of Indeterminacy*, MIT Press 1st edition. Cambridge, Mass.: MIT Press.

Borcherding, K., Eppel, T., and Von Winterfeldt, D., (1991). Comparison of Weighting Judgments in Multiattribute Utility. *Management Science*, 37(12), 1603 – 1619.

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the internet: self-regulation or government regulation? *Business Ethics Quarterly*, 16(3), 323-342.

Buckman, J. R., Bockstedt, J. C., & Hashim, M. J. (2019). Relative privacy valuations under varying disclosure characteristics. *Information Systems Research*, 30(2), 375-388.

Burell, G., and Morgan, G. 1979. *Sociological Paradigms and Organisational Analysis*. London: Heinemann.

Burrows, R., Johnson, P., and Johnson, H. 2014. "Influencing Behaviour by Modelling User Values: Energy Consumption," *2nd International Workshop on Behaviour Change Support Systems, PERSUASIVE'2014*: University of Bath, pp. 85-93.

Cao, Z., Hui, K. L., & Xu, H. (2018). An economic analysis of peer disclosure in online social communities. *Information Systems Research*, 29(3), 546-566.

Catton, W. R. (1954). *Propaganda effectiveness as a function of human values* (Doctoral dissertation, University of Washington).

Catton, W. R. (1959). A Theory of Value, *American Sociological Review* 24(3), 310-317.

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. *Information Systems Research*, 27(4), 848-879.

Chambal, S., Shoviak, M., and Thal, A. E. (2003). Decision Analysis Methodology to Evaluate Integrated Solid Waste Management Alternatives. *Environmental Modeling and Assessment,* 8(1), 25-34.

Charron, C. G., Evers, S. M., & Fenner, E. C. (1976). Beliefs, Attitudes and Values. In *Behaviour* (pp. 19-32). Palgrave, London.

Chellappa R., and Sin, R., (2005) Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, 6(2-3), 181-202

Chen, S., and Dhillon, G. (2003). Interpreting Dimensions of Consumer Trust in E-Commerce, *Information Technology and Management* 4(2/3), 303-318.

Chiu, C.-M., Wang, E.T.G., Fang, Y.-H. and Huang, H.-Y. (2014), Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. *Information Systems Journal*, 24(1), 85-114.

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, 26(4), 675-694.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), 60-67

Clemen, R. T. (1996). *Making Hard Decisions: An Introduction to Decision Analysis* (2nd edition). Belmont, CA: Duxbury Press.

Coleman, J. S. (1986). Social Theory, Social Research, and a Theory of Action, *American Journal of Sociology,* 91(6), 1309-1335.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23(5), 401-417.

Connor, B. T., & Doan, L. (2021). Government and corporate surveillance: moral discourse on privacy in the civil sphere. *Information, Communication & Society*, 24(1), 52-68.

Cooper, M. R., Morgan, B. S., Foley, P. M., & Kaplan, L. B. (1979). Changing employee values: deepening discontent? *Harvard Business Review TA*, 57(1).

Coughlan, R. (2005). Codes, Values and Justifications in the Ethical Decision-Making Process, *Journal of Business Ethics* 59(1-2), 45-53.

Cranor, L. F. (2003). P3P: Making privacy policies more useful. *Security & Privacy, IEEE*, 1(6), 50-55.

Crossler, R. E., & Bélanger, F. (2019). Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. *Information Systems Research*, 30(3), 995-1006.

Culnan, M. (1993). How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3), 341-363.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, 33(4), 673-687.

Cupach, W. & B. Spitzberg (1998) 'Obsessive Relational Intrusion and Stalking', in B. Spitzberg and W. Cupach (eds) The Dark Side of Close Relationships, pp. 233–63. Hillsdale, NJ: Erlbaum.

Cupach, W. & B. Spitzberg (2001) Obsessive Relational Intrusion: Incidence, Perceived Severity, and Coping, *Violence and Victims* 15(1), 1–16.

Dalvi-Esfahani, M., Ramayah, T., and Rahman, A. A. (2017). Moderating Role of Personal Values on Managers' Intention to Adopt Green II, *Industrial Management & Data Systems* 117(3), 582-604.

Davis, M. S. (1971). That's Interesting! Towards a Phenomenology of Sociology and a Sociology of Phenomenology, *Philosophy of the Social Sciences* 1(2), 309-344.

Davis, M. S. (1986). That's Classic! The Phenomenology and Rhetoric of Successful Social Theories, *Philosophy of the Social Sciences* 16(3).

Derlega, V. J., and Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, 33(3), 102-115.

Dhillon, G. (1995). Interpreting the management of Information Systems Security. PhD Thesis. London School of Economics, UK.

Dhillon, G. S. (2002). Social responsibility in the information age: issues and controversies. Hershey, Pennsylvania; London, Idea Group Pub.

Dhillon, G. & R. Chowdhuri (2013). Individual values for protecting identity in social networks. *Thirty Fourth International Conference on Information Systems*. Dec 15-18. Milan, Italy.

Dhillon, G. & Torkzadeh G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal* 16(3), 293–314.

Dhillon, G., & Kolkowska, E. (2011). *Can a Cloud Be Really Secure? A Socratic Dialogue*. In Computers, Privacy and Data Protection: an Element of Choice, 345-360.

Dhillon, G., & Smith, K. J. (2019). Defining objectives for preventing cyberstalking. *Journal of Business Ethics*, 157(1), 137-158.

Dhillon, G., and May, J. (2006). Interpreting Security in Human-Computer Interactions. A Semiotic Analysis, in *Human-Computer Interaction and Management Information Systems: Foundations,* P. Zhang and D. Galletta (eds.). Armonk: New York: M E Sharpe, pp. 281-291.

Dhillon, G., Oliveira, T., & Syed, R. (2018). Value-based information privacy objectives for Internet Commerce. *Computers in Human Behavior*, 87(October), 292-307.

Dhillon, G., Oliveira, T., Susarapu, S., and Caldeira, M. 2016. "Deciding between Information Security and Usability: Developing Value Based Objectives," *Computers in Human Behavior* 61(August), 656-666.

Dimock, M. (2019). Defining generations: Where Millennials end and Generation Z begins. Pew Research Center, 17(1), 1-7.

Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, 29(6), 1–19.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti C., (2006) Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389-402

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research*, 26(4), 639-655.

Dinev, T., Xu, H., and Smith, H.J., (2009) Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy, Proceedings of the 42nd Hawaii International Conference on System Sciences.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295–316.

Eriksson K, Kerem, K., Nilsson, D. (2005). Customer acceptance of Internet banking in Estonia, *International Journal of Bank Marketing.* 23(2), 200-216.

Ewenstein, B., and Whyte, J. (2009). Knowledge Practices in Design: The Role of Visual Representations as 'Epistemic Objects', *Organization Studies* 30(1), 7.

Fischhoff, B. (1991). Value elicitation: Is there anything in there? *American Psychologist,* 46(8), 835.

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, 25(2), 91–109.

Fridgen, G., König, C., Häfner, L., and Sachs, T. (2016). Providing Utility to Utilities: The Value of Information Systems Enabled Flexibility in Electricity Consumption, *Journal of the Association for Information Systems* 17(8), 537-563.

Fried, C. (1968). Privacy: A Moral Analysis. *Yale Law Journal*, 77(21).

Gal-Or, E., Gal-Or, R., & Penmetsa, N. (2018). The role of user privacy concerns in shaping competition among platforms. *Information Systems Research*, 29(3), 698-722.

Gandy O., (2003) Public opinion surveys and the formation of privacy policy, *Journal of Social Issues*, 59(2) 283-299

Garfinkel, R., Gopal, R., & Thompson, S. (2007). Releasing individually identifiable microdata with privacy protection against stochastic threat: An application to health information. *Information Systems Research*, 18(1), 23-41.

Gerlach, J. P., Eling, N., Wessels, N., & Buxmann, P. (2019). Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy. *Information Systems Journal*, 29(2), 548-575.

Gholami, R., Watson, R. T., Molla, A., Hasan, H., and Bjørn-Andersen, N. (2016). Information Systems Solutions for Environmental Sustainability: How Can We Do More? *Journal of the Association for Information Systems* 17(8), 521.

Ghoshal, A., Hao, J., Menon, S., & Sarkar, S. (2020). Hiding Sensitive Information when Sharing Distributed Transactional Data. *Information Systems Research*, 31(2), 473-490.

Gibson, J. J. (1986). The Ecological Approach to Visual Perception. *Hills-Dale*, NJ: Lawrence.

Giddens, A. (1984). The Constitution of Society. Berkeley. CA: University of California Press.

Gillon, K., Branz, L., Culnan, M., Dhillon, G., Hodgkinson, R., & MacWillson, A. (2011). Information security and privacy—rethinking governance models. *Communications of the Association for Information Systems*, 28(1), 33.

Gioia, D. A., and Pitre, E. (1990). Multiparadigm Perspectives on Theory Building. *Academy of Management Review* 15(4), 584.

Goodhue, D.L., and Straub, D.W. (1991) Security concerns of system users: a study of perceptions of the adequacy of security, *Information and Management*, 20(1), 13-27.

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E., & Zhdanov, D. (2018). How much to share with third parties? User privacy concerns and website dilemmas. *MIS Quarterly*, 42(1), 143-164.

Gopalakrishnan, A. (2009). Cloud computing identity management. SETLabs briefings, 7(7), 45-54.

Gottwalt, S., Ketter, W., Block, C., Collins, J., and Weinhardt, C. (2011). Demand Side Management—a Simulation of Household Behavior under Variable Prices, *Energy Policy* 39(12), 8163-8174.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: a conceptual framework. *Information Systems Journal*, 25(6), 579-606.

Greenaway, K.E., and Chan, Y.E., (2005) Theoretical Explanations for Firms' Information Privacy Behaviors, *Journal of the Association for Information Systems* 6(6) 171-198.

Gregory, R. & Keeney, R. L. (1994). Creating policy alternatives using stakeholder values. *Management Science,* 40(8), 1035–1048.

Guo, KH, Yu, X. (2020). The anonymous online self: Toward an understanding of the tension between discipline and online anonymity. *Information Systems Journal*, 30(1) 48– 69.

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, 30(2), 220-269.

Hambrick, D. C. (2007). The Field of Management's Devotion to Theory: Too Much of a Good Thing? *Academy of Management Journal*, 50(6), 1346-1352.

Hann, I., Hui, K., Lee S., and Png, I., (2007) Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach, *Journal of Management Information Systems*, 24(2), 13-42

Hedström, K., et al., (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems,* 20(4) 373-384.

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 38(2/3), 472-484.

Hernandez, J. M. C., Mazzon, J. A. (2007). Adoption of Internet banking: proposition and implementation of an integrated methodology approach, *International Journal of Bank Marking*. 25(2),72-88.

Hirschheim, R., & Klein, H. K. (2012). A Glorious and Not-So-Short History of the Information Systems Field. *Journal of the Association of Information Systems*, 13(4), 188–235.

Hoffman, D., Novak T., and Peralta, M., (1998) Building consumer trust online, *Communications of the ACM*, 42(4).

Hoffman, D.L. and Novak, T.P. (1997), A New Marketing Paradigm for Electronic Commerce, *The Information Society: An International Journal*, 13(1), 43-54.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 1(March), 275-298.

Hu, T., Dai, H., and Salam, A. F. (2019). Integrative Qualities and Dimensions of Social Commerce: Toward a Unified View, *Information & Management,* 56(2), 249-270.

Hui, K., Teo, H., and Lee, S., (2007) The Value of Privacy Assurance: An Exploratory Field Experiment, *MIS Quarterly*, 31(1), 19-33.

Hunter, M. G. (1997). The use of RepGrids to gather data about information systems analysts. *Information Systems Journal,* 7(1), 67-81.

Hutchby, I. (2001). Technologies, Texts and Affordances, *Sociology* 35(2), 441-456.

Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, 7(5), 95-107.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note - privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 24(3), 579-595.

Johnson, D. G. (2015). Technology with no human responsibility? *Journal of Business Ethics*, 127(4), 707-715.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), 387–402.

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, 58(9), 697-720.

Kahneman, D., & Lovallo, D. (1993). Timid choices and bold forecasts: A cognitive perspective on risk taking. *Management Science*, 39(1), 17-31.

Kahneman, D., & Tversky, A. (1982). The psychology of preferences. *Scientific American*, 246(1), 160-173.

Kapoor, G., Zhou W., and Piramuthu S. (2009) Challenges associated with RFID tag implementations in supply chains. *European Journal of Information Systems*, 18(6), 526-533

Karjoth, G., Schunter, M., & Waidner, M. (2002). Platform for enterprise privacy practices: Privacy-enabled management of customer data. In *International Workshop on Privacy Enhancing Technologies* (p. 69-84). Springer, Berlin, Heidelberg.

Karjoth, G., Schunter, M., & Waidner, M. (2002). Privacy-enabled services for enterprises. In *Proceedings. 13th International Workshop on Database and Expert Systems Applications* (p. 483-487). IEEE.

Katzan Jr, H. (2011). On the privacy of cloud computing. *International Journal of Management & Information Systems*, 14(2), 1-12.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE*, *7*(4), 61-64.

Kazancoglu, Y., Kazancoglu, I., and Sagnak, M. (2018). Fuzzy Dematel-Based Green Supply Chain Management Performance. *Industrial Management & Data Systems* (118)2, 412-431.

Keeney, R. L. (1988), Structuring objectives for problems of public interest. *Operations Research* 36(3), 396–405.

Keeney, R. L. (1992). *Value-focused thinking: a path to creative decision-making*. Cambridge, Mass.: Harvard University Press.

Keeney, R. L. (1993). Creativity in MS/OR: Value-Focused Thinking—Creativity Directed toward Decision Making. *Interfaces*, 23(3), 62–67.

Keeney, R. L. (1994). Creativity Decision Making with Value-Focused Thinking. *Sloan Management Review/Summer*. 35(4), 33–41.

Keeney, R. L. (1996). Value-focused thinking: Identifying decision opportunities and creating alternatives. *European Journal of Operational Research*, 92(3), 537-549.

Keeney, R. L. (1996). *Value-Focused Thinking*. Harvard University Press.

Keeney, R. L. (1999). The Value of Internet Commerce to the Customer. *Management Science*, 45(4), 533–542.

Keeney, R. L. (2004). Making better decision makers. *Decision Analysis* 1(4), 193–204.

Keeney, R. L. and Raiffa, H. (1993). Decisions with Multiple Objectives. Cambridge, Massachusetts, Cambridge University Press.

Keeney, R., (2001). Modeling Values for Telecommunications Management. *IEEE Transactions on Engineering Management*, 48(3), 370-379.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), 607-635.

Keil, M., Park, E. H., & Ramesh, B. (2018). Violations of health information privacy: The role of attributions and anticipated regret in shaping whistle-blowing intentions. *Information Systems Journal*, 28(5), 818-848.

Keim, G. D. (1978). Corporate Social Responsibility: An Assessment of the Enlightened Self-Interest Model, *Academy of Management Review* (3)1, 32-39.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, 25(6), 637-667.

Kennedy, E. H., Beckley, T. M., McFarlane, B. L., and Nadeau, S. (2009). Why We Don't" Walk the Talk": Understanding the Environmental Values/Behaviour Gap in Canada, *Human Ecology Review*, 16(2), 151-160.

Kennedy, H., Elgesem, D., & Miguel, C. (2017). On fairness: User perspectives on social media data mining. *Convergence*, 23(3), 270-288.

Kim, S. H., & Kwon, J. (2019). How Do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information? *Information Systems Research*, 30(4), 1184-1202.

Kim, Y. (2011). The pilot study in qualitative inquiry: Identifying issues and learning lessons for culturally competent research. *Qualitative Social Work*, 10(2), 190-206.

Kirkwood, Craig W. (1997). Strategic Decision Making, Multiobjective Decision Analysis with Spreadsheets. Belmont: Wadsworth Publishing Company.

Kleppner, D., Sharp, P., Berger, M. A., Bradburn, N. M., Brauman, J., Chayes, J. T., ... & Arbor, S. (2009). Committee on Ensuring the Utility and Integrity of Research Data in a Digital Age. National Academy of Sciences, 4.

Kling, R. (1996). *Computerization and Controversy: Value Conflicts and Social Choices* (2nd ed.). San Diego, CA: Academic Press.

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research*, 126(March), 221-238.

Krebs, P., & Duncan, D. T. (2015). Health app use among US mobile phone owners: a national survey. *JMIR mHealth and uHealth*, 3(4), e101.

Kubli, M., Loock, M., and Wüstenhagen, R. (2018). The Flexible Prosumer: Measuring the Willingness to Co-Create Distributed Flexibility, *Energy Policy* (114), p. 540.

Kuhn, T. S. (1970). *The Structure of Scientific Revolutions*, (Second edition, enlarged. ed.). Chicago: University of Chicago Press.

Lagoze, C. (2014). Big Data, data integrity, and the fracturing of the control zone. *Big Data & Society*, 1(2),

Leavitt, N. (2009). Is cloud computing really ready for prime time. *Growth*, 27(5).

Lee, A. S. (2004). Thinking About Social Theory and Philosophy for Information Systems, *Social Theory and Philosophy for Information Systems* (1)26.

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.

Leonardi, P. M. (2011). When Flexible Routines Meet Flexible Technologies: Affordance, Constraint, and the Imbrication of Human and Material Agencies, *MIS Quarterly* (35)1, 147-167.

Leonardi, P. M., and Barley, S. R. (2010). What's under Construction Here? Social Action, Materiality, and Power in Constructivist Studies of Technology and Organizing, *Academy of Management Annals* (4)1, 1-51.

Leonardi, P. M., and Rodriguez-Lluesma, C. (2012). Sociomateriality as a Lens for Design, *Scandinavian Journal of Information Systems* (24)2, 79-88.

Lewis, M. W., and Grimes, A. J. (1999). Metatriangulation: Building Theory from Multiple Paradigms, *The Academy of Management Review* (24)4, 672-690.

Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, 21(6), 621–642.

Li, X. B., & Qin, J. (2017). Anonymizing and sharing medical text records. *Information Systems Research*, 28(2), 332-352.

Li, X. B., & Sarkar, S. (2006). Privacy protection in data mining: A perturbation approach for categorical data. *Information Systems Research*, 17(3), 254-270.

Li, X. B., & Sarkar, S. (2011). Protecting privacy against record linkage disclosure: A bounded swapping approach for numeric data. *Information Systems Research*, 22(4), 774-789.

Li, X. B., & Sarkar, S. (2014). Digression and value concatenation to enable privacy-preserving regression. *MIS Quarterly*, 38(3), 679.

Liebenau, J., and Backhouse, J. (1990). *Understanding Information*. Basingstoke: Macmillan.

Lincoln, Y. S. (1985). *Organizational Theory and Inquiry: The Paradigm Revolution*. Beverly Hills: Sage Publications.

Liu, Z, Wang, X, Min, Q, Li, W. (2019). The effect of role conflict on self-disclosure in social network sites: An integrated perspective of boundary regulation and dual process model. *Information Systems Journal*, 29(2), 279–316.

Locke, E. A. (2007). The Case for Inductive Theory Building, *Journal of Management* (33)6, 867-890.

Louis, M. R., & Sutton, R. I. (1991). Switching cognitive gears: From habits of mind to active thinking. *Human Relations*, 44(1), 55-76.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems*, 26(6), 546–563.

Lu, H., Hong, Y., Yang, Y., Duan, L., & Badar, N. (2015). Towards user-oriented RBAC model. *Journal of Computer Security*, 23(1), 107-129.

Lüscher, L. S., and Lewis, M. W. (2008). Organizational Change and Managerial Sensemaking: Working through Paradox, *Academy of Management Journal* (51)2, 221.

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. In *Data Politics: Worlds, Subjects, Rights.* Eds Didier Bigo, Engin Isin, and Evelyn Ruppert Abingdon: Routledge, 64-77.

Mai, B., Menon, N., and Sarkar, S., (2010) No Free Lunch: Price Premium for Privacy Seal-Bearing Vendors, *Journal of Management Information Systems*, (27)2, 189-212

Malhotra, A., Melville, N. P., and Watson, R. T. (2013). Spurring Impactful Research on Information Systems for Environmental Sustainability, *MIS Quarterly* 37(4), 1265-1274.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.

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

Margulis, S. T. (2003). Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*. Vol. 59(2), 243-261.

Margulis, S. T., (1977). Conceptions of Privacy, Current Status and Next Steps. *Journal of Social Issues*. Vol. 33(3), 5-21.

Marx, K. (1973). *Karl Marx on society and social change: With selections by Friedrich Engels*. University of Chicago Press.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176-189.

Martin, J. (1988). Organizational Culture and the Denial, Channeling, and Acknowledgement of Ambiguity. In L.R. Pondy, R.J. Boland, Jr., and H Thomas (Eds), *Managing ambiguity and change*, John Wiley, New York.

Martin, J. (2002). *Organizational Culture: Mapping the Terrain*. Thousand Oaks: Sage Publications.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 10(1), 5-12.

May, J., Dhillon, G., & Caldeira, M. (2013). Defining value-based objectives for ERP systems planning. *Decision Support Systems*, 55(1), 98–109. 036

Meglino, B. M., Ravlin, E. C., and Adkins, C. L. (1989). A Work Values Approach to Corporate Culture: A Field Test of the Value Congruence Process and Its Relationship to Individual Outcomes, *Journal of Applied Psychology* (74)3, 424.

Melville, N., & McQuaid, M. (2012). Research Note - Generating Shareable Statistical Databases for Business Value: Multiple Imputation with Multimodal Perturbation. *Information Systems Research*, 23(2), 559-574.

Menon, S., & Sarkar, S. (2016). Privacy and Big Data: Scalable Approaches to Sanitize Large Transactional Databases for Sharing. *MIS Quarterly*, 40(4), 963-982.

Menon, S., Sarkar, S., & Mukherjee, S. (2005). Maximizing accuracy of shared databases when concealing sensitive patterns. *Information Systems Research*, 16(3), 256-270.

Merrick, J. R. W., Parnell, G. S., Barnett, J., & Garcia, M. (2005). A Multiple-Objective Decision Analysis of Stakeholder Values to Identify Watershed Improvement Needs. *Decision Analysis*, 2(1), 44–57.

Merrick, J. R., & Garcia, M. W. (2004). Using value-focused thinking to improve watersheds. *Journal of the American Planning Association*, 70(3), 313–327.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), 65-74.

Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), 65-74.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, 23(2), 103–125.

Mishra, S. & Dhillon G. (2008). Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment. *European Conference on Information Systems.* p. 1334–1345.

Mitroff, I. I., and Silvers, A. 2009. *Dirty Rotten Strategies: How We Trick Ourselves and Others into Solving the Wrong Problems Precisely*. Stanford, Calif.: Stanford University Press.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of Internal Medicine*, 151(4), 264-269.

Moores, T., and Dhillon, G., (2003) Do privacy seals in e-commerce really work? *Communications of the ACM*, Vol. 46(12).

Morgan, G. (1980). Paradigms, Metaphors, and Puzzle Solving in Organization Theory, *Administrative Science Quarterly* (25)4, 605.

Morgan, G. (1997). *Images* of Organization, (2nd ed.). Thousand Oaks, Calif.: Sage Publications.

Morgan, G., and Smircich, L. (1980). The Case for Qualitative Research, *The Academy of Management Review* (5)4, 491-500.

Morris, C., (1956). *Varieties of Human Values*. Chicago: Chicago University Press.

Musson, G., and Tietze, S. (2004). Places and Spaces: The Role of Metonymy in Organizational Talk, *The Journal of Management Studies* (41)8, 1301-1323.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79 (1), 119–158.

Nunes, S., Dhillon, G., & Caldeira, M. (2015). Value Focused Approach to Information Systems Risk Management. Conferência da Associação Portuguesa de Sistemas de Informação, (15)15, 103-115.

Ogbanufe, O., & Gerhart, N. (2018). Watch it! Factors driving continued feature use of the smartwatch. *International Journal of Human–Computer Interaction*, 34(11), 999-1014.

Okoli, C. & Pawlowski, S.D. (2004). The Delphi method as a research tool: an example, design considerations and applications, *Information & Management*. 42(1) 15–29.

Orlikowski, W. J. (2007). Sociomaterial Practices: Exploring Technology at Work, *Organization Studies* (28)9, 1435-1448.

Orlikowski, W. J., and Gash, D. C. (1994). Technological Frames: Making Sense of Information Technology in Organizations, *ACM Transactions on Information Systems (TOIS)* (12)2, 174-207.

Orlikowski, W. J., Yates, J., Okamura, K., and Fujimoto, M. (1995). Shaping Electronic Communication: The Metastructuring of Technology in the Context of Use, *Organization Science* (6)4, 423-444.

Orlikowski, W.J., Robey, D. (1991) Information technology and structuring of organizations. *Information Systems Research*, 2(2), 143-169.

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, 26(6), 642–660.

Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs*, 12, 269-288.

Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems*, 26(1), 37–65.

Parnell, G. S., Conley, H. W., Jackson, J. A., Lehmkuhl, L. J., and Andrew, J. M. (1998). Foundations 2025: A value model for evaluating future air and space forces. *Management Science,* 44(10), 1336-1350.

Parnell, G. S., Driscoll, P. J., and Henderson, D. L. (2011). *Decision Making in Systems Engineering and Management*. John Wiley & Sons.

Parrish, J. L. (2010). PAPA knows best: Principles for the ethical sharing of information on social networking sites. *Ethics and Information Technology*, 12(2), 187-193.

Parsons, T. (1951). *The Social System*. NY: Free Press. 575 pp.

Parsons, T., and Shils, E. A. (1951). Values, Motives, and Systems of Action, *Toward a general Theory of Action*, 33, 247-275.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 35(4), 977-988.

Pavlou, P., Liang, H., and Xue, Y., (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective, *MIS Quarterly*, (31)1, 105-136

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 693-702). IEEE.

Pearson, S., & Charlesworth, A. (2009, December). Accountability as a way forward for privacy protection in the cloud. In *IEEE international conference on cloud computing*(pp. 131-144). Springer, Berlin, Heidelberg.

Peto, J., Fletcher, O., & Gilham, C. (2004). Data protection, informed consent, and research. *British Medical Journal. 328*(7447), 1029-1030

Phythian, G. J., & King, M. (1992). Developing an Expert System for tender enquiry evaluation: a case study. *European Journal of Operational Research,* 56(1), 15-29.

Popper, K. (2005). *The Logic of Scientific Discovery*. Routledge.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems*, 19(2), 181–195.

Posner, B. Z., & Munson, J. M. (1979). The Importance of Values in Organizational Behavior. *Human Resource Management*, 18(3), 9–15.

Post, R. C. (1989). The social foundations of privacy: community and self in the common law tort. *California Law Review*, 77, 957-1010.

Pötzsch, S. (2008, September). Privacy awareness: A means to solve the privacy paradox? In IFIP Summer School on the Future of Identity in the Information Society (pp. 226-236). Springer, Berlin, Heidelberg.

Pramatari, K., and Theotokis, A., (2009) Consumer acceptance of RFID-enabled services: a model of multiple attitudes, perceived system characteristics and individual traits, *European Journal of Information Systems*, 18(6), 541-552.

Prosser, W., (1960). Privacy. *California Law Review*. Vol. 48(3), 383-423.

Pym, D., & Sadler, M. (2010). Information Stewardship in cloud computing. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)*, 1(1), 50-67.

Rai, A. (2017). Avoiding Type II Errors: Formulating Is Research Problems That Matter," *MIS Quarterly*, 41(2), iii-vii.

Raiborn, C. A., and Payne, D. (1990). Corporate Codes of Conduct: A Collective Conscience and Continuum, *Journal of Business Ethics* 9(11), 879-889.

Raiffa, H. (1968). *Decision Analysis; Introductory Lectures on Choices under Uncertainty*. Reading, Mass.: Addison-Wesley.

Reichheld, F., and Schefter, P., (2000) E-Loyalty: Your Secret Weapon on the Web, *Harvard Business Review*, 78(4), 105.

Reiman, J. H. (1976). Privacy, intimacy, and personhood. *Philosophy & Public Affairs*, 26-44.

Richards, N.M. and D. J. Solove, (2010) Prosser's Privacy Law: A Mixed Legacy. *California Law Review*, 98(6), 1887

Ritchie, J., Lewis, J., Nicholls, C. M., and Ormston, R. 2013. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. Sage.

Roberts, M. E., Stewart, B. M., & Tingley, D. (2019). STM: An R package for structural topic models. *Journal of Statistical Software*, 91(1), 1-40.

Rogers, E.M. (1995). *Diffusion of innovations*. (4th ed.) New York: The Free Press.

Rokeach, M. (1973). *The Nature of Human Values*. Free press.

Rokeach, M., & Ball-Rokeach, S. J. (1989). Stability and change in American value priorities, 1968–1981. *American Psychologist*, 44(5), 775.

Rosen, J. (2011). *The unwanted gaze: The destruction of privacy in America*. Vintage.

Rosenbaum, S. (2010). Data governance and stewardship: designing data stewardship entities and advancing data access. *Health Services Research*, 45(5), 1442-1455.

Saaty, T. (1980). The Analytical Hierarchy Process. NY, NY, McGraw-Hill, International.

Sandhu, R., & Samarati, P. (1996). Authentication, access control, and audit. *ACM Computing Surveys (CSUR)*, 28(1), 241-243.

Sassen, S. (2006). *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton, NJ: Princeton University Press.

Schmidt, R.C. (1997). Managing Delphi surveys using nonparametric statistical techniques, *Decision Sciences* 28 (3) 763–774.

Selart, M., and Johansen, S. T. (2011). Understanding the Role of Value-Focused Thinking in Idea Management. *Creativity and Innovation Management*, 20(3), 196-206.

Selznick, P. (1984). *Leadership in Administration. A sociological interpretation*. University of California Press.

Sheng, H., K, & Nah, F. F.-H. (2010). 'Understanding the values of mobile technology in education: a value-focused thinking approach'. *ACM SIGMIS Database* 41(2), 25–44.

Shih, H., Lai, K., & Cheng, T. C. E. (2017). Constraint-based and dedication-based mechanisms for encouraging online self-disclosure: Is personalization the only thing that matters? *European Journal of Information Systems,* 26(4), 432–450.

Shin SK, Ishman M and Sanders GL (2007) An empirical investigation of socio-cultural factors of information sharing in China. *Information & Management*. 44(2), 165-174.

Slater, S. F. (1997). Developing a customer value-based theory of the firm. *Journal of the Academy of Marketing Science*, *25*(2), 162–167.

Smircich, L. (1983). Concepts of Culture and Organizational Analysis, *Administrative Science Quarterly* 28(3), 339-358.

Smith H. J., (1993) Privacy policies and practices: inside the organizational maze, *Communication of the ACM*, Vol. 36(12), 104-122.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015.

Smith, H.J., Milberg, S.J., and Burke, S.J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices, *MIS Quarterly*, 20(2), 167-195

Solove, D.J., (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*. Vol. 154(3), 47-560.

Son, J., and Kim, S., (2008) Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model, *MIS Quarterly*, 32(3), 503-529

Sotto, L. J., Treacy, B. C., & McLellan, M. L. (2010). Privacy and Data Security Risks in Cloud Computing. *World Communications Regulation Report*, 5(2), 38.

Spates, J. L. (1983). The sociology of values. *Annual Review of Sociology*, 9(1), 27-49.

Spitzberg, B. & Rhea, J. (1999) 'Obsessive Relational Intrusion and Sexual Coercion Victimization', *Journal of Interpersonal Violence* 14(1), 3–20.

Spitzberg, B., Marshall, L. & Cupach, W. (2001) 'Obsessive Relational Intrusion, Coping, and Sexual Coercion Victimization', *Communication Reports* 14(1), 19–30.

Spitzberg, B., Nicastro, A. & Cousins, A. (1998) 'Exploring the Interactional Phenomenon of Stalking and Obsessive Relational Intrusion', *Communication Reports* 11(1), 33–48.

Stamper, R. K. (1973). *Information in Business and Administrative Systems*. New York: John Wiley & Sons.

Stanovich, K. E., West, R. F., & Toplak, M. E. (2013). Myside bias, rational thinking, and intelligence. *Current Directions in Psychological Science*, 22(4), 259-264.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49.

Stone, E.F., Gardner, D.G., Gueutal, H.G., and McClure, S. (1983) A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psycholo*gy. 68(3), 459–468.

Straub, D., and Collins, R.W., (1990) Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy, *MIS Quarterly*, 14(2), 143-156

Strengers, Y. (2012). Peak Electricity Demand and Social Practice Theories: Reframing the Role of Change Agents in the Energy Sector, In *The Global Challenge of Encouraging Sustainable Living*, Ed. Shane Fudge, Michael Peters, Steven M. Hoffman, and Walter Wehrmeyer. Edward Elgar Publishing, 18-42.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11.

Suchman, L. (2007). *Human-Machine Reconfigurations: Plans and Situated Actions*. Cambridge University Press.

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, 37(4), 1141-1164.

Syed, R., Dhillon, G., & Merrick, J. (2019). The identity management value model: A design science approach to assess value gaps on social media. *Decision Sciences*, 50(3), 498-536.

Tan, F. B., and Hunter, M. G. (2002). The Repertory Grid Technique: A Method for the Study of Cognition in Information Systems, *MIS Quarterly*, 26(1). 39-57.

Tang, Z., Hu, Y., and Smith, M. (2008) Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor, *Journal of Management Information Systems*, (24)4, 153-173

Thomson, K. L., & von Solms, R. (2006). Towards an information security competence maturity model. *Computer Fraud & Security*, 5(May), 11-15.

Thornborrow, T., and Brown, A. D. (2009). Being Regimented: Aspiration, Discipline and Identity Work in the British Parachute Regiment, *Organization Studies* 30(4), 355.

Torkzadeh, G., and Dhillon, G. (2002). Measuring Factors That Influence the Success of Internet Commerce, *Information Systems Research,* 3(2),187-204.

Trang, S., Trenz, M., Weiger, W. H., Tarafdar, M., & Cheung, C. M. K. (2020). One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, 29(4), 415–428.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254-268.

Tsohou, A., & Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology & People*. 31(5), 1047-1068.

Valogianni, K., and Ketter, W. (2016). Effective Demand Response for Smart Grids: Evidence from a Real-World Pilot, *Decision Support Systems*, 91(November), pp. 48-66.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management science*, 46(2), 186-204.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, 24(1), 115-140.

Vom Brocke, J., Loos, P., Seidel, S., and Watson, R. T. (2013). Green IS. Information Systems for Environmental Sustainability, *Wirtschaftsinf* 55, 295–297

Vroom, V. H. (1964). Work and Motivation, *NY: John Wiley & Sons*.

Walsham, G. (1995) Interpretive case studies in IS research: nature and method. *European Journal of Information Systems* 4(2), 74-81.

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-preserving public auditing for data storage security in cloud computing. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE.

Wang, H, Lee, M, and Wang, C. (1998). Consumer Privacy Concerns About Internet Marketing, *Communications of the ACM*, 41(3), 63-70.

Wang, Y. S., Lin, H. H., & Luarn, P. (2006). Predicting consumer intention to use mobile service. *Information Systems Journal*, 16(2), 157-179.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20(3), 267–284.

Warner, R. S. (1978). Toward a Redefinition of Action Theory: Paying the Cognitive Element Its Due, *American Journal of Sociology* 83(6), 1317-1349.

Warren, C., and Laslett, B. (1977). Privacy and secrecy: A conceptual comparison. *Journal of Social Issues*, 33(3), 43-51.

Warren, S. D., and Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

Watson, R. T., Boudreau, M.-C., and Chen, A. J. (2010). Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community, *MIS Quarterly*, 34(1), 23-38.

Watson, R., Atkinson, I. & Rose, K. (2007) Editorial: Pilot Studies: To Publish or Not? *Journal of Clinical Nursing*, 16(4):619-620

Wattal, S., Telang, R., Mukhopadhyay, T., & Boatwright, P. (2012). What's in a "name"? Impact of use of customer information in e-mail advertisements. *Information Systems Research*, 23(3), 679-697.

Wei, C.-C. (2008). Evaluating the performance of an ERP system based on the knowledge of ERP implementation objectives. *The International Journal of Advanced Manufacturing Technology,* 39(1-2), 168-181.

Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM*, 10(9), 533-537.

Westin, A., (1967). *Privacy and Freedom*. New York: Antheneum.

Westphal, J. D., and Khanna, P. (2003). Keeping Directors in Line: Social Distancing as a Control Mechanism in the Corporate Elite, *Administrative Science Quarterly* 48(3), 361-398.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note - effects of individual self-protection, industry self-regulation, and government regulation on privacy

concerns: a study of location-based services. *Information Systems Research*, 23(4), 1342-1363.

Xu, H., Teo, H., Tan B., and Agarwal, R., (2009) The role of push-pull technology in privacy calculus: The case of location-based services, *Journal of Management Information Systems* 26(3), 135-173.

Yankelovich, D. (1978). The New Psychological Contracts at Work. *Psychology Today*, 11(12), 46.

Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal*, 30(5), 791-844.

Zuboff, S (2019) *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior*, 8, 53–111.

# Appendix

The appendix includes all the interview data, coding and analysis.

Interview 1

I am a little concerned but more for the awkwardness or how stupid I would look if someone looked through my search history, I am less concerned when on my phone since it says when the camera or speaker is being used so I feel like I have more control and trust my phone more than my laptop. I feel the most concerned whenever I see advertisements for things, I was talking about but never searched with on my computer or phone.

I would like to be able to filter who can view my profile, be able to automatically filter spam accounts that message me without having to make an executive decision especially if it's an account messaging me for the first time with a link. Also, to be able to choose what they have access to straight away such as Instagram having access to the camera and microphone but only when taking a picture/video or when sending a voice note.

Morals of keeping data limited to myself and only the company as it is becoming increasingly worrying such as with Facebook where there has been breaches in data, truth in what happens with my data such as any sharing and the option to easily access where my data and to who it is being shared to. Transparent communication if my data has been breached as I would be more grateful in finding out from the company than finding out from a news outlet.

I see if my data will be shared with third party apps/companies that are not relevant to the site that I am on, also through personal experience not sharing information through google docs for raffles as I have seen an increase in spam emails, also I try to see if it will impact my future employment if anything that I do will hold me back from progressing my career. Also, I look at if I would be happy with my information being shared such as pictures by looking to see if it will impact me in the future, this can be if anything can be used against me when applying for a job opportunity or even if it pictures me in a bad light in any way as that can all be used

against me in the future, I also assess if it’s something i would share with friends in person or not as it is a clear indicator if that’s an appropriate bit of information to share

Interview 2

I am in terms of what I post and who can see it due to the nature of my profession. Good reputation and social standing are important in my profession so I must not have anything on my accounts that can discredit the profession. I also worry about my browser history and my carbon footprint as nothing is ever really deleted online. Email privacy was a huge one but since the new data protection laws this is not much of a concern.

It would be ideal to be able to choose who can see what and who can access your account. It would also be ideal to be able to see what your profile looks like to the public, e.g. people you are not friends with. Facebook offers this feature, so it is easy to monitor this, but Instagram does not as of yet. It would also be good if all websites did not need access to cookies as this affects browsing on every website.

I am quite lax with my privacy online and always accept all cookies and such. My personal rule is don't post anything I would be embarrassed of or that could embarrass someone else. I also make sure that I don't post anything that I would not want the people in my life knowing, meaning only the people close to me have an all-access pass to my life and my online presence. I also try not to enter my email into sites which I am not familiar with to avoid consistent emails.

I look at what I would think if someone else posted it, I look at what potential employers may think, I look at how it may make others feel and I look at it is necessary to share this part of my life online. If the website does not seem legit or if the entering of personal information seems unnecessary then I do not do it to protect my privacy from potentially unreliable sources.

I literally just answered this question on the last slide so I will say the same answer here. Risks and benefits go hand in hand when looking at privacy online. If the benefits such as subscription services, job applications, cookies for better browsing outweigh the risk I said in my previous answer then that’s how I weigh them to ascertain how I share my privacy online.

Interview 3

I have most of my social media private and only accept friendship/follow from people I know, and I also report and block people that seem sketchy. I also block bot accounts and most accounts like that because they're not trustworthy, as well as porn accounts because they might steal my photos or something like that. Also, racist, misogynist, homophobic, transphobic, xenophobe, and overall people that don't respect others deserve a block and report because they're potential danger not only to me but also others that fit at least one of the categories mentioned above.

The ideal situation and position to have on social media such as Facebook, Instagram, twitter, Tumblr, etc. would be to only interact and allow access to what you post with people that you know and trust, which doesn't happen most of the time.

My individual values concerning my privacy online consist of trying my best to keep trustworthy, nice people whom I know and know that do me good and make me feel good not only about myself but also about society and the world.

I never share private stuff, always try to be lowkey voicing my interests and nice stuff but never compromising my safety and privacy. I always stop and think if it will compromise my safety and privacy, if it might turn out to be a problem I won't share it. I also never share private stuff, I just voice/share my interests vaguely and superficially.

My main privacy concerns when it comes to privacy is my personal data being hacked. In more detail, I fear that someone can steal my banking details and steal my money. After that, it's stealing my personal info to impersonate me on social media, or even manipulate my public photos to look like private photos and spread them around the internet. Every day I end hearing about a new leak or a new scam on the internet that actually makes me want to delete all my internet accounts

An easy interface that allows you to manage which people see your content, and some type of security systems that prevents fake accounts to see your content. For example, when creating an account, social media should have some type of verification, to stop all the fake and bot accounts from being created, it would avoid people falling into scams or getting hacked.

I keep my social media private and still avoid posting about more personal information. I am very careful about the pictures of myself or my friends I post, and always make sure that they cannot be taken out of context or be manipulated into more inappropriate material. I never use third party apps and keep my accounts to the bare minimum required.

I actually don't even share my private information online, not even with internet friends or real friends. I've seen enough scams, news, and things going wrong to share my information. But still, even though I do not share, I'm still somewhat scared that someone is going to hack me and use that information to do not so legal and moral things and ended up controlling my life.

I weigh the risks very strongly. I have used the internet for about 10 years, and I am always on top of every scam and security situation. I do whatever is possible to be safe on the internet so, obviously, I do not share private information online, when creating account and things of that sort, I always resort to the bare minimum of information required.

Interview 4

When I use the Internet, I am not concerned that my searches are saved or that ads related to my searches are displayed. What worries me is that data such as my name, my passwords, my address, my face or that of my relatives are collected. For this reason, I avoid repeating passwords, publishing images or photos of myself or my surroundings and not providing more data than necessary. I also usually avoid pages that do not seem safe or that request to download a program.

Since I was old enough to use social networks, I have taken precautions not to show or share more than necessary, in this way I can avoid getting involved in cases of cyberbullying, kidnapping or extortion. But actually, I don't usually use these social networks for anything other than hanging out with friends, that is, I don't post anything. In addition to taking measures such as: not accepting requests from strangers and not repeating my passwords for my different accounts.

It will sound repetitive but to keep my safety before other users of the platform, I do not publish anything that may reveal places where I have been, or specific addresses, or relevant dates, or photographs where I or my family may appear, nor do I share my schedule or calendar of activities, I do not share the place where I study or in the future my work. To contact me using the networks, I must first know the person in reality.

I do not usually share my private information more than with my contacts, that information is not published for general knowledge. But to share some information from time to time with my colleagues, friends or family, generally I do not have any problem as long as it makes sense, I mean, some hour, place, names or anecdotes. In no way would I share passwords or accounts, even if it is friends or family who ask for it. With a stranger I will most likely make fun of him before avoiding him permanently.

First of all, I consider the importance of certain data, access to accounts, the emails or messages that I could receive, the money that I handle in an account, such as: PayPal, etc. Then I try to get an idea of who would want to know that data or who it could be useful to. So, I consider, why share something so important. If there is an alternative to prevent me from giving information, then I would take that alternative.

Interview 5

I don't tend to worry about my privacy much. I do what is recommended to me by service providers (Google, Samsung, etc.) to keep my information safe, but no more. My main concern is my passwords being compromised in some way, I've read other people's stories about this recently so I have been thinking about it a lot more. I've never cared much about social media sites, but I do worry about how much information they can hold about someone. A stranger could easily find out where I live and what I look like.

To keep my privacy, I use a non-identifying username that can't link back to me. I also don't use the same one for all of my social media accounts. I don't post pictures of myself or friends and family either. To keep my personal information within the sites private I make sure not to leave my password saved in devices that do not belong to me and I make sure to have 2 step verification active whenever possible. I also use the randomly generated passwords recommended by Google when creating new accounts.

I assume that " individual values" refers to things that are important to me and that guide me. I don't worry too much about certain accounts of mine being compromised because most websites have ways to help me get them back. What matters most to me is to keep my identity hidden. To keep my face and address anonymous. I am currently no one on the internet and I want it to stay that way as long as possible. I want the internet to stay away from my real life.

I hate to share my private information online, but I've noticed that I tend to do it a lot more easily in public settings such as discord groups. For example, everyone else is talking about where they live, and I don't want to be excluded so I tell them some information about me. It might be some sort of peer pressure. I tend to prioritize making others happy over my own comfort when it comes to matters such as these. I don't really think about my privacy when I am in these situations.

This question was just asked of me. Answer: I hate to share my private information online, but I've noticed that I tend to do it a lot more easily in public settings such as discord groups. For example, everyone else is talking about where they live, and I don't want to be excluded so I tell them some information about me. It might be some sort of peer pressure. I tend to prioritize making others happy over my own comfort when it comes to these things.

The thing I am most concerned about when I go online the is security of my sensitive information such as passwords and personal information. I am relying on plug-ins to block trackers and unwanted cookies, so I am not that concerned about trackers and cookies. I am also very cautious when downloading software as to not download viruses as I know how ingenious these can work these days. Therefore, I scan everything I am remotely suspicious of when downloading files.

The ideal situation to manage my privacy is to have a menu of options screen where I have a full overview of what information is visible to who including third parties and am able to block this information to certain sources as advertising companies. This way it is easy to see to who my information is visible and who is able to use this information for what goals.

Things I value the most regarding online privacy is the security of my sensitive information as I do lay may trust on third parties by letting them have my information and trusting them not to sell/share this information without my consent. I also value transparency because of the same reasons as I think third parties should be fully transparent on the way they handle your information.

I do weigh the benefits over the negatives as sharing information on the internet is almost mandatory these days, one cannot create an account of participate in social media without sharing a lot of information. Therefore, I consider if sharing information online is worth the risk of my information being leaked out / used by third parties. This also depends on the type

of information as for instance, I will be more likely to share my age for creating an account on a website than to share my address.

Interview 6

Will all the speculation it is kind of hard to not be a little concerned in regard to my privacy. I feel that sometimes my privacy is not guaranteed on social media and that is mostly expressed by the advertisements that are shown on my feed. I feel that social media does all it possibly can with our personal information to generate income and that is pretty scary to me. My concern is that this gets worse, and companies start to give out more and more information without consent!

I personally normally have two accounts. One that has more followers and more movement and another that is only for close friends of mine so that we can easily interact and show our life with "no filters". The usage of close friends, for example, on Instagram is also a good innovation for people that only would like a selected amount of people to watch their stories!

I strongly defend my privacy online and I think we should all do it too! We have the right to our own privacy, and no one can use it in their favor, whether it is economic or social, to gain more popularity. Privacy online is one of the biggest concerns in modern history and we should fight for its security, which is also our individual and collective security as a society!

I do not really think about this. I do not often see any problem and if I do, I just won't put in my details. But anything that might seem suspicious or too personal should be radically ignored for our well-being! The online world can be very dangerous, especially with our own privacy information that makes us unique and, therefore, valuable for online/social media companies.

Once again, we should always see what risks may be involved. If we find any information that any site wants us to give out to be very personal or kind of suspicious, we should reconsider giving out our information on that site. Too much information gives us exposure in a bad way, it might even make us vulnerable in regard to powerful companies that obtain such information about our privacy!

Generally speaking, I am not that concerned about my privacy. If I use an incognito tab it's more because I'd be embarrassed if people saw what I googled. I don't mind the government finding out the weird stuff I google. At least I do not mind with our current government. I understand why it would be different in a country that's stricter about what the inhabitants are allowed to google. I don't think hackers can do much with my online information, I am but a poor student.

I absolutely do not mind random people knowing my age or name or the city I live in. I wouldn't want them to have my address or full name. It would be ideal if I could share these things without having to worry about people using my information or even my pictures for evil doing. I don't think my current government can do much with the information I share online. I believe they would be able to retrieve most of the information I share online some other way anyway.

I truly don't have many individual values. I think most people of my generation are a lot more open about their lives online than generations before me. Which also means it will be less important what I've shared online once I want to get a serious job. The only thing I value is people not stalking me and people not using my pictures as if they belonged to them, if that is even part of online privacy.

I generally do not share my phone number with people, because I have bad experiences with people knowing my phone number while I did not want them to have it. I don't mind people knowing my age, first name or the city I live in. I don't share my specific address, because this would give very easy access to stalking and general weirdness. I mostly share equal amounts of personal information as the person I am talking to.

Oh, I might have miss understood the last question. Recap: the benefits are mostly friendships and being able to share my emotions with people who understand. The risks mostly have to do with catfishing and people who intend to use my own information

against me. I have certain moments during which the paranoid thoughts about this happening are worse, but generally speaking I am not too worried.

Interview 7

As a normal person I don't really concerned because I believe that being on social media or doing work for university doesn't affect my privacy. However, there is things like my location, my routines and other habits that computers can know about me that bother me that companies know. I am also afraid about how susceptible we are to information and how social media can manipulate us as they control what we do or do not see in our feed.

I would like to be sure that i can't be hacked. Using other ways of authentication reassure that. I also would like to be able to know who saves my photos (by saving or screenshot). Sometimes our posts go all around the world and I would like to really limit it to the people I want, not only on stories. Finally, I would like to know what the social media site really knows about me, what interests they think I have and the people that they think matter most to me.

I believe in control about our own data, controlling what we really share with the world and with the social media site, that we are not at risk of being hacked or having my information/posts stolen without my consent. I think the most important thing is really the security of the personal applications, like bank apps or smart home apps. Those apps have really confidential information and must be in trustworthy hands.

When it is for spending time, like social media, I don't usually share personal information, neither my phone number nor my address nor things like that. On work sites where I have to log in and share some lowkey personal information I try to make that as safe as I can. On other things like a one-time visit site or a game I don't share any information

When I spend time on social media sites, I share only the things I'm obliged to, but I avoid share my birthday, my phone number, my address, among other things. On time visit sites and games I share the lowest, barely the name, just really an email, and not even the main one. On work related websites where I have to share more personal information, I usually choose a stronger password to feel safer.

Interview 8

I am concerned about the use of images of myself online, therefore, I keep my social media profiles private. I also tend not to accept people that I do not know in real life. I also am concerned about my bank details being stolen so I avoid dodgy looking shopping websites. I also do not click on any links sent to me in spam/scam emails. Other than this, I don't really think too much about my privacy online.

For Snapchat, YouTube, Facebook and LinkedIn, I keep my accounts private and only allow access to people that I know in real life. However, when using Instagram and TikTok, I know that there is an opportunity for making money and receiving free clothing if brands like your content. Therefore, I keep these accounts more open, and I will accept people that I do not know. I do not use any other social media.

I don't really do too much except keeping my social media private and shopping wisely. I have not heard of anyone in my personal life having serious issues with a breach of privacy online, so it is not something that I worry about all that often. I would consider my physical privacy and safety to be more important because at the end of the day (aside from my bank details), if someone had access to my online profiles, I could just make new ones.

I like sharing nice pictures with my friends and family online. I see this as a benefit. However, being a social media influencer is not my job, so I do not spend too much time on this. I don't share anything other than photos of myself. I would not share my location as this could potentially affect my physical safety - which I consider to be more important.

There is a risk that people could find out your location and stalk you or rob you. But honestly the likelihood of this actually happening is so low that I don't really think about it too much and I continue to share images of myself online. I don't engage in conversations with strangers, and I block anyone that is doing anything weird as a form of protection.

Interview 9

I have some concerns and use a VPN, but I believe that this will not prevent certain information of mine from being used. Websites exchange customer information between one another, and I do not think there is much I can do about that. I try to use safe payment methods, such as PayPal, wherever I can in order to prevent websites from acquiring my bank card details. Privacy is important and I believe that there should be more transparency about what data is being collected from users online.

No one has the time to read a huge document on terms and conditions, so I wish that websites would be more transparent with what data they collect. Also, instead of giving a set of agreements which we must consent to, I wish that there were possibilities to customize the options and let the individual decide their level of privacy for themself through deciding what data they are fine with sharing and ticking boxes for this.

I have developed longer, more complicated passwords over time. I use PayPal instead of giving away my bank card details wherever I can, especially when using new websites which I may be unfamiliar with and not trust yet. I feel as though online companies and social media websites should be clearer about the information they take from users, how they personalize advertising etc.

Sharing information mostly occurs when creating new accounts on websites so, if I am interested in joining a platform, I am happy to provide some information they may require. Online shopping also requires some user information, and this may be more crucial too, but giving out some details in order to be able to carry out purchases is important to me.

When using new websites which I am unfamiliar with, I always look them up and check their validity. This happens especially when making purchases from new websites I had never used before, and I tend to check first whether they have any social media profiles for their

business and then checking their reviews on other websites. If this all seems alright, I will purchase from them.

Interview 10

I am a little bit concerned due to everything I hear all around the internet. I still think that all of us get abused online and have no idea how much information is taken from our devices. Still, I also think that I am not a target for anyone, but I am not sure. I am a software engineering student which makes me even more aware of all the dangers of the internet and it is really scary to think that some of the things I ear can be done by anyone basically. I hope I am wrong.

I do not know what would make it more private, but I would like to get some kind of briefing to those dangers by anyone that knows something about that matter. I think a lot of people that use these kinds of platforms, such as social media, don't really get the dangers around what they are doing, and the data that they are making possible to get. Hopefully someone thinks about this and helps people out

I really think it is very important to protect yourself and your privacy when you go online. You are constantly in danger and you need to prepare for that. I have tried a little bit changing some of the settings, using VPNs, and managing the platform to be as safe as possible. In spite of that I don't think I've been very successful, but I've surely done more than a lot of people, but also less than a lot of people too. I am looking forward to searching a little bit more about this subject know that I've done this study

I try to share the less possible about my private information online. But it is very hard due to our life being 90% online. I am studying software engineering and I already spent a lot of time online. Now, with the pandemic of covid 19 I spend even more time. Above all that, now I spend my leisure time online which makes me share a lot more things online and makes all of this situation even worse

I try to think about what could happen to the data I share and think about how worth it is. I don't think I have the best risk weighing actually and I am looking forward to working on it. Also, if you keep thinking about that you will never use the internet again so that makes it hard

for a person that need to use it every day. I guess we can learn a little bit about that and implement it

Interview 11

I am concerned about my privacy, that's why I use adblockers, and browsers like Brave which block trackers and malicious content from the web. The main reason why I want to keep my privacy is because you never know in which hands can your info fall into, like recently that Facebook had a data breach. Websites like Facebook and Google track a lot of information, and get a lot of data from their users, that's why I avoid them usually

Usually, I use tracker blockers and I don't use the social media that much, I only have Instagram installed on my cellphone and other social media apps I don't have them installed, I also don't put out much info on my profile and keep them mostly private from everyone except my friends. I also keep in mind to use different passwords on each social media site, so in case of a breach they don't get all my info.

I believe that it's always important to protect our privacy, since data is incredibly powerful, it can fall into the wrong hands and be used for manipulation, blackmail, credit card theft, and even things that seem harmless like targeted advertising makes us more susceptible to wanting to buy every single thing that we are shown. People may say that if you don't have anything to hide why care about your privacy, but you never know how your data may be being used.

I try to not share a lot of private information, only what is needed, and I check if I trust the website or not, for example I wouldn't trust Facebook with my data. I also check what is the benefit of sharing my info, if I don't think the benefit outweighs the risk, then I don't share my data. The benefits are mostly weighted based on how much I need it

To think about the risks, I think about the reputation of the website/app I'm sharing my info with, if it has had data breaches or security concerns, I think about how dangerous it would be if that info were made public, so for example sharing my credit card numbers and info, is something I would be very careful with and have a higher risk than sharing my birthdate or the things I like for example

Interview 12

Generally, I don't worry about my privacy because I know my computer is well protected, but it's better to be safe than sorry, so I always try to check my computer with antivirus etc. Additionally, I know what sites to enter and what not to enter, when something looks suspicious, I just avoid it and that's it. Above all, I use the internet with my head and not thoughtlessly, I don't upload strange pictures or posts so I think I take good care of my privacy

First of all, in the settings, I mark that only my friends can contact me and see my posts, then I mark most things on my wall as private or visible only to friends. Often there are bots or viruses that through different people trying to push us a link or something similar, but it is visible at once, so such people warn about it or remove from friends

Basically, the only thing I want is to make sure that no one I don't know can see the content I post on the internet, so as I wrote earlier, I try to set everything up so that only my friends can access it, and in case of emergency I don't upload anything that could get me into trouble, and that's it as far as my individual security measures are concerned.

All in all, the benefit of this is that more people will be safer on the internet, and the current situation has meant that more people are online than ever before, which means that not all new users or "old people" know what can wait for them, so it is worth making them aware of how they can move around safely on the internet without worrying about the dangers it brings.

Mainly that people who care about my data can work out how to get through or bypass these security measures to get access to my data, big hackers can work on breaking into individual databases just to steal them and thus steal or harm people, or push malware to do it for them, which I think is worse than a normal hacking attack and harder to defend against.

I think everyone is concerned to a certain extent. Personally, my main concern is my information being stolen, mainly emails and credit cards. On the other hand, people discovering something like my search history or browsing history isn't particularly concerning to me, but

if it could be avoided, I'd prefer it that way. Things like spying through microphones and cameras are also very concerning but I have my own countermeasures against that so it wouldn't be as likely to happen.

I don't use social media very often so my information on those platforms is minimal. However, I believe that when it comes to social media, it is the users who should be cautious about the information that they're sharing. I believe that the option to make the profiles private is sufficient to avoid any unwanted privacy breaches. In my opinion people should just be more careful about what they post on social media.

Like I mentioned before, I believe that the first line of defense against privacy issues online is to be wary of what you post online, especially on social media. However, when it comes to more serious matters like your e-mail or PayPal account being stolen, there isn't much we can do aside from installing a good antivirus and using a VPN if push comes to shove.

When it comes to sharing information online, I either do it to people I know personally or that I deeply trust, or I just don't do it at all. The risks far outweigh the benefits. If I were to post a photo on social media I would do so but making sure that I didn't attach a location, at least if I'm at home. I believe that most of the privacy issues can be avoided if we are just more mindful about what we share online.

As I stated before, I think a harmless photo here and there isn't going to do any harm, I think the problem arises when you also share a location. If you're doing it to a tightly knit group of people that you trust entirely, I don't think it would be a problem. Basically, I believe that the risk is directly correlated to the amount of people who will have access to your information.

Interview 13

In general, over the years that I've been using the internet, I've come to accept that you often have to give up a certain level of privacy to gain the benefits of internet usage. The idea of my data being constantly tracked is somewhat unnerving when I think about it, but my concerns about it come and go. It can feel invasive at times (e.g. being shown targeted ads or looking through the list of information Google has collected based on my usage), but in the end, my data is just part of a sea of data being collected from billions of people, and the convenience generally outweighs my concerns.

I've always kept my social media profiles private and don't ever really post, so I've never been super concerned about my privacy in relation to other people. In terms of the company collecting my information, I suppose the ideal situation would allow me to control what kind of data they collect and analyze from my usage of their platform. I'd also like to be able to see what type of information is collected, since knowing the extent of the data they have and how they collected it would help ease some worries. Essentially, customizability and transparency would be ideal.

Personally, I feel like privacy online isn't fully attainable at this point without sacrificing a level of convenience and enjoyment, and I've become okay with that. My data is such an insignificantly small portion of the data that companies have collected from billions of people that it's hard to really care about what they know about me. It can feel a little invasive when I think about it more, but ultimately, I'm not super concerned with maintaining privacy when I've already given it up in several ways.

Generally, if I'm asked to share private information, I consider the source, their potential reasons for collecting the data they're asking for, and whether the outcome I get from entering my information is worth giving them my data. If the source seems sketchy or they're asking for information that I don't see their need for, then I usually decide that it's not worth it to enter my

data and find another method to obtain the same benefits without needlessly giving away personal information.

My general risk assessment steps involve looking at the source and considering what they might want from the data they're collecting. If I can't see why they might need the information they're asking me to provide, then I won't enter it and will find another way to do what I wanted the initial source to do. There are certain data points that I pretty much always consider too invasive to share (e.g. address, personal phone number).

Interview 14

My information being shown to the public, e.g. if there is no option for a private profile. My personal and sensitive information not being kept confidential and being open to anyone and not protected, for example, my address, bank information, personal email and phone number. I am also worried about hacking and viruses. As well as fraud, spam emails and catfishes.

I would like to have complete control over who sees my posts, as well as limiting the access to my friends list. I would like to be able to view my profile from the perspective of another user when I update my privacy settings, to ensure the settings I have chosen are to my liking when keeping information private. It would also be great if the information, such as messages etc, would be encrypted to ensure I wouldn't be hacked.

I want to keep my information as private as possible online, considering I am a very private person. I would also like to ensure none of my personal details, including my personal email, home address, phone number and bank information were being kept by any website. I change my passwords regularly and don't consistently use the same password across all platforms to ensure complete security of my accounts.

I decide whether the information is suitable for online viewing and whether the information is too personal or not. I also ensure that my location is not tagged. I think about whether the information is appropriate, because once it's online it cannot be removed and may harm me in the future. I think about whether I'd want my relatives to see it, and if not I know that it wouldn't be suitable for sharing online.

I check to see if there is any information that could identify my location, Place of work, or education location. If there is, I understand there is a risk of me being followed or found by a stranger. There is also a risk that inappropriate information that I may have shared online could

potentially harm me in the future and my future career. There is also a risk of my bank information being shared by a website that is not secure.

Interview 15

Yes, I am concerned. My main concern is in regard to what information the websites I use store about me, and if I have any control over that. I also have concerns about what they do with my data, particularly if they sell it to other websites or companies. Another thing that bothers me is if, when I delete something online, from my social networks, or from a cloud service, if it's really gone or if they store it without me knowing about it.

Ideally, I would have full control about what data I give to the websites, and of that data, what the websites are allowed to store and share to advertisers, for example. I should also be able to, at any time, see everything that the websites have stored and learned about me, with an option to delete anything I'd want to.

I'm really worried about my privacy online, and it troubles me that not everyone thinks like me. This way, websites keep getting away with enormous privacy violations. Unfortunately, using the internet nowadays isn't a choice, especially with the current pandemic. A lot of the times, you're forced to use Zoom or a similar program, and you're not allowed to have any privacy concerns, otherwise you could lose your job or be expelled from school/college.

If it's something that I wouldn't mind sharing in public, like my favorite color, or a photo of me in casual clothes, I don't really care, since it's not something that people can really use against me. Maybe the photo, but anyone I see on the street could take a photo of me without me knowing, so this isn't really that different. My only concern is when I share something private, in a group chat or in a private conversation, unless that website or app has built-in encryption, there are no guarantees that someone couldn't just get access to my messages and read them.

I don't often share private information, but when I do, I try to use a service with encryption, like WhatsApp, so I know that, even if a hacker gained access to my conversations, they couldn't actually read the messages. The same applies to an employee of the messaging service

company. When this isn't possible, I try not to share super private things, since I don't have this assurance that those messages won't be read by someone else.

I am not really concerned about my privacy, at least when I’m using the app just to see what other people are doing. I don't post many things online because I don't feel I want people to know that much about what I am doing. So, it depends a little bit on the situation. I don't care that much about cookies for example, but I'm concerned about what I post online and what others see.

My ideal situation to manage my privacy was that there wasn't any publicity so there were no cookies. No one looking to what I'm looking, and programs and clouds to manipulate me. That's something I can't control that much. What I can control is about what I post online so I'm not concerned about that. I don't have much to say about this, but it says that I should write at least 350 characters.

My individual values that I use to protect my privacy online is to know and be aware about what I post online and to second thought things out. Another way is to sometimes use anonymous mode, so no one is controlling me. I have a tape in my camera just in case someone is spying me. I don't have much more to say but I'm obligated to write 350 characters, sorry.

I weight my private information a lot online, so I don't just post anything. In social media that is done just to text another people I don't care that much, because I know that everything is recorded if it's not in person. When I call someone, I know that that call is being recorded in the cloud so, in relation to texts, messages and calls I don't care that much.

I weight the risks of sharing my private information quite a bit, so I don't share much on social media like Instagram. But when we are talking about WhatsApp and things like that I don't care that much, because, if it's not in person, everything is being recorded anyway. When I call, text or message someone I know it's all being recorded in the cloud.

Interview 16

Normally when I go online, I don't have as many concerns about my privacy as I think I should have. I'm mostly concerned about how and for what my data will be used. I read a little bit about terms and conditions of the websites but that's all.

When it comes to social media, I'm always concerned about my personal information but once again, I don't do much about it and I use them normally, it never happened to me something that violated my privacy, so I keep using them with not much concern.

I think that a summarized terms and conditions and some promises that my privacy wouldn't be violated would be a good situation to manage the privacy. I also think that if social media sites are honest and tell us what they'll be doing with our personal information and/or what are the risks could help too.

The ideal situation would be a very simple one, essentially because there're people like me that don't understand much about data and privacy on the sites.

My individual values pertaining to protecting my privacy online are my personal information and how the websites can store and/or use them for other things that I did not agree to. When using a website, I'd like to make sure my information wouldn't be somehow stolen and used for other things that are ahead of the main purpose. I know internet is a dangerous place, but my privacy is important, and websites should not be invasive.

I always try to think about the dangers of putting my personal and private information online but if I see that I can have some benefits on it, I usually just share them and don't think much about it. I also try to see if the website/ social media is trustworthy and then decide if I put information there or not. But normally I only share personal info on "secure" websites.

I weigh the risks of doing so by thinking about how they can use my personal information to somehow put me in danger. I try not to put too much information about myself, especially credit cards and banks information, but I'd share names and other things that don't see very

harmless to me- but I think of how a violation of my privacy could affect me and put me in risk.

Interview 17

Yes I am very concerned all of my social media are private and I do not allow any friends or follow requests from people that I do not know besides that I do not post pictures like when I am drinking or smoking and I do not want to be tagged in photos like this and I tent to make the person remove the photos that I do not feel that are considered proper and well about all the data that Facebook Instagram etc. takes well I can't do anything about it so I do not care for it

Well all options are ok Facebook and Instagram have all of the options that I need, and I cannot elaborate about privacy settings because I do not know how they work I don t know how much of my data is being taken o there is one thing I do not want to be asked about my phone number and my date of birth of my surname pretty much anything all of those should be optional

Same answer as in the previous questions I do not want to have a bad image online I do not want to be seen by people that I do not known, and I do not want to be asked about my personal things.

Well it depends on what I am sharing for example I was in the youth council of my town so the benefits are just straight sharing of information and promotion of my institution and more privately social status is pretty important when you are meeting new people online and did'nt see in real life yet overall the benefits are far greater than the drawbacks

This is the same question again and your questionnaire doesn't take 10 minutes to end give next time so more insight into what I am about to write the risks are none if you take care of your photos and think before you act the only risk is your friends when they upload a photo in which you are without asking for your permission that's it I do not have anything more to say so I would want to get to the next question.

Interview 18

I mostly try to keep my name and very personal details secure. I don't go out of my way to do so but I like to keep things to myself if possible. I'm not very concerned unless it's a shady website that can use that kind of stuff in an inappropriate way. I'm mostly worried about scams and people I know finding my anonymous accounts in certain social medias

Make everything optional. I don't like social media sites that ask for my number as confirmation. Ideally everything that violates your privacy and is turned on by default should be disclosed when signing up. For example, Twitter shows followers your liked tweets and that's something that cannot be turned off yet at no point during the sign up do they say so.

I tend to go by the words "if you have nothing to hide, you have nothing to fear". However, I think everyone should have the choice to be 100% anonymous if they so wish. I try to keep things I share online to a minimum, but I won't particularly care as long as it's not used against me. Having a presence online is ultimately unavoidable so why make a big deal about it

Depends on what kind of information. If it's a trustworthy company or site I'm willing to share my personal details. Most times it's a service and in a way, you're giving something in return for that service. I don't see many cons to having your information out there, it's something that's asked from you almost every day online. If I need something and all I have to do is share some info to get it then I'll do it.

First you have to know if it's a trustworthy website. Is sharing my information here now something that'll give me problems later? Most mainstream websites won't have much of a risk. If I'm considering sharing my information to another person online that's more difficult to judge so I usually avoid that. If it's a transaction, it's about knowing how to use the right method and the right platform.

Interview 19

When It comes to browsing the internet, I rarely use unknown or shady pages, I mostly just use your usual YouTube, Twitter... Although I sometimes need to download or search for information in weirder pages, but I have barely felt insecure, because I, of course try to take the necessary safety measures like obviously not giving any personal information to people I don't know, not pressing any links I don't trust and you're all of that stuff. So basically, I'm confident in the online pages I use but sometimes I still get a little nervous when I have to use a suspicious page.

I think all of the primary social media sites I use do a very good job at stablishing a good foundation for a solid set of options to manage anyone's privacy, mainly due to the settings you can apply like only showing info like your real name to mutual or being able to block whoever may be annoying you... And also, another very important thing is being able to set two-step verification on your account so that it's harder for others to hack into your account or something.

I think that it's a thing to be taken seriously, because even with the internet being a great tool for a lot of things, it has a lot of qualities that can make anyone scared, because some people can truly be ruthless. But of course, not everyone is like that, and most big pages and corporations try to give everyone the tools to have their private data and lives protected in the case someone would try to access that, although they're not perfect.

Yeah, for the most part I do, like I said, you can't just give your personal information for free, because that's just putting a target in your head, but you can't also just close yourself fully, sharing info online isn't necessarily a bad thing if you do it fully knowing that it's not going to backfire. So in my case, I won't give really personal data like where I live in precisely or things like that unless it's because I need to buy something from Amazon or anything like that.

It usually depends in what page and for what am I going to use it, for example, I won't give any information on where I live, bank data, my personal life or things like that in social media, but if I'm buying something from a well-respected page then I obviously need to give a very good amount of information, but just like I said, when interacting with people my information is only given to people, I know personally.

Interview 20

When I use the internet, I have concerns about my privacy as I have been a victim of a hacking attack on my accounts. Since then, when I use the Internet, I try to be more intelligent. I am afraid that I may be attacked again and lose access to my bank accounts or social media. I try to visit websites that are secure and those that have security certificates. In addition, I try to change account passwords every month and use two-step verification.

I should be able to choose which data is made public and control who can see my profile. Possibility to set the visibility of messages about the profile and the actions taken on it. I should be able to set who can invite me or follow me on social media and who can contact me through them, so I have more control over people who have bad intentions towards me.

After all, I use social media anyway, although I do not look perfectly at personal data protection. Social media is the largest method of communication with other people, which leads to the fact that the data shared there should be well protected, but people will use them anyway, regardless of security because it is the most popular and fastest way to contact others.

There is no advantage in sharing your personal data on the internet because anyone who wants to know can learn a lot about us. it is different for people who run a business because sharing their data by them can help in the development of the company and earnings. I think that after all, every head should think what he puts into the Internet because it can harm himself. safety first and foremost.

The risk of sharing your data is high, because hackers or people who want to do it out of spite may use it. You should carefully put things on the internet and think twice if you need to make it available. I try not to disclose any data that is confidential or valuable to thieves. I use various types of protection to prevent data, account and other items from being stolen.

Interview 21

I never reveal my real name, age or where I’m exactly from nor what I do on my day or where I study.

I never trusted anyone online that much. I've been online for over 7 years and all I experienced was people ditching each other for different benefits. So, I always try to hide myself and who I am and always hold a nickname and i will try to be unknown because you can never trust people online.

When I create an account online, I always use a fake name and never make it my real name. I also avoid scummy DMs and never try to get baited into something I won't do.

I never post pictures of myself and never reveal my identity or how I look like. Never would have a bio about my gender, age, where I’m from, race. What I look forward to is to help people not get baited into the fake world online.

When it comes to my privacy, I value it the most and try to keep it valuable because if anyone catches anything about me they will use it against me. Whether blackmailing or threatening to do illegal things.

I am a developer and I really know what the risks are when you reveal any of your identities. Cyberbullying will come on the line, threating will come etc.

I try to reduce sharing my information online as much as possible and if it’s necessary for me to share it I will try to make sure who is receiving the information and have an idea about their background. Before that I will make sure I'm not being scammed for whatever reason. There are only few websites online that have SOME of my information. And I will try to keep it as less as possible.

I make sure not to give it to untrustworthy websites or companies or to people that have no background or reputation. I inform myself about who I am contacting before I decide anything

or share anything.

Interview 22

I am aware that my presence on the Internet is constantly monitored, but I am not afraid of this information. I know that my private data is scrambled and stored in safe places. In addition, I do not put very private data on the network but adds some photos from my Instagram trips and nothing else. I rather use forums like Reddit where I hang out. My only concerns are that after entering my data in, for example, Google, you can learn three things about me because everything is linked to my accounts, I think that it should not be possible to search for data in these or other places.

If my data were not collected and it would be encrypted. Honestly, that's all and I don't know what I can add to it, because these two simple changes would allow unauthorized people to not have access and those who should not have access to our data in such a simple way. I believe that there should be such a law in every country. I do not like the fact that there are frequent hacking attacks and data theft because it is a very laconic helmet for hackers.

Privacy is so valuable that it is protected by law. Provisions on this subject can be found in such legal acts as the Convention for the Protection of Human Rights. Whether online in a computer system or in a paper document, my fundamental data protection rights must be respected whenever data is stored or processed which directly or indirectly identifies you as an individual. My data cannot be processed without my knowledge or consent.

I have access to many things, we can do various official matters via the Internet, we have bank accounts, and Internet payments are instant and easy to perform, additionally, we have the opportunity to use various social media such as Facebook, Instagram, etc. These services still need some of our data so that it is not so easy to create multi-accounts and manipulate various information for this reason.

I have access to many things, we can do various official matters via the Internet, we have bank accounts, and Internet payments are instant and easy to perform, additionally, we have the opportunity to use various social media such as Facebook, Instagram, etc. These services still need some of our data so that it is not so easy to create multi-accounts and manipulate various information for this reason.

Interview 23

I am worried that my data will be misused or that it will leak. If I give a credit card number, I'm afraid they will rob me. I always have to read the purchase conditions carefully so as not to be cheated. But anyway, I don't think that when I shop online they will take my data for external use, somehow I don't think too much about it. I don't think anyone needs my data, I'm an ordinary person. I have accounts on various websites and feel as if they do not breach my privacy.

As if I could manage who sees my data, or that my data is simply not stored anywhere, I can control it. Now the privacy settings are insufficient for me, but I don't mind. I don't want my data to be saved on some servers because I don't know how it will be used. I would prefer to know what is happening with my data and that I could manage it with the appropriate settings.

I have never delved into it; I am not very interested in this topic. I know that online privacy is important, I don't want my data leaked out myself. It is important that people are more informed about how their data is used, so that most of their data, which seems completely unnecessary, does not have to be shared with websites. Protecting privacy should be more important to people, but now everyone feels safe sharing loads of information about themselves.

I rarely provide information about myself on the Internet, when I want to buy something, I try to use BLIK so as not to give my credit card. But for example, sites like Facebook or Instagram, I share some photos, posts there, and I'm glad that others can see it, but I don't share private data. I never do it, except in private messages (I don't know how private they are).

I believe that sharing private information about yourself on the Internet carries a considerable risk, be it theft or the acquisition of your identity. I am always concerned that

what I am sharing will be used against me. I don't want them to extort money from me because they stole some of my private information or because they are going to try to destroy my life.

Interview 24

Sometimes, I have some problems with having my contacts on social media because i never know who as access to them, I always double check the regulations to see if there are not any "plot hole."

But now a days I feel that maybe old people are very easily abused on that page. On Instagram for example anyone can see your photos but even people whom you do not want to see.

Maybe if you could have access to who visits your profile who sees your photos, but in that people, you should include programmers from the actual social media site, because those are there persons you cannot see accessing you private information and that can expose all of it at the same time overall maybe a board with all this information would be a good idea to manage your privacy.

I believe I should have access to anything related to me, we all should be able to see that information on a daily basis, this way we can control our own privacy regarding only our information and there would not be any programmers who could steal that information and spread it online to other users and persons.

I also think people should be more aware of what they post on social media I rarely put private information on social media but when do I always think what could happen if that information is leaked, I only use Instagram and WhatsApp because of it, I had Facebook but eliminated my account because of information leaks, after that I always think first and never created a new Facebook account, because of that reason...That’s it I guess.

Unfortunately, there are unscrupulous people on the Internet who are looking to take advantage of you. As I said on the previous question I always think first before posting anything online because it happened to me once on Facebook my private information was stolen and put online by some people who I don’t even knew I ended my Facebook account because of that.

Interview 25

When I go online, I am a little bit worried about my privacy, but I understand how little control I have over it now that I have created accounts in slot of websites and inserted slot of personal information into it! With that in mind I try to not insert much more relevant information in new websites. In social media I try to keep it simple and private. I feel that I am a conscious internet user, but I understand how powerless I am when it comes to defend my privacy.

The ideal situation would be to use an anonymous profile. Either that or I would use my own profile with the least information possible, meaning that the perfect profile would only have my name and maybe my age. For that reason, I try to keep pics to the minimum. It would also be good to prevent strangers to see my information and profile. Relatively to the website's connection to my browser and computer, it would be better if it had absolutely none, not being able to save passwords and emails.

I face internet has a very good thing however I feel like I know the negative sides it has. I understand that my profiles and accounts are an extension of me that is in danger of any company's desire. Internet has become the best way to spread political ideas and use marketing. With that in mind I tend to disapprove or suspect of anything that I see online. I try to give it has little attention as I can and I try to Talk about subjects I see online with other people that I know and might have different opinions. It is dangerous to only see the side that internet wants to show you.

I try to only share private information that can't or can only very hardly be used either to Identify me or to position me in a certain ethical, moral, political spectrum. Know that slot of websites use algorithms based on spectrums I tend to try to keep away from any certain spectrum. This obviously doesn't work every time. I don't usually think that there's any benefits to sharing my information. When sharing private information, I weigh the risks by

understanding what information I give can relate me to any moral, political or ethical spectrum. I would only share information that would relate me to any spectrum if there's money to be earned and if the place that I am sharing my information with is reliable. I would say that if there's any social or financial benefits for me, I would be able to share some of my private information.

Interview 26

Yes, I often feel worried about hackers that can easily rob my identity and/or see me through my camera. I feel worried about my personal information principally on google. I often feel worried about my conversations for instance, on WhatsApp. Facebook is not working well in protecting the users' information. And the one last thing that sometimes I feel worried about is the possibility of being voice recorded.

Do not publicize anything that can compromise your identity. Do not talk to strangers, do not give any passwords from anything at all at anyone or public in your profile page or something. When using a laptop cover your camera, I mean just for the case, use verified sites and use an antivirus to protect you even more. And have extra careful in any social media.

I always try not to give any more information than necessary, maybe do not use pics of me or I can always put my accounts in private mode so I can control better who sees what and I can decide who can see my profile. Do not share my private information online and be extra careful in social media because you never know who is on the other side of the area.

I do not share my private information anywhere. It can happen that sometimes I can say where I am or where I am going but is always measured with care and I can always control who is watching my things and that makes it easier to know what to share. You can always block users and have your account public, but i think that blocking users and having your account on private it is the best method.

Again I do not share my personal information online, but if I did so I think I would block all the people so that they would not know where I am or what I am doing, or who I am with. But better than that because it gives a lot of work, I would maybe weigh the risk of sharing private information and probably would put my account on private. I think that I would weigh the risk and do the last option.

Interview 27

Yes, I’m worried about my privacy because everything we do is under control. I know that I sign a contact whit I accept everything but at the same time I thing that big data is to much evolved and that it take to many information from us. I'm worried that social media create personalized contest that give you on you home page everything you want. I'm worried about how much "internet" knows us and how it could personalized every aspect of our life.

The solutions would be to not to use the information from my research to create a personalized home page. I don't know how, but the information about me has to be used only for me e not for making any kind or research about me. So I think that we need to be educated about how to use social and we really need to know what the social media really do with our information, maybe with conditions more explicative when we open a social page.

I don't use too much social media, because I know that it's quite impossible to make my information useful for social. So I try to use a VPN and not to search specific thing that I could find out from social. I didn't post any sensible content, because I know that when I post something in the same moment I post, it would be forever online, also if I delete it.

I valued the advantages in consideration of what I want. So if I’m an influencer I need to post everything of my life, but if I’m not, I try to post less than influencer. I know that there is a lot of advantages to use our private information online but I don't use to do that. So I try to understand what I could receive from posting something personal and I know that I don't need to do that.

I think it is very risky to share information online, but now especially with the pandemic it has become inevitable. there are many risks in doing so and despite the reassurances of the various social companies, big data check all our information to try to create a well-organized and structured profile, in order to offer increasingly personalized feedback.

Interview 28

When I go online I always get concerned if someone is accessing my computer or tracking what I am doing. I also like to cover my camera just in case someone is watching me. Other than that, I don't really worry that much, it is a thought that is not present in my mind. To be honest, I always think that my phone is always listening to what i am saying because the ads always match what I talked about.

I am not really sure. I am not into security programs so I don't really know what to do to improve my safety and privacy. Maybe I can change my passwords from time to time and make them harder and longer, I could use a VPN to not be tracked 24/7, I could search things with Tor instead of other searching engines like google chrome just to be safer, I could have a verification thing activated to receive a text message on my phone giving me a specific code.

Even though sometimes I don't really pay attention to that and forget that my privacy can be violated, I think that privacy is the most important thing when you navigate online and there should be easier ways to be safer because most people, when they go online, they are just having fun or learning something but no one can ever be relaxed because, at any point, someone can be watching them and their moves.

I actually hate when I have to share my details online because I always end up scared that my information will be stolen and used to steal my identity or steal my money or something like that. It is always scary. So any time I have to do that, I try to make sure that the website is legit and will not be stealing my information to use it later for something else.

Every time I have to share my information online, I always get scared that my information will be stolen, either for a steal of identity or for stealing any information or money or something else. And, if I really have to share that information, i always try to see if the site is really legit and if it is safe to do so. I weigh the risks a lot when i do this and it can be very dangerous for anyone.

Interview 29

Over the last 10/15 years of my life i have used a computer almost every day, I've had an internet connect since 2010 and been using a VPN since 2017.

I am mostly afraid of identity theft and usage and monetization of data. I have had conversations in private that have influenced my recommendations in different websites using cookies, if that is possible, it is also possible that big tech corporations also gather data like political statements, private conversations involving delicate themes and information. Privacy has been a hot topic in recent years and I think that corporations have to much power with the data that the are allowed and capable of collecting.

It would be ideal if those sites did no monetize private data as in some of them we even pay for some services, sites should have options that disable/enable different options of gathering data, even if privacy came at a cost, like a small fee for no adds or disable "features" that may require the user to share very private information. I also think that it's almost impossible to as an user and a normal society member to manage their privacy as it is not a very discussed topic and most of the times it is not discussed but experts in the area.

I don't mind sharing information that might benefit me, but I tend to always use a VPN when doing important things that I do not with to reveal to the public, like checking and using my bank account, applying to jobs and searching for some topics that might be controversial to the people you know IE if I am researching for whatever reason a political party's agenda just to be informed about them, I do not with to be bombarded by their propaganda in the future.

I tend to think about the benefits of subscribing and logging different contents and websites, some may not be what looks in the surface, I normally browse other people opinions, normally using reddit or non paid reviews on YouTube. if it looks to good to be truth, normally it is and if it's free, I can't expect to be protected by the sites as they many times sell my data to third

parties. I think in the future governments will restrict the usage of private data, but this will come at a price.

I always search about what I am trying to do, check if the offer is legitimate and if I can do something to protect myself, sometimes the site has a dodgy record and that becomes a no for me. I also use a non important email to subscribe to sites that I don't plan on using that often and that email has absolutely no information about me besides the name. If the site is beneficial to me after I've done my research I will probably use it, if not, I will try to get a better alternative.

Interview 30

When I go online, I do not really worry about my privacy, because I think that I am quite erudite in this matter and try to leave as little personal information as possible, or I try not to perform any dangerous actions, for example, downloading strange files and clicks on strange links. The only thing that worries me is the attackers who use social engineering to their advantage and deceive other innocent people.

I try to use private profiles everywhere, to which I will add those people I know personally. Also, I do not share any personal information, since you never know who can use it for any purpose, including against me. I do not give access to applications that they definitely do not need, for example, my calls, tracking my location, and others. Personalizing app settings is the ideal situation.

Only I should have access to my data, I am not going to use services and applications where I will not have the opportunity to refuse the service to share with developers or other people. This applies not only to me, but also to other people. I am worried about the safety of all people, since the number of cyber attacks related to data leaks is only increasing, most often this is due to the negligence of the company whose service we use.

The only advantage that can be from the fact that you share your personal information is that you are given advertising personalized for you and your requests. But this is a very dubious advantage, because if I need something, then it is unlikely that I will do it from advertising, most likely I will find what I need on my own, and advertisements only spoil my life. From this we can say that I do not see any advantages.

Whenever I share my personal information on the Internet, I am always aware that data can be stolen by hackers, because there is no 100% secure storage system. The first risk is data leakage and use against me.

The second risk is that they will follow me, steal my data so that I do not know about it, thanks to the numerous accesses that we ourselves give out to the application, site or service.

Interview 31

When I go online I’m concerned about my personal information being harvested and shared with third party agents that may have use them with malicious intent. My biggest concern is my fiscal location being unknowingly shared since that could lead to physical harm! I'm also concern about banking data and social services since that could cause massive economical damage!

I'm not really sure about that but the aspects I would emphasize would be that my phone number, address should never be public, my images, direct messages and deleted posts should not be accessible for other people as that could leak private information I would also make sure that most people use 2 factor authentication as that helps prevent password leaks.

I want my address, phone number to be private so I don't use them in hardly any website and almost exclusively for purchases in trusted online stores. I don't give most apps on my phone access to my personal data such as my gallery, messages and banking data so that I keep my personal data safe from third party agents. I also deploy the usage of VPNs and such in some untrustworthy websites.

I definitely take the risk into consideration when sharing my private information online and so I hardly use it mostly for purchases or banking only on trusty online stores and certified banking apps. I think you can’t really avoid your data being harvested at this point so I just try to avoid the shadiest websites and stuff but I can’t avoid some social medias or google so I just got to be okay with that.

When sharing my private information online I definitely take into consideration the risks associated with doing it so I really try to keep it safe from third parties with malicious intent. I think its unavoidable that your private information is going to be harvested by some websites such as Facebook Instagram twitter google but you just got to be okay with that and try to avoid giving your data to shadier websites.

Interview 32

I don't have much concerns with regards to my personal life as I try not to share personal details about myself online however that being said there is always personal details online. I get concerned when sites say they collect cookies or when they request your location. I also find it concerning when I talk about a certain product and then I see ads for it on my feed even when I have not searched the particular item.

I like that Instagram has settings where you can turn your account on private or share stories only with certain individuals. I think that there should be something where you can't get friend requests or follow requests from people who have no mutual friends or followers as you. I like that when someone DMs you that you can choose where to accept the DM or to choose whether it has been seen. I would also like it to be more difficult for accounts to get hacked, especially when certain accounts are linked to your payment details etc.

I do not post anything that could be potentially incriminating in the future. Whether that includes it hurting my chance at a job opportunity or portrays me in a certain light. I don't post much except for images that portray me and my close friends. And I don't post anything revealing because people can steal those images. A rule I use is I would not post anything that my family members can't see and that's my way of protecting my identity and reputation.

I look at how this post or picture can reflect on me or the people in it. If it has a potential to cause harm or is questionable in nature I will not post it. My accounts are also on private so to an extent I am aware of the people who can view any information I share. But if the information is private and not necessary for other people to see in any way then I will not share it. I will only share or post when it is seemingly innocent and fun and there seems to be no negative repercussions.

I look at myself and the people related to the information I will be sharing. There has to be no possible negative outcome I can see for me to post it. I am very particular about I share as I

a persons entire reputation or identity can be defined but what they put online. I do not like to be contained by an image online or always feel like I have to live up to that persona, as a result, I only post things that I would feel comfortable if anyone I know comes across it and sees it.

Interview 33

Sometimes. It really depends on what site I'm visiting. When registering I usually come up with a completely new nickname that I don't use anywhere else. I know how easy it is to stalk someone just by googling their username. Other than that I try not to disclose most of my personal information or location (with exception like dating sites, legal advice forums etc). I do it because I fear of my friends or just some random people from internet stalking my activity and finding some unpleasant things about me.

Sadly these two social media sites are the ones I actually have my personal information on. It's because I use Facebook mostly so my real life friends can find me, and what's the point of having a fake name if they can't find me by it. I try to minimize what I post there and usually only use it for texting with my friends. On Instagram I only have my pictures and not even my real name is mentioned anywhere. It also isn't linked to my Facebook profile in any way.

I'm not really sure if I understand this question correctly. I think I value my face the most, because I can always change my name and location if I really want to, I can't really change my face so easily. And even if my location and name leaks out, so what. Nothing much will really happen. Of course I wouldn't be alright with it, but if no one's searching purposely for me, nothing bad could really happen.

In the first place it depends whether it's necessary or not. If it's not, then I most probably won't disclose my personal information. It also depends whether only site owners will see it, or other people too. I would never sell my privacy for money unless I was really in a tight spot. The most deciding thing whether I will disclose my personal information or not depends on my circumstances at the moment.

The most important risk for me is it leaking out online so that everyone can check it just by searching for my name. That's why I could never become a public figure, because I don't think fame and money is worth my privacy. Money and fame are temporary, privacy is eternal and

once lost, it's really hard to get it back. When disclosing my personal information, I make sure that even if it leaked out, it would be as little as it's possible.

Interview 34

Yes, I am concerned about my personal information and the way it is used. So many times we need to give certain information to sing up in social media apps, or in students platforms, so I always think where is my information going, who is reading all the information. Its sounds a like a conspiracy, but its a thought I always have.

Also I am concerned when some apps ask me to use my location.

I think it would be good that social media sites don't overstep the way they use all the information we gave them. It is very common that when you search something in google, then you will receive some advertisements related to the search, so it's kind of stressing that this happens every time you search for something. Some moderation is this would made more attractive to join new social media sites.

I think the main value is responsibility, when you log in into social media apps, you need to know what kind of information its "ok" to give, and what kind of information it is convenient to keep, as I had said, you don't know exactly who can see this information, so you need to be very careful on what you sure in this sites, especially with personal information.

By the I will receive but giving certain information, but I always think first on what would cause that I share certain information, in social media apps or when signing up in other sites. I have very clear, that there is some information I would never share in online sites. So up to this, I evaluate the situation and the importance of my information.

I know Personal information, excluding my name, email address and some irrelevant information, would take so much risks by sharing it, so I prefer not to share my private information, doesn't matter the social media site, or in internet and specially, on very unknown sites . So I don't take risks in this type situations and try to share the less information I can.

Interview 35

When I find myself online, I always try to take different precautions. I never try to publish much about my life, whether professional or personal. And I have a lot of care on the sites or applications I have. I try never to overexpose myself. I am afraid of what is exposed about me online as well as about my family. I try as much as possible to contain things as private as possible, I am careful to have the PC camera covered and microphone lock. It is not being paranoid it is trying to take care of me to the fullest.

I keep my location permission off as well as my microphone. Only active when necessary. The ideal for me in these applications would be to have something that ensures our privacy, I have been attacked online several times on Facebook, so maybe I stopped using the account. I am afraid of my online exposure I deal well with it but I am afraid of what it may cause in the future. More and more people are judged by what they publish and do not publish online. And it can cause problems at work.

Online privacy is important for numerous reasons. I don't want to share details of my personal life with strangers and it's hard to be sure what personal information is gathered and by whom: information collected by one company might be shared with another. My values are very focused on Protect personal security; Allow anonymous political speech;

I am very careful to do something like this. I always try to be sure with whom I am sharing what I should share. It is important to care even if you know people. We cannot share everything online. We have to maintain care, at the level of images and information. I am so excited about this that we can find it available online: Create strong passwords. When creating a password, think beyond words or numbers that a cybercriminal could easily figure out, like your birthday.

Don't overshare on social media. ...

Use free Wi-Fi with caution. ...

Watch out for links and attachments. ...

Check to see if the site is secure.

I am guided by the following in order to reduce the risk.

Interview 36

I am afraid that third person will find out about me. Privacy is important to me. I am careful about the pages I go to. I am often afraid of pages resembling primitives and check if the page is real. Before registering on a given website, I carefully check the regulations and personal data protection. I'm afraid someone will get my credit card number, home address, telephone number or social security number. I don't want to be robbed or that someone has my confidential information.

When I do not have to provide my address, date of birth, telephone number. Also, I would feel safer if strangers did not have access to people in my group of friends or to data shared only with people I know. I care about the protection of personal data through social media. I would feel safer if I could decide who sees my data and be able to share it only with the people I choose. This would make the use of social media feel safer.

I don't want strangers to know too much about me. I don't want anyone to know what sites I'm going to, what they're writing about with friends or what photos they have in the gallery. I also care about confidential data such as PESEL, date of birth, telephone number or place of residence. I would like such data to be made available only to people who consent to it. I am very irritable on the web and I am concerned about many aspects of sharing data with each other.

Often, websites better match the content displayed on them through the knowledge of which websites we enter or in what age range we are. This allows you to better match what is displayed on the page. By sharing data, we can find our friends on social networking sites or create accounts on different sites. e.g. on Instagram, marking the place where we took the photo

or who we are with allows you to get more likes. I think that despite the fact that you should be careful what and to whom you share.

Risk is an important factor for me. I am always afraid to mark locations where it is located so that no one will rob me at that time. I am also careful about sharing my data on different sites for fear of personality theft or taking credit for me. With too much shared data, you can run into serious problems. you can also experience theft of accounts on social networks, which can make a career very difficult for popular people.

Interview 37

When I go online I do have some concerns, but they are mostly minor things, relating to breaches in security and personal data, and those dont happen very often due to the job done by the social media people. Another thing that helps me get a little less anxious is the fact that are sites than can track if have been vised in some of those security breaches.

In an ideal situation I would only share what I want to share with my friends (photos, videos, etc), but for getting in the platform most of the time you have to share other information, which are good if they get leaked like your phone or your address. So, yes, in my ideal situation I would only share what i want and not what i need to get in the platform from the beginning.

Regarding the protection of my privacy online, my values are mostly keeping what I can to myself and only share somethings that will not affect my life in the future (either my fault or the platform). I do not use VPN for misleading my location, but I should think about it. More than that I don’t really think anything more is necessary to protect me.

When sharing my information online, I take into account factor like the amount of friends I have on the social media in question, the interactions I can get with them through the internet that I would not get in other way, but I also take into account the risks of getting my information on another account that could get leaked. Based on this assessment, most of the time the benefits outweigh the risks.

When sharing my private information online, I always take into account the risks. I have a threshold of what’s acceptable when I enter some site or platform. This means that, for example, some sites asks for my location, or notifications when is not needed at all, this can be a great red flag that will get me alarmed that something fishy is happening.

Interview 38

There are times when I am very concerned about my privacy, specially when men approach me in social mean. But there are times when I seem to care very little and actually forget that the internet keep all your records. I have no current concerns over it but there where times where I cared about my photos or even conversations. Exposure has been the biggest concern in my mind lately, but even worse is exposure coming from people I actually know.

I wouldn't be so sure since I have no knowledge in that field but maybe photos posted by people and with identification on me should only be seen by the people we have in common. Only one device should have the account or the account record and the data should be kept somewhere else and restored once the account is logged in. A new location of login should be sent to multiple emails. And there should be more than one step to log in to a account.

I mean privacy as a whole is a value I keep. I wouldn't want someone to watch me through a window so I wouldn't want them to watch me through a profile. It's a new weird way of stalking. My values are compassion, to not do to others what I wouldn't want someone to do with me, privacy (all my accounts are private), loyalty, won't allow anyone to talk shit on social media about my friends, caring, only positive comments!!

Well sharing your personal information can give you different ways of viewing result like in test like calculating something, your personal information is often used for data to a company and the company ends up building the app or the site for your profit. Per example, YouTube used your likes, your age, your views to give you a platform where you find what you like. You benefit from it.

Not much, I usually keep it private for other people, other than my age I don't seem to be very scared of anything else or to expose anything else. Truth is I don't weigh those risks in comparison to what I should. I don't know what else to say and I can't go to the next question

so I am sorry for writing and it's of no use for the study. At this point I don't know what to write!!! I am sorry.

Interview 39

I am somewhat concerned about privacy. Scandals like Cambridge Analytics worry me to some level, in the sense that "how reliable can a company be when having your personal information?", and "can it visualize my specific personal information, and can it sell it to other individuals or organizations remaining unnoticed?". It is also concerning the number of hackers who can bypass the security system of the servers, and have full access to all data of those servers. This is also something which should be much more regulated, and have legislation assuring our privacy. The EU, however, has been doing a great job and making good first steps.

I think that it is somewhat hard to control and manage our own privacy. The privacy which we should be able to access, and manage, it's the privacy that allows other users to check, for instance, my profile, send dm's, check my photos, check my status, ... It should be assured by Facebook, Instagram, Snapchat, or any other social media, that cookies and other data analytics trackers are not used to monitor the behavior of the user, neither the preferences he has. Google has abused this system, not too sure about Facebook, but the fact is that, for me, privacy should be worked internally, and given to everyone, whether that person wants exposure or not, privacy should be assured. However, allowing the user to make his profile more public up to some level should also be allowed.

I think that I am a bit introverted, and somewhat shy sometimes, and I enjoy having my own free time, thus, I'm a much more "private" person than most people probably are. I think it is only fair and just that the user is protected against the greedy side of the companies, and the external threats that hackers constitute nowadays. It is always important to have a little exposure, like for instance, LinkedIn is a social media platform where most users (an overwhelming majority) want to have exposure, and make a name for themselves so that they can get a better work opportunity or more exposure to their businesses, though those are very

specific cases, as most media platforms are open to a wide range of ages, and have more of a "relaxation" or "social connection" objective than LinkedIn has.

Like for instance, in LinkedIn, it is essential to share your private information (up to some level): your education, previous jobs, skills, previous experiences, photos, and out-of-work interests. In surveys, for instance, like this one, we are giving away our private information (it will still be private, but studied), so other people can study our behaviors and preferences, though the major difference from this with all other social media platforms, it is that we consent, and we are happy to share our information with others. It is beneficial to the point that it can help to understand our process of decision-making and our general reasoning on any topics. It can also help businesses to make better products or understanding the opinion of the public of their products, and getting feedback.

I think the risks are always implied whenever we create an account for any website or social media platform. The risks, which are getting your private information exposed or sold to someone else, are always there, regardless of the website being owned by an SME or a multinational. The risk of putting your credit or debit card information are always very high, and thus, in most websites, with some exceptions, I do not share those. The risks may seem very small for some people, as we may be one of thousands who got their data leaked, however, when the data is organized and well-identified, it becomes a much bigger risk, though we do not know that when we enter in any website.

Interview 40

Of course, I always think about my privacy, but pretty often I don't have enough time to make sure site or something is safe. I just try to make sure I don't leave there any sensitive data such as ID. I have heard about hacker attacks concentrated on sites users  personal data. I wouldn't like to see my ID in hackers hands. Having my ID they could easily take some credit and put me in trouble. I think that's the worst that could happen. That's one of the reasons I do my best to stay incognito.

Having full control on every single aspect would be great, but I guess its impossible. This type of data is pretty valuable for sites such as Facebook, Instagram. That's the price we are paying to watch sweet photos of our friends and idols. As I said being able to delete, move, do anything I want would be great and I hope one day I will find a site that allows such actions.

Well my favorite is VPN. Being able to kind of hide in the network sound pretty good and it is actually. I just feel a little bit safer knowing that potential hacker or whoever trying to watch my moves or even get into my computer has to do much more just to find me and then connect with me. Pretty useful tool honestly. And VPN is the only one I use.

Well I don't. Most the time I just accept terms and conditions just to get through. Sorry but as I said earlier I don't have any code for sharing my personal information. Most the time I just do that. For me site has to look sketchy to have any kind of thoughts before accepting. I hope that my answer helped you already because that is all I can say

Well I already told you in the previous slide so let me just skip this.

Interview 41

I am not too concerned about my privacy online. While I do avoid a certain level of exposure, I still am quite open and usually don't think that much before posting online or engaging with social media posts. What concerns me most is the fact that whatever I post online may very well still "exist" years later, regardless of me deleting the original post.

It would be ideal to be able to choose exactly who gets to see my posts and be notified if someone saves them/screenshots them. Although this doesn't directly affect me, it would also be great to truly implement an age control that doesn't leave young girls and boys at the hands of people who don't mean well; I believe their privacy should be preserved and social media sites definitely should have the responsibility to guarantee that.

The most important thing for me is transparency. I would like to be sure that the things I share with a certain person or group of people don't reach anyone else's eyes. I would like to be sure that the data I share with a website (be it my debit card info, my address or even my full name) don't get shared past the absolute minimum. The last thing I want is to be misled and used for someone else's benefit.

I value commodity and having fun online. Usually, there's nothing I would consider posting online that I would hate to see become public. Therefore, for the most part, and personally speaking, there are only benefits to sharing my information online. In regards to private information such as bank account date etc., I only ever share it when I really need to and don't have another option.

I only share things that wouldn't hurt me or anyone if they were to go public. For my personal situation, I don't believe that are many risks, as I am also careful to read terms before signing up for anything online or giving my personal information. However, the situation would look a lot different if I were a teenager or someone older with more to my name and more responsibilities.

Interview 42

Not really, I just want for people not to know where I live and I don't like when strange people get in contact with me. It scares me that a person from another around the world can have access to all my information and know things about me. Other than that I'm not very careful with what I do online, which is bad and should have more precautions with that kind of stuff, because it can be a nightmare. The only thing I know I am very careful with is spam email and people trying to get money from me.

When I'm visiting any social media site like Facebook, Instagram or there social media websites I just put my account private so that only people that I accept or friends follow me can watch the stuff I post and share. I also only accept invitations from people I know, friends, family or friends from friends. I also don't share personal information like my address, phone number or all the stuff I do on my day to day life so that people don't know my schedules.

I do not to share information with strangers, I do not to share my personal life in any kind of social media platform (Facebook, Instagram, WhatsApp, Twitter), I have all my accounts private, I do not talk to strangers online, I try not to share important information online. I don't reply to spam email. I also think it's important that everyone follows this rules because there are many people who would be particularly naive to get caught in traps like this online.

When sharing your private information online, I first see if it is a trustworthy website, if it has something that can provide me that can cause a good impact on my life, like prolific, I shared my information with them because even though it is trustworthy (I researched about it first), I can also make money out of it, so for me it is a huge benefit for sharing my information. Other website I trust to have my information is LinkedIn because i can get job opportunities from there which is also a huge benefit.

When sharing your private information online I always check if the website I go in are reliable, or if they give me benefits for sharing my info. If a website doesn't give me any type

of advantage or benefits I don't trust it to have my full information, like Facebook or Instagram. That's why I also have my accounts on private, so people from outside can't access any type of information I put on the website and that's really it.

Interview 43

When I go online I'm constantly concerned about my privacy, every single time. Every time I search something on the internet, every time I go on the social media or even when I watch a video. I'm super anxious that someone can seek for my information or I'm even more worried about giving "free traces" about myself or about my family. Maybe I'm too worried about it, but I just want to live my life without risk. Now-a-days everyone one is online, every single info about a person is online, that's how it's working the society at the moment, so I guess everyone is concerned about it.

When visiting any social media site, like Facebook, Instagram, snapchat or every single social media I would like to manage my privacy as much as I want. For example, I would like that every personal information is locked and ourselves can manage to unlocked as many information as we want to be shown to the other users, so people would feel more safe to go on any social media since they can choose the information about himself to be shown at the public.

My individual values pertaining to protecting my privacy online are: Efficiency, by the administrators of the social media in a way that they concern about their users' privacy; Maintenance works and upgrading works of the "protecting system" in a way that the ones that own the app can avoid every single way of "scamming information";

Speed, so that the ones that works only to protect their users' data can work on fixing every single type of problems related to the "emission of an user's data in their social media".

When sharing my private information online, I weigh the benefits of doing it in a way that I feel more comfortable about it. Obviously I don't like sharing my information online to strangers, but I feel pretty confident of sharing some personal information to friends of mine that I've met on the web and that I've developed an intimate connection with them

When sharing my private information online I weigh the risks of doing so I a way that I feel more comfortable about it. Obviously I would never share my personal information to stranger, but I would feel more comfortable about giving some small information about myself to some friends of mine that I've met online in a way that we can keep in contact with each other and obviously with friends that I've established an intimate relationship with them based on trust.

Interview 44

I use many social media apps but I'm not concerned since I don't use them actively, meaning I watch videos and like stuff but don't things myself. So not really since I try not to share any personal information online. I've seen people doing stupid things online and people reporting them, causing them to get kicked out of school or losing their job and I'm aware of how posting certain things online can affect me in real life.

Since I usually create a private account without telling any of my family or friends I would others not be able to find me through my mail address, phone number or through another social media site. I also like it when there's a feature that lets me save it without having to like it and thus letting other people know like the save feature on Instagram. And of course, being able to create a private account or make your posts private.

I want to be able to use the platform when I want to and to also be able to delete my account or posts whenever I want to without. Since I'm a very private person I would never use my real name or give out any important information about myself to strangers. I would also not want any social media to give or sell my information to others without my consent.

I would not share any private information for the sake of my security and the effect it can have on me in real life. But I have seen cases where doing so benefited them like when they a sickness or are being abused by their parents. They shared very private information, asked for help or money and I think those cases did benefit them and probably would've done the same thing. But if there isn't a really important reason then I don't think that sharing private information online has any benefits.

The same as with the benefits. I personally think that sharing or oversharing online is a bad thing, especially for young people who feel frustrated and want to be heard by others. What's posted on the internet stays on the internet and something stupid someone has said on the internet 10 years ago to look edgy could cause them to lose their job. And as an employer, I

also wouldn't want to hire someone with a bad reputation so to me the risks are high and there are almost no benefits.

Interview 45

When I use the internet, I tend to be very alert. I'm afraid to expose my private info, such as my IP, location, the name of my family members or even my who are my friends. So I tend to only view things on the web and have all my account on every social media private. I have gone to such length that nowadays I have a VPN subscription and two factor authentication on every social media platform.

To have privacy online I tend to have all my social media profiles private and only accept friend requests from people that I know in real life that are my friends. For example on Instagram, the social media that I use to communicate with my friends, I only use the close friend feature of Stories to post things on it, so that only my closest friends can see it.

Well I wouldn't say that I have a particular reason to protect my personal data online, I use the internet since a young age and was taught to protect my self online with the same care that I protect myself in real life. So I would say that the reason to do so is that myself online is an extension off me offline, and for that like I wouldn't leave my front door open to every stranger I don't leave my online door open.

I usually think about what would i gain to do so. So if the outcome that I'm thinks is not worth it I would thinks twice. I would say that giving weigh to my action related with sharing private info are so much complex. As I have said before my online self is an extension of me, so it is difficult to explain this things. But I would say that I give them the same weigh to my private info as I give to my personal life info.

As easy as seeing if the personal info can be so sensitive, that some one may find who I am an what I do outside of the social media platform, of course I'm talking about completely strangers, if there person in question is a close friend, family member or even work colleague I have no problem whit it. So any kind of location in posts or even photos of famous places I tend to not post to every one or I only share it whit my friends.

Interview 46

My ideal situation would be that any site or social network would let me choose when and where people can see my information, my activity, if I am on line, or if I read a message. Let me choose whether I want my information to be used for advertising or for research. Don't use features like the camera or microphone without my consent. Don't save the sites I visit so that no one knows whether I visit them or not.

As soon as I enter an app like Facebook or Instagram, in the privacy settings I only publish the information I want, I deactivate my online status and annoying notifications. I deactivate data collection for advertising. I keep my profile private and when I upload content I try not to show recognizable places or personal data. As I have a private profile I show it to my friends and family without any problem. I also keep a close eye on who follows me.

As soon as I enter an app like Facebook or Instagram, in the privacy settings I only publish the information I want, I deactivate my online status and annoying notifications. I deactivate data collection for advertising. I keep my profile private and when I upload content I try not to show recognizable places or personal data. As I have a private profile I show it to my friends and family without any problem. I also keep a close eye on who follows me.

I try not to share too much information and if I have to, only as much as is necessary. If I do it is because the site asks me to and I will try to keep it as private as possible. Only the site will handle that data and hopefully not use it for anything else. I check if this is the case in the terms and conditions. If my privacy is violated I try to delete my user and all the information I have on the site.

Interview 47

Everything you post online is visible to everyone. A harmless picture can trigger unwanted attention, a tweet can put you on a bad position. The need to always be concerned and triple check everything you post. And most importantly, how your social "footprint" can damage your career opportunities. Everyone makes mistakes but when you make them online the consequences are worst.

I think they have evolved so much by adding the close friends story feature in Instagram but Facebook still has so many privacy issues. At the end of the day you can't really depend on the apps themselves to protect your privacy because, regardless of how they approach this issue, someone will always find a way to violate your privacy. But I do think they should adopt harsher punishments when an account is reported.

I always keep a small social group online so that my posts have a smaller chance to end up where I don't want them to. I always check everything I post and never do it hotheaded, I never post anything too reveling so I am very conservative in that regard. The most important values for me are: coolness, conservative, entertaining and never boring, and security; the last one being the most important for me and all this comes up to.

Is it going to have a negative impact on my life? Is it going to affect my job opportunities? Does it leave me vulnerable to online predators? Does anything in this post reveal to much personal information? Is this ok according to community guidelines? Will this make anyone feel uncomfortable, including myself? Does this attention help me or does this hurt me?

Exactly like in my previous answer. Those questions either give me benefits or unwanted risks so if the risk is not worth taking i won't take it. And the truth is, in most cases sharing my private information online is not worth it. Because social media is such a big part of our day to day lives everyone knows everything about everyone, and that is due to over-sharing online.

Interview 48

Usually I'm not concerned about privacy but of course, that I suspect some sites. My concerns is that they robbed my information of credit card per example. I play some games such as league of legends and valiant, and I would be very sad if they steal my account. Some of sites to see movies and series have a lot of publicity and some of the sites look like they have virus which I think it can damage my computer.

Normally the social media is one place to post about you, your favorite things, your animals, etc.. and I think that who post in Facebook and Instagram normally is not concerned about your privacy. However, sometimes the social media request a lot of personal information, such as, telephone number, location, sexual interest, age, etc. I think that the social medias apps should certificated that minors do not entry the social media because can be easily deceived by adults.

Normally I avoid sites that look like have virus or a lot of porn publicity because I feel that, that sites may have virus that damage my computer. In social media, I search for put the minimum things possibly and not post photos of family per example. In my phone and my computer I have anti-virus app that helps me to avoid this virus and tell me when I have virus in the pc. In my phone I tried to not turn the location on.

Normally I try to not share my private information but if I want to be in the social media community I try to not post a lot of photos of me and my family. First, I check if the site or social media app is safe and then I put my information there. Now, I just want to be happy so if the social media will be making me happy, I do not care sharing my information.

The risks of sharing information is, my information like image, passwords etc., but can be used to make false identity and to make false announcements on the internet. I think its risky if we share our information about our banks account because it can be stole by any hacker, since there are a lot around the world. we should also be carefully sharing our sexual

information, like our interests and genders because of the people who have mental problems about the kind of situation.

Interview 49

Yes, I’m concerned about my privacy. When I have to send my personal data to any site i always check the site, the story of website how long it is on internet, the CEO of the site. My biggest concerns about my privacy are database's leaks, also I’m concerned about someone breaking into my account, which happened to me before on my social media. I'm worried about that someone might break into my bank account and steal my money or make debt on my ID and that I would have to pay for it

My best situation to manage my privacy shouldn’t exist. I don’t know why I should share my ID on a Facebook profile or other social medias(different situation for bank, business accounts). That would be ideal for me but I know that Facebook requires you to send them some verification, so the data that I send to them should be only visible to a small amount of people. They should be stored on a some top tier protected storage, cloud so there couldn’t be any leaks

Firstly, I don’t share information about me when I don’t need to, when some website tells me to share my phone number with them, I'm quitting from this website. Also I check my email address on a haveibeenpwned.com frequently and I try to change my passwords on a different websites every year. I don’t download any stuff from sites that I don’t personally trust, like torrents.

I’m considering the benefits of the website which i try to make an account on. Like bank accounts, that is needed for a living, or sharing my information on trusted stock markets.

When I come to conclusion that website is asking for too much and I won’t be using that website for long period of time like some online shops, when I would want to buy only one item in that shop and I would need to share with them my ID or link my bank account then I quit from ever making account on this shop.

In aware of the risk about the information that I share, I know that every site can become vulnerable to hacker attacks and data leak's so I try to cut that to a minimum. I know sites that I send my ID on or share my phone with them and when I will hear about some leak or something like that I will restrict my bank card, I think the risks are minimal when you know what are you doing on the internet.

Interview 50

My biggest concern when I go online, is my data being collected with cookies. I've studied about this subject and nowadays every site collect cookies. I really think that big companies are extracting our data. It is very frustrating to see our data being used to demand publicity for us. Facebook for example is one of the companies that does this. To finish I'm really concerned about everyone privacy, because internet isn't a secure place anymore.

I think that the authorities of each country, should have access to the entire code and ensure that all international and national rules regarding data are complied with. It makes no sense that they can manage the data as they please and for the media they want. I always try to block cookies and erase my trail on the internet. I also feel that people should have more knowledge about what's going on with their data. But in the case of my country, we have an elderly population in social networks, which makes everything more complex.

I had talked about this topic before. But we can use various technologies such as the use of virtual machines and VPNs. Personal text encryption would also be an excellent method however I am aware that it is a very complex area for most people and having to change mindsets is neither easy nor quick to achieve. Just starting to implement methods in the virtual education school would be an excellent idea.

I think there is no benefit whatsoever when it comes to obtaining data from people. I think that companies only use this for their own benefit and so that they can increase their sales, which is why I mentioned earlier that the authorities should be aware of everything that is happening on the internet.

The internet can be an excellent platform if it is used for good and not for extracting data from those who pass there.

Interview 51

I am concerned that these networks have access to my data and can use it however they want. Everything that goes on the internet stays on the internet and I'm afraid that one day I will regret publishing certain things. It is really scary realize that internet control our lives. I worry about the exposure that the internet causes and the way that exposure affects people.

When entering one of these platforms, it is mandatory to submit some of our data. But I think that in order to better control our privacy, we have to expose ourselves less, because the more we expose, the more data we are providing. The most basic way to control privacy, is to put the profile in private and only allow access to people you trust. When someone has children, it is also important not to expose them for their safety.

I confess that despite worrying. I am not a very careful person. I feel that I should be more careful when browsing the internet, as I know the risks that this brings. I am a person who does not publish many things on social media and in that I consider myself careful. However, I go to many sites and submit my data, clicking many times on the part where I declare that I have read the terms and conditions for the use of my data and I have not actually read it.

For me in particular, the only benefit it gives me is freedom of expression. But I realize that for many people it is an incredible platform to expose and share their work and projects. The truth is that when we share private information about us on internet, it doesn't bring us so many benefits. It brings benefits to the people who control the information and have access to it.

When I share this information, I don’t worry too much about the risks, as I’m usually doing it for some purpose. I am more concerned about this when I see documentaries or people warning about the dangers that this entails. When I share this information, I am aware of the risks and I set a limit on certain sites, so that they do not have access to data such as the telephone number or identification card. There is certain data that I refuse to put on certain websites.

Interview 52

I wish that the sites won't sell my personal data, and I hate seeing my data on ads... Also the protection of private life is essential since a possible injury might be impossible to repair. Everyone is aware of the invasion of private life caused by social media with a distinct emphasis on FB as the first mover in this business, but in the end only refers to possible financial damages. In my opinion the safety of the internet transactions is only a secondary aspect of a much bigger problem, which is protection of data on internet.

The privacy issue definitely bothers me, we should be way more concerned about the way corporations make use of our data. Facebook data privacy scandal centers around the collection of personally identifiable information of "up to 87 million people" by the political consulting and strategic communication firm Cambridge Analytica. That company and other were able to gain access to personal data of Facebook users due to the confluence of a variety of factors, broadly including inadequate safeguards against companies engaging in data harvesting, little to no oversight of developers by Facebook, developer abuse of the Facebook API, and users agreeing to overly broad terms and conditions. This is my opinion on Facebook with some parts taken from the web.

I don't like to share my location and my personal data. I try to use socials as little as I can. When that information gets posted online, it is no longer private, and may end up falling into wrong hands. Even if you have put in place the highest possible security measures, some of your friends, colleagues and companies you interact with on social media, can end up leaking your personal information.....

I hope that the information will be useful, phones with cameras make it very easy and alluring to share photos, and it is understandable people want to share. It is also difficult to argue that every posted photo is going to lead to a scam or be hacked. The more photos reflect

the context of a person and their relationships with others, the more that person can be denoted by their location which in turns allows hackers greater access to personal information.

The problem is that there are so many photos of people, he says. There is a possibility that someone will attach a name to your photo. If you appear in a photo of friends who also have been tagged, people with malign intent can try to trace these relationships and use them to fool people into giving up information. It is amazing how much stuff is out there about everyone, and what people share about themselves, often without being aware they're doing it.

Interview 53

I think it's really important to have a knowledge about being safe on the internet. I'm currently using VPN on my browser and I also own an antivirus program which has firewall so I can feel really safe during surfing on the internet and I'm not really concerned about it. If I wouldn't have all of those safety things I'll be concerned about my front camera, private files, etc.

In my opinion the best way to visit social media with feeling of privacy would be using fake accounts to avoid being recognized by the system. I also recommend to use VPN and avoid clicking some suspicious link. Sometimes your friends may get virus and text you with that kind of malware/spying links. However I don't think that we should be afraid of every place on the internet

Honestly the main reason is that I don't want to be hacked and I really care about my data. Especially about my bank account, social media accounts, etc. I used to generate different passwords with symbols and numbers. I believe that there's no way to scam me by any obvious way like fake link or keylogger. I've never given my personal information to any stranger on the internet.

I can share my private information online when I'm announcing something on eBay or if I'm looking for a job and I want to appear like a person who is trustworthy. Honestly I don't like to do it and I'm doing it only if it's needed. When you are honest with people they like you more and you can start your own site on Instagram or Facebook. That answer was really hard for me because I don't like to share information about me online.

In my opinion, sharing your data on the internet is very dangerous because strangers who have bad intentions towards you may use your personal data in an inconvenient way for you. strangers who have bad intentions towards you may use the fact that they have your personal

data to hack into your bank accounts and deprive you of money, or they may impersonate you on the internet for malicious purposes.

Interview 54

I am sometimes concerned about my privacy. When I upload a picture of myself I do not know what someone can do with that photo. For example someone can steal my identity somehow and write some horrible stuff to other people. Moreover sometimes I am afraid that someone is capable to hack my phone and can see all my pictures in gallery, private messages, passwords, notes etc. I am also stressed while doing online payments because I always imagine to myself that a person could hack login and password to my bank account and steal my money.

I always try to have really hard and complicated passwords on my social media's accounts. I think I have good private settings everywhere. I do not accept every friend request on Facebook, only people I know in the real life. I do not chat with strangers. On Instagram I have a private account and I also do not accept every follow request. But I know that there is always a risk despite all of that.

I have some rules. For example I do not post too many things from my private life and photos of my family members. I do not share private information about myself (where I go to school/ work/ my address/ my telephone number etc.) I have strong passwords everywhere. Moreover when I travel somewhere, I do not share my exact location when I post something online (only after I leave this place and feel completely safe).

When I was younger that had more benefits. For example- one could see where someone goes to school. And when it was the same school as yours it was a nice reason to start a conversation or ask about this school (when you were considering to go there). But now I do not see so many benefits of doing so. I think that when I am older I am trying to be more safe on Internet because I am more aware of the risk of sharing too much private information.

I am aware of that risk. For me it is very important to keep my accounts on social media so safe as possible. The risk is huge. These days everyone can check your address or other private

information when you are not careful on Internet. And many horrible things can happen because of that. Everyone should protect its privacy and take it really serious.

Interview 55

When I go online, I already know I won't be incognito, so I just accept how it is. I know my information will be used to present me with advertisements that fit my persona, for example, and the only reason it stays like that is because there are laws that prevent more. I wouldn't call it concern, though. I don't like that it is this way, but I don't think I can do anything to prevent it, because I will always have to use the internet for work, or for leisure.

Obviously put in as little information as I can. But, it will know my interest just based on the pages I follow (which is the only purpose of those sites) so, just by using them, I will give to the site more information than I would like. Since I can't control that well what those sites know about me, I just don't care, I just accept it and use them as long as I feel safe doing so.

As I stated previously, I just accept that other people will not respect my privacy, so I just use what feels safe to use. I don't really think about what info will be stored about me, and just "go with the flow" :D. We will evolve to be more and more controlled, so, in my opinion, we should just embrace the saddening future that embraces us. Good luck to you all! :D

Well, it all depends on if I feel like my information is stored in a place where people cant misuse it. Any sites I don¬¥t have confidence about, it is very possible that I will give fake info, or try to go around it. Basically, it all depends on how bad I need what the site has to offer and how safe the site feels. It never feels very safe to put my info anywhere tho :D

I always think on how safe is the site and how legitimate it feels. I will only put in my information if I really need it, and if I feel that it will not be misused by third parties. Basically, it all depends on how bad I need the service that the site provides and on how safe the site feels. It never feels totally safe to put my info anywhere tho (even irl!)

Interview 56

When I use the internet, I am a bit worried about my privacy. But I know I have to be safe. When I am not using my webcam, I have it covered. I am also careful about what I post on the internet because it is a public place and almost anyone can see what I have written or posted somewhere. I remember to log out of accounts that I used before. I take into account the possibility of hacking into my account etc. Safety first of all.

I am careful with what I post. I don't show my private life on Facebook, Instagram and other social media. As mentioned before, I log out after using the page. I also take into account what I write to my friends and send them in a private conversation. I am aware that a hacker could enter my account at any time and use various information against me. I try to be careful and I think it works out for me.

First of all, as I mentioned before, I am not presenting my private life online. I also ask my friends not to mark me in the photos and I do not publish them myself. In my settings, most of my stuff is set to private, for example, my friends list is only visible to me. I rarely write comments so that it isn't so easy to get any information about me. There is little information about me on my profile such as where I live, my relationship status, etc.

I only provide the information that is necessary to set up an account. I am very happy that specific data is protected by a privacy policy that allows me to live with the awareness that my data is safe. I also like the option that my personal data can only be seen by me, for example, my date of birth. I respect that when the website is not collecting detailed information about me. The sense of security also gives me the opportunity to refuse to use my camera, etc.

There is always a risk. It all depends on the website and its privacy policy. In my opinion, the greatest risk is on websites that are not very popular, especially when they collect detailed information about you. Hacking attacks or data leaks happen many times, but what I publish and write can hardly be used against me. I am only afraid of behavior in public places that I

will not log out of the account and someone will be able to read my private conversations and spread things further.

Interview 57

I don’t have many worries because I know how use Internet ,but my biggest concerned will be data lick from website like amazon or eBay. or scam product sell and reason for that is pretty simple I don't like to be scam. other then this too example, nothing worry my when i go online and that because I’m host my own website and I know something about online security.

I don't really know I must accept cookies or I can't use a social media so I do not have much to say in this case. on my social media I share only things what I want to share or show. things like some photos of me or some share mems with my friends so I do not use social media often. for example I practically not use Facebook any more, I use more messenger but this isn’t social media, only social media what I use regularly this will be Instagram.

I try to protect my privacy online using many ways by just checking certificate HTTPS on every website I have been, and I double check is website is legit and I don't give my personal data to website what looks suspicious or not right on any way, I have on windows defender, I don’t use links send by person I don't know and I don't trust, this is how I protecting my privacy online

Identity theft occurs when someone gains access to your personal information and pretends to be you online. Individuals who have accessed your personal data can retrieve your login information for various websites or commit cyber crimes such as tax fraud, all while posing as you. Identity theft is the type of crime that can have long-lasting repercussions for both your digital privacy and your online reputation.

I only sharing information what is called "safe data" by that I mean data like weigh or some information about appearance or what food I like or my hobby this is harmless information unless you are creepy stalker or rapist, other I that I do not sharing any of my personal data like where I life or where I like to eat and what I like to do in my free time.

Interview 58

Yes, I'm concerned about my privacy. I'm afraid that someday my boss or someone important will find something "stupid" about me in the Internet or that something will leak because of no control of what I'm putting on the Internet. What is more, I'm aware that every move on the Internet leaves "footsteps" so it's definitely concerning, because after searching for, for example, shampoo, later I have a lot of ads about this shampoo. That shows that we have no privacy when using the Internet - someone is watching all the time - cookies.

I think such sites should primarily not save our recent searches, on the basis of which they send us ads later. it's a bit scary because we feel like someone is following us. besides, I would feel more privacy if there were no anonymous comments option, if everyone could only have one account - it is known that loads of people use social media to observe people in an unhealthy way, which violates someone else's privacy. besides, anyone who does not have an account should not be able to view a person's account on portals.

I believe that the protection of privacy is very important. Everyone should be careful what they put on the Internet, because as we know, nothing is lost on the Internet and what seems irrelevant to us now can be very disadvantageous, for example, at work. Besides, I think that everyone should take into account that by uploading something to the internet, everyone can see it, and not necessarily what we show to our friends should be shown to our family. as well as the fact that cookies track our every move.

Actually, there aren't many benefits that come to mind, but if I had to choose something, it's probably that when you put something on the Internet, you can show off to your friends. Vacation, significant other or whatever. It can help us in our social life, it can make us better perceived. Maybe we can find some friends because of that. However, I still think that privacy is more important than showing anything to friends, so it's hard for me to find more benefits.

I always pay a lot of attention to what I post on the internet. I value privacy, I think that I do not want the whole world to know everything about me, that in the future I would have to be ashamed of what I put on the Internet in front of the employer, which is why I make sure not to post stupid things. I always think a few times before anything lands on my social media profile, so I really appreciate keeping my privacy in check.

Interview 59

Normally when I go online, I am not too much concerned about privacy. Considering data is normally harvested from a lot of people and sold in packs, I am not really afraid that someone specifically checks my data since no one really cares about what I do. I am not really concerned that I'm being sold in big racks of data amongst all other people because it is inevitable that we all are being sold since we all use the same apps from 3 companies.

The ideal situation would be to just simply have control over what permissions I give and are specifically shown to other people. However, considering that most of the applications just care about your money, that would never be implemented. I think that most of the people that use those applications just don't care what that means. The big corporations however really care about the data that they can get out of you so it is really profitable for them.

My values in pertaining my online privacy are that I want to be in control of what I publish and what is shown to the people I want and when I want and if I want. Once upon a time I used to really care about the privacy because I was afraid of people in real life knowing my online persona which I tried to hide from real life. However, I think as we grow older we usually stop caring about that and are just fine from what is on the internet.

I think that people normally don’t really care on what information they share online when they are older because we grow to understand what we are and stop trying to hide our online identities. With that I think that we do have some benefits if we just go along with it but should also know what are our limits to make sure that they aren't broken by the big companies.

I think that we care too much about our online privacy because everything is already online and we know that the big companies can get all the data they want even if we don't consent so we aren’t really in charge of what we have online or not considering we actually did care. It is known that we, as we grow older stop caring that much about what we share on the internet since we see a lot of old people sharing information that thy shouldn’t on the internet.

Interview 60

Most of the time I go online I am not thinking much about my privacy, unless I am doing/searching something I preferred to stay private. The only things I normally am concerned are private information like where I am, my passwords and other important information about myself that could be used for something harmful against myself or my family. I think growing up using the internet made me less concerned about online privacy, as it become something so normal that I don't think much about it, unlike my parents for example, who seem much more aware of it.

My ideal situation would be my location stays private to most parties, and especially from anyone that might want it for harmful reasons, same goes for my passwords, private photos and maybe one of the most important ones, my messages, as most messages are exchange with privacy in mind and the breach of such would be not only harmful for all the parties but a really big invasion of our privacy.

I use incognito mode from time to time, especially when I'm looking for something I really want to stay private, I try to limit what I share on social media, always keeping in mind that most things rarely stay private to the public target I had in mind when sharing, I stay away from anything that looks sketchy and as such could compromise my privacy. I also try to share the least amount of private information I can like names, passwords, where I live, where I am when posting something.

I weight the benefits of sharing something online by understanding how important and private the information is versus what I'm getting in return, for example sharing my name and an email to get an Facebook account is a trade that seem acceptable, but if I was being asked for phone number, and exact location, bank account and other more private information it would no longer be ok.

If the information I'm sharing doesn’t seem to be putting me in great risk of identity theft, or money theft, like sharing my bank account information, or physical and mental risk like sharing my and my family's exact location and potentially getting robbed, or stalked I then assume it is fine to share online and worth the risk of putting out there.

Interview 61

In general when I go online I am not worried about my privacy but sometimes i have some concerns such has being robbed or scammed by a site or person. Despite of that i can live with that can of concerns i just turn on my VPN to by a little bit more safe. To conclude the internet is a pretty safe place i just think that a lot of people take advantage of innocent people that are not prepared for the danger of the internet.

Visiting social media like Facebook, Instagram, twitter, tinder or even YouTube and twitch your privacy its very important to then so you are pretty safe on there site but would like to know the type of things that they can get from my logins and what type of things they do with that information. So that said i would like to have a setting that said where, what and when will they use my logins.

Online privacy is important for numerous reasons. You don't want to share details of your personal life with strangers and it's hard to be sure what personal information is gathered and by whom: information collected by one company might be shared with another. You might be uncomfortable with bespoke, targeted ads that remember your internet search history. Even more problematic is information sold from one company to another, or data gathered and shared without your consent. Ultimately, this is identity theft.

Identity theft occurs when someone gains access to your personal information and pretends to be you online. Individuals who have accessed your personal data can retrieve your login information for various websites or commit cyber crimes such as tax fraud, all while posing as you. Identity theft is the type of crime that can have long-lasting repercussions for both your digital privacy and your online reputation.

Identity theft occurs when someone gains access to your personal information and pretends to be you online. Individuals who have accessed your personal data can retrieve your login information for various websites or commit cyber crimes such as tax fraud, all while posing as

you. Identity theft is the type of crime that can have long-lasting repercussions for both your digital privacy and your online reputation.

Interview 62

To a certain extent, yes, but clearly far less than many others. For example, I feel no need whatsoever to hide my age, nationality, or hometown. I also don't feel very reserved about sharing photos of my surroundings. Even my name feels fairly safe to share since it's extremely common in my country, but I don't just throw it around, either. My face is something I only share in places where I feel completely safe, but I'm totally fine with complete strangers hearing my voice.

I'm not sure what this question even means. I appreciate the fact that most social media platforms let you make your account and posts private if you want to, although I've never used that option myself. In general, the more I can customize who can see which of my details, the better; it's nice to be able to choose between several visibility options like everyone/friends/no one for each piece of information. I also want to have the option to limit the data the site itself collects about me. Facebook must die.

I don't want random people to be able to find my real identity based on semi-anonymous interactions, but it's fine for people I know and trust to know who I am. But even random people can have any information that'll keep the conversation going as long as it doesn't break the above rule. At the same time, though, I want advertising companies to have as little information on me as possible, as I would like for them to burn in hell.

As far as companies are concerned, I'm willing to share a lot as long as I get something somewhat tangible out of it. When dealing with individual people, though, I'm a bit more reserved, but just participating in a conversation or even just making a joke is still enough to get quite a few details out of me. The closer I am with the people who can read the conversation, the more I'm obviously willing to share.

Will a complete stranger be able to find my real-life identity based on this? Will this information be sold to a dozen advertising companies immediately? Does it look like I'll start

getting spam calls or emails because of this? These are the main risks I think about, and while I'm willing to help advertisers build a better profile of me if I get something nice out of it, if I think the answer to either of the other two is yes, I won't share anything.

Interview 63

Personally, I am concerned about not knowing what kind of people can see my personal information and also how the website uses it. I am also concerned that they may take information about relatives or close people, as well as children or young minors.

I am concerned that they may extract photos or documents from my devices and that they may be published. Another thing that worries me a lot is knowing that my conversations, photographs, documents, bank information, etc. can be seen by the creator of the web platform.

My ideal situation would be if they did not ask me for personal information, without providing my phone number, just confirming my identity with an email. That I could not receive messages from people I do not have added, that people I do not know cannot see my publications, or photos. Make sure that the information I give cannot be used by them. That my information or things that interest me are not provided to third parties, so that it is not invasive advertising and that I do not have to provide information about my location.

I believe that online privacy has to be very clear and honest, each person deserves respect and freedom to be able to share or express what they feel without fear of feeling observed by people they do not know and also, the creators of the platforms have to be responsible with the information that can be deposited on their websites to provide greater reliability to their users. There has to be a cooperation from both parties to create a safer society.

I think it has benefits and also that it has no benefits, it is useful so that the platform can get to know you better and can offer you things that are to your liking, so that they can provide you with a better service, but it also has things that can be scary to people, how much information do you provide, how much do they know about you and how far that information can go, if it can fall into more than people who do not have good intentions.

In my personal opinion, the risks are high, as I mentioned before, you never know how far the information you provide to the page goes and if it is really safe there. I try not to provide

information that puts my safety and the people around me at risk, in order to live in peace. I think platforms have to be clearer and more transparent to create greater reliability.

Interview 64

I am actually not concerned, even though I know that there is people that thinks that they can be stolen financial information or personal photos and that stuff. I thing that I use protected web sites and even if I can be stolen information I don't think that I am a super famous guy to be chased to rob some of that. So I am pretty confident when using online sites.

Just not accepting unknown people and try to avoid any questionable page. Not giving important information through messages and not posting private information. I have never been hacked or had any problems of security. So I think that is useful when protecting privacy. Also, not writing my passwords if I can not verify that it is the legit place or maybe not using the same password all the time may help.

As I said in the past two questions, is important to verify your pages and not accepting weird people. Maintaining your passwords save in a notebook and not sharing important stuff in messages. Being aware of every movement you do even if you are on a safe page. Not using public internet to navigate into your important pages and not sharing any passwords.

There is some benefits like getting personalized adds and find something you were interested in. Share the location may help for security help and maybe to avoid any kind of fraudulent moves sharing personal information works. The bad side is if someone manage to hack the data base and get into all that information that you don't make public. Anyways is kind of hard to be the one hacked, the security has been improving since the beginning and everyday is safer.

Is pretty dangerous, as I said, cause someone that you don't know can manage to hack the site or if you post it publicly you can give bad people information useful to do criminal activities that may affect you. When sharing private information online you have to know

which kind of information you are sharing and to who you are sharing it, even though there is always a chance to be filtered and getting public or used to bad things.

Interview 65

Since I don't post much about my personal life I really don't have that much worry although I put my account private sometimes to manage who sees my profile. If I was a person who posted a lot about my personal life I would be much more worried about my privacy and worried about who was seeing my posts. I really think that people should be careful with what they post online since everyone can see it.

I would manage a lot my account, seeing who is following me, who could see my posts, maybe changing my account to private in case I didn't feel safe with unknown people seeing my private life. I could always block someone who's annoying me or unfollow someone who's acting weird.

But I think the best way to deal with it is to share your private life only with your friends.

Well since I don't share a lot about my life on the social media usually I don't give much attention to things like that, normally what I do is in case I change my account to private I only accept people who I know or people that don't seem to be there only to hate and things like that. And if I don't have my account in private and I want to share something more private I share only with my friends or with the people who I want to share that with.

I only share something personal if I know that it would not have much deal in my life if it gets in the wrong hands, If it is something that I feel comfortable in sharing I think it isn't that important. And if I'm sharing something it's for people to improve and learn more, I would only share things that are interesting for me so I don't worry about posting it.

I only share something personal if I know that it would not have much deal in my life if it gets in the wrong hands, if it is something that I feel comfortable in sharing I think it isn't that important. And if I am sharing something it is for people to improve and learn more about it, I would only share things that are interesting for me so I don't worry about posting it.

I don't feel concerned about my privacy when I go online, because I don't usually post a lot of my life on social media, however, I guess that if I did I would be okay with it because I don't think there is much to be afraid of as a man.

In my opinion, due to our society being sexist and misogynist women have to be more careful about those things, and so, can't be as careless as men are.

In my opinion, when visiting a social media site the ideal situation to manage our privacy would be that no one was able to take screenshots and only allowed people could see our posts. That would cause a problem due to the involvement of influencers and famous people and so there should be different rules for them.

However, most people go to social media with the objective of being noticed and so wouldn't agree with this terms I don't have a lot of individual values pertaining to protect my privacy online, I simply don't post anything that I don't want to be seen by people who I don't have a lot of confidence with so that my information doesn't end up in the hands of people who should not have it, however, as I had said before I am not very worried about it because I don't post a lot.

I only share my private information online when I really have to (such as shopping online, buying tickets, or paying for vacations), on social media I do not post anything that I feel like should not be there because in my opinion, the benefits of doing so are so low that only when there are no downside you should do it.

In conclusion, I do not post anything without weighing the pros and cons of it. I usually am careful with how much personal information I reveal online. Sharing your phone number, birthday, address, and other personal information can mean you are at a greater risk of identity theft, stalking and harassment. This includes information you post on social media such as Facebook, Twitter, Instagram, or any other social media site. Your personal information can

provide instant access to financial accounts, credit record, and other assets and so I am very careful about it. Anyone can be a victim of identity theft.

Interview 66

Yes, I'm concerned. I very rarely post anything under my own name. I don't want people I know in real life to be able to find me online. I'm cautious when I log in to my bank account and government websites. I'm sure if someone searched long and hard enough, they could some information about me and my accounts, but I doubt they could connect them to each other. Most of the real stuff is beyond my control (e.g. info on school websites), so I don't see a point in worrying about it too much.

Being able to turn off every personalization and ads or sponsored posts (why do I have to see clothes all the time and my brother gets cars?). Option to like/upvote something without displaying my name. It's really bad on Facebook. I don't like or comment there, because my real life friends would see it.

What happens online, stays online. What happens in real life, doesn't ever go online. It's better to keep these things separate. That's why I refuse to tell Google my age (and why I hate AVMSD). Also, never the government with private information. I know they probably know all about me, but there's no reason to make it easy for them. And that's it, really. Privacy at the cost of an empty Facebook page.

I have to gain something. Delivery information is acceptable. Giving an example to illustrate a story, too (but nothing too personal, that could be used to identify me specifically). I don't think about it. It's more like an instinct to protect my privacy. To only give necessary information. In everyday life it's not an issue because I don't have many social media accounts.

The same way I weigh the benefits. I don't think about it. The default setting is not to share anything unless I have to.

I have no idea what else to write here to reach eighty words. I don't have an elaborate strategy of dealing with privacy issues. Maybe some people do, but I'm not one of them. What I do at the moment seems to be working for me so far.

Interview 67

Each one of us should be concerned about our Privacy on the internet. When we surf the internet data is stored physically and the companies that own these servers ideally own all your data. Your data can be put up for sale anytime. However, I do not pay too much attention to it, because checking each page separately would take a long time, which would make it impossible to use the Internet smoothly, and in fact, we are not completely sure what will happen with our data.

I would like to be sure that my data is safe on the company's servers when using social media. I would like to be able to decide if I allow the use of cookies or if I want to have personalized advertisements according to the information they collect about me. Social networking sites should be fair with us about the information they collect about you.

First of all, on the Internet, I want my sensitive data to be safe. I want to be sure that my passwords will not be stolen, that the data from my ID, my home address or my credit card details are safe on the servers of the websites I shared them with. I do not want to participate in a situation where someone takes a loan for me, will pretend to be me and will have my data only because some company has secured them badly.

I think that personalized ads are very good for me, that google offers me sites, groups, shops or things that interest me at a given moment and allows me to save time searching for them on the Internet. The information provided by me on the Internet also makes it easier to pay online and use my banking as well as dealing with official matters online.

I believe that the risk associated with sharing data on the Internet is large and you should be very careful with whom we share it. however, nowadays it cannot be avoided. it is a ubiquitous phenomenon and we must learn to deal with it to avoid being surprised later. at the same time, international corporations must pay utmost attention to the protection of users' personal data.

In most assorted websites I don't visit often I try to disable all cookies I can when they make it easy. But in websites which are harder to disable cookies in I often don't care enough to disable them so I just leave the website or try to find a way to work around it. I'm worried about how much of my data is being shared among varying companies since I'm aware those companies are way less varied than it seems and by analyzing which websites I visit they can make a very detailed profile of who I am and how to better advertise to me. I also worry about my privacy in social media considering the amount of time I spend there and how much of my information it holds but considering how much harder it is to avoid social media I dont make as much effort as I'd like, even though considering how my number was recently leaked through facebook that makes me more willing to make changes.

Minimizing the information I share publicly and privately through the social media, having the different ways through which the company collects my data be explained in a plain and understandable manner and allowing me to disable all the mechanisms of data collection I wished. Also having the option of using a VPN be allowed, to minimize how much of my information is shared to other entities.

I try to protect my data as I can, but often I don't care enough to look into all the ways a company tries to collect my data and either avoid a website or just use it anyway, though if the website has a small owner who needs the income related to ad revenue I am happy to turn off my ad blocker and use it anyway. However, in situations were the data collection is extreme, such as the planned change of WhatsApp ToS on data collection, I will boycott the service no matter what and search for alternatives.

I try to weigh in both how important the information or service I seek from a specific website is to me, how much I'm willing to care about my information at any given day, how easy it is to disable all cookies I can, whether or not VPNs are allowed and whether or not the website has a small owner who depends on my traffic. I tend to be a little too lenient out of

laziness but in specific extreme situations I will make any changes I can to avoid losing control of my information.

I try to avoid sharing private information at all costs, but depending on how important the service who asks me that information is to me I will allow it. The degree of privateness of the information required is important as well, and how often I use the service and how well I know how the service deals with private information. If sharing with another individual online I tend to weigh in how much and how long ive met the person as well as what I am using to share that information through.

Interview 68

When I go online I'm always concerned, nowadays the concept of privacy is a simple lie we tell ourselves to ease our minds, the way big companies can track our desires a recommend products that they heard in a conversation or found by looking at our search history is my biggest concern, the 24/7 monitoring is the biggest fear. Therefore I search for alternative ways such as different browsers that don't keep cookies or VPN's to keep me protected.

The ideal situation would be to have full access to my recommendations and the algorithm they use to cater to the people, being able to define what I want or do not want to be recorded and targeted at me. Also have an option to totally reset that type of information or see the logs stored about me. Having a private page where only people that I want could access could also be a plus, the current private accounts still puts us out there in the search finds.

I think all information should be accessible by the ones that create it, meaning that I should know what they know about me and even declare what I want to keep private, the use of VPNs nowadays is a likely a must and I recommend but still our security is deposited in yet another third party corporation, we currently don't have a first line of defense based on the user itself, so that is the point I would give most value.

I always share private information with a big level of caution, I tend to search about the site I'm sharing it with, if it had problems with other users, if there is a way I could create a barrier between me and the site itself, as in, using a post office instead of a real address or create temporary credit cards for payments online. When using a VPN I like to jump between IP's as to not stay connected to the same one in consecutive days.

I'm always attentive to the risks, as I mentioned before I always search about the site and company behind it, see the other customers reviews and see if they had any recent mishap or scandal, I tend to always protect my payments as well as my address, name and likeness, always

creating different emails for different sites based on the trustworthiness of each, even if I'm 100% sure about the site I still take precautions.

Interview 69

Sometimes yes, sometimes no, when it comes to very private, sometimes I worry not to leak it on Facebook, which I use a dozen times a day, if it is about less private and confidential information, I do not share it on the Internet, so I do not have to say about it bac it is worse if he writes some private messages with family members who put less emphasis on being more anonymous on the internet

The ability to encode messages with a password or something like that, preferably coding on the server, which makes it more difficult to hack messages and delete them so that you can permanently erase them and someone who allows it will have access to my account or phone will not be able to read them then I would feel there is nothing to fear, Facebook could follow the same path as the TOR or telegram

Personally, in order to feel safe on the Internet and not to be afraid that something private will leak or be acquired by a hacker or a person who steals my phone, I try to use applications and communicators that focus on the user's safety, let's give it a telegram has a lot of nice security, which makes it very sensitive I write news just through him.

Big advantages of this can be seen on the sites for dating or meeting new people, let's say you meet a new person and instead of just a profile picture you can find out where he is studying or where he lives, which makes it easier to start a conversation or see if we have mutual friends or similar interests but Also, you cannot overdo it with providing all the information on the Internet.

First of all, you cannot give all your information at the very start because people who want to manipulate you often can let go if you are not so willing to give all information about yourself, the next risk is that people can pretend to be someone else on the internet just to do someone is hurt, so there are many pluses, but there is also a very high risk that you will come across a person who wants to do something to you.

Interview 70

My main concerns are about my personal safety. I am afraid that my personal data like ID number, address, etc. go public and people may use that data to make damage in my life. If a lot of this info gets leaked, things like identity theft may happen. Identity theft is by far my main concern because it can make you lose jobs, trouble with degrees, fake bank accounts that create debt in your name.

I use discardable credit cards to shop online, so I am not concerned about my money safety.

In my opinion, to create a social media account we should only need to give an email and name. The app should not be allowed to go get your cell number and our contact list. 35 If I want to see my contacts who have that social media, I should ask for them to search only if I want to, that should not be a default setting. The same thing happens to my location, if I want to see posts related to NYC instead of my city posts, I should be able to change it. By default the app should have access to no information of mine.

I have all my social media in private mode. I keep a very strict list of people that follow me. In Facebook, I have many friends but I don't post anything not related to work. In Instagram, I try to make my posts as plain and with less data as possible. If I want to post something more private, like my house or my ticket I use Close Friends. 68 In Twitter I post very little info, I don't post an expensive thing I bought or where I will be going later.

In sharing information online I weight the benefits. If it is something as simple as to get permission to access my contacts, in order to find someone account I allow it. But if I have to give personal data like ID number to a not so trusty site, I won't give it. So, I weight the importance of the data I am allowing the site to use, my trust in the website, what will my data be used to and, most important, what will I get in return of the data I allow to use.

When sharing info online, I weigh the risks of the data by validating how that data can be used against me. I am okay with sharing my contact list if I am asked for it. But if it is personal info, like my address I am not willing to give it. I weight the risks by analyzing how personal is the data I am giving, and if it is something you can find if you search it online. My degree says a lot about me, but if you search my name online you find it. So, it is not a risk to share it if I am asked.

Interview 71

Yes, I am. I am afraid of people trying to steal my personal goods, like money, data and identity. That is why I use VPN sometimes or other ways of encrypting my identity. But I also think that is not that easy to steal my personal stuff. And I always try to trust https:// websites, and that is a thing that I always look for when I go on a website that seems "shady".

I think I would be fine if there are some sort of options to enable/disable my agreement to certain things. Despite the fact that I know that Facebook, Instagram, Twitter, LinkedIn, etc. have access to some of my personal data, I would try to trust them either way because I think that those big companies will not try to use my data for another purposes. Anyways I would like that all social media had encrypted messages.

I always try to check if the website is https:// because, in a certain way, that means that the website have some type of security, so I tend to trust this websites normally. When I go to some "shady" websites I always try to use a VPN network so I can have my data secured. Long story short, I think that those websites have my personal values but I trust them either way so I can use them freely.

I think I value the pleasure and the advantages that that app/website can give me. For example, in a online wallet, I trust those systems because I know that I can take some type of benefit. On social media, I think that it is good to be aware of the risks but, in a personal opinion, I think they are good because they have various qualities, such as entertainment, some news, etc.

When sharing my private information online I weigh the risks by viewing the benefits that the app or website can give to me. If I like the website or app enough, I may tend to trust it more but I always check the privacy terms of the website or app that I am using so I can be certain about the usage of the website or app, so by doing that I know that the website is trustful.

Interview 72

I wouldn’t say that I worry about much, I mainly just wonder to what degree I'm being tracked and whether or not my experience is somehow "fabricated" by that. Besides that, I also worry about the amount of my personal information (and which) that is kept, analyzed and perhaps even distributed. Lastly, since I tend to do a lot of online shopping, I'm concerned by the possibility of having my banking info recorded. Although it is a rare issue, I still think it's common enough for people to worry.

When using any sort of social media or platform, I would like to receive as much information as possible regarding the future usage of my personal information. And, on top of that, a clearer and more easily accessible way to customize precisely which information I allow to be retained. It’s important to be cautious and ensure that you keep your personal information from getting into the wrong hands.

We all have things to hide. And when it comes to online privacy, there tends to be highly sensitive personal information involved. I don’t think these are the types of things you’d like broadcasted on your social network for the entire world to see. It's my information, my habits and patterns, and my actions. Nobody else's, that's why I take care about keeping it mine

Obviously, it has its benefits. Today you can access almost anything on the internet, from entertainment, credit and financial services to products from every corner of the world.

However, when weighing these benefits to it's more problematic counterparts, I'd say the latter have a much stronger, deeper weigh associated to them, taking in consideration that big issues can come to those who have their information stolen, for example.

Taking in consideration that just about anyone is vulnerable and can be a victim of identity theft, I'll consider the risks to be extremely high. From account numbers, passwords, and other information, when you put anything in an email, or social media, you are posting something

that has the potential to become public, I think we should act as if the internet wasn't private from the start.

Interview 73

My personal information being made known to the public. For example, my image, my address, my financial information. Also, I'm afraid big business or social websites might be able to track my information down and sell it on shady places or in the deep web. Another worrying possibility is my passwords being stolen in some way because my information is not stored in a safe way. Still, overall my biggest concern and the most plausible one is my private information being stolen.

My ideal situation would be me having total control of who gets to see my information. Being able to control who has access to it, or who it's shared with. Also, being able to delete all my information from the social media, all my photos and everything, would be an incredible addition. Also, it'd be good to know who downloads my photos, or who screenshots them. Also not being able to screenshot my photos would be good. Also I'd think it should be mandatory for social media websites to not be able to track what you search on google.

My individual values are very important. I never upload any personal photos, nor give any information about myself, as I'm very cautelous with that kind of stuff. I tend to not talk much about my personal life, though sometimes it probes to be very difficult. Also, it's important for me to not have my photo anywhere on the internet, and I don't like knowing that my personal information is somwhere on the internet, so I don't have many of the most popular social websites.

I just do a balance. I need to know if it's something too private, or if it's something irrelevant that won't do any harm for other people to know. If it's something irrelevant that I know will be funny or interesting to tell, I just do it, but if it gives out too much information I don't write

anything about it. Also, when uploading photos I'm meticulous it won't give any information about where I live or how I look like.

If I give out too much personal info I think about the negative consequences. For example, someone pretending to be me, or someone stealing my image for something, and if I give out personal information, I think someone might be able to use that information against me, or use it against my loved ones. Though I have to admit that when talking about the internet I tend to think mostly on negative terms, because I find it difficult to find something positive.

Interview 74

Sometimes I feel kind of insecure searching on the internet because all the cookies that the websites have, when it is needed my email or some personal information I always think twice and try to understand why they need the information, and I only write it in the sites that I know to be safe or if they are very known. The most thing I am concerned about the privacy is that it seems that people are pretending to be someone else or use fake accounts in the name of another person, and that can really affect our lives, personally and in the work environment.

Other people shouldn't see what I like and I always try to show photos or publications that are more private to the ones I know, but the reality is that I am friends in Facebook, per example, that I don't see anymore nor are my friends currently, I would like to be more easy to unfriend people that are not part of your life ate the moment. I don't post a lot of things in the social media so I don't feel that insecurity, but I feel that a lot of people exposes themselves, but, in other hand they choose to do it so they should know that it can have some bad consequences.

I think I am a little bit reserved when it comes to personal stuff like my home or my family, so to post something about it I have to feel secure about my privacy and the people that will see that. I am also very protective person so I would not like to be exposing someone that could have any problem after that post. I don't really want to know every detail about a persons life so I think that people shouldn't post very personal things because of that and thinking about their privacy protection.

Most of the times I think about what I post, but my social media accounts are all private so only the people I accept to be my friends see what I post. Sometimes I don't think that much, most when I am travelling or with my friends doing something different that I consider interesting, I like to share with the people that follows me. The benefits can be so many, we

can be more connected through the things that we share and it can star a lot of conversations about that topic I posted.

I weigh the risks in the most of the times, I don't post anything too personal or about my relationship, or my family or friends that wouldn't like me to post, I always ask permission to post things about the others. In my case I think the risks can be a lot, like people stealing my identity or creating some false rumors or sign up in some sites in my name.

Interview 75

Not really. It depends on what sites I go into, if I go into sites which is owned by big companies, I'm not scared about giving out my information. If its a website I don't really know about, I will be more careful with what I say. Social media wise I have private profile on Instagram, but I accept almost everyone anyways. I have a lot of different social medias and I post a lot about my daily life so for me I'm not that concerned about privacy when I go online.

If I understand the question correctly I think its good that Facebook and Instagram for example have many different privacy settings, which you can change to however you prefer it to be. For me I have private Instagram because I'm afraid of someone that I don't know to know private information about me. I think it should be even more specific privacy options that you can choose, so maybe even more people will make an account on it.

I think the most important things to hold private can be your name and location. On Facebook etc. its easy to find out your school, family and everything. On Instagram it can be more difficult. But I think as a 19 year old boy I feel more safe, thinking that a girl that is the age of 14 should be more careful, having private accounts on both Instagram and Facebook.

I don't really think about it that it matters for my part. For me for example when I show the location of where I was, its just for trying to make people jealous if I have been to a famous place, or just adding a place to try to be funny. I don't really think about the negative sides of it, which I probably should do. Well I Norway its safe anyways :).

I think that I feel more safe because I live in Norway, so if I share pictures of my family members or my location I don't really think something will happen. I would have been more careful if I was on a travel in another country where I was not known, especially if my account was public. Because then strangers would know where I lived. And people think Norway is rich so, even more dangerous.

Interview 76

I am concerned about privacy because I use a lot pages like PayPal and bank accounts. I know that google takes my information to improve the experience of ads and that's ok with me. But I am really worried because I now know that I am really not invisible in the web and everything that I do someone can see it. It's strange but I still don't share so much information to prevent a bad event from happening. That's what I think.

My ideal situation would be not to share a lot of information about myself, to keep my sensitive information out of the social networking sites like Facebook, because I know it is not safe, due to the large amount of news about data breaches. This is the best I can do to prevent my information from being posted on these sites. I also think Instagram could be a good site, but it is also dangerous. I really don't know what they do with my information.

I think they need to protect and respect my information, keeping it safe from bad people. And they must also respect my opinions, many times I have seen censorship because someone does not think exactly like the people at the top of these sites. That is sad, but I think it is very scary and at the same time it is a difficult situation. In history there have been people with excellent ideas who were considered ridiculous in their time. But also bad people.

I usually think: is this sensible? Is this information that could be misinterpreted? Is this information very important because it is about bank or payment? Is this offensive to people? It's hard, so I really think I'm limited on many occasions to really express myself. If it is something that does not belong in the questions, I post it, if it would make someone happy with my post, then I proceed to do it, otherwise I save. The social media life is hard.

If it is something that could be risky, then I do not post it, as offensive to some group and sensitive as rude medical images (because I study medicine). Facebook already has a lot of censorship, so I limit myself to only posting memes. I consider myself a person who does not

have radical opinions, but I really like to read different opinions because that is diversity in the world. If all opinions were equal, the world would be boring.

I am concerned that someone would be tracking my online activity. I am concerned about data collection agencies selling my online activity data to advertisers. I am concerned about the government spying on me for no reason. I am also worried about online spammers, phishing emails and other such hacking methods which could be used for malicious purposes.

The ideal situation would be to not provide too much personal information to these social media platforms. It would be good to know what kind of data is being collected from me. it would also be good to know if I can get the data deleted from their servers and what kind of purposes they use my data for and who can access it. other than that, it would be useful to have options to easily connect/disconnect/block certain users.

Personally I am not in favor of online websites collecting too much personal information about me because of privacy concerns. I try to give as little data as possible in order to use any service. I am okay with giving out general demographic information about myself but anything too specific and I am concerned. I use all sorts of tools to try to protect my privacy.

The only benefit is when the website or the service I am giving my information is really important for me to use. in this case i don't hesitate when giving out my info. one example of such a service is money transfer websites. they really need my information so as to check for money laundering etc. so I won’t hesitate to give out information. in case of less important services like music streaming etc. I try to give as little information as possible.

I always think about what would happen if my data gets leaked, would I be personally threatened? for example, would my physical safety be in danger, would I stand to lose financially because of a data leak. this is what mostly my line of thinking is when I am providing information online. other than that, I don’t think much about it when giving out information online.

Interview 77

I am sometimes concerned about people such as hackers finding personal data. There's always a risk that your computer could be exposed to malware or viruses that can steal people's private information, including things like addresses, passwords and financial info. In terms of privacy it's also concerning as the internet is mostly an anonymous place and I think knowing that there's a risk of being hacked etc. is a worry.

In terms of social media, I'm concerned about strangers seeing what I post. The ideal situation to manage my privacy would be that my social media accounts are set to private, meaning that someone will need to send me a friend request to see any information about me or the things I post. Also having backup passwords and backup emails and thorough security checks so that it makes it harder for hackers to access my account.

Personally, privacy is quite important to me. I think that the internet has potential to be quite dangerous. In terms of my values about protecting privacy, I think it always pays off to be safe rather than sorry and to go through the effort to set up those things like backup emails and things so that you're at less risk of having your internet privacy invaded. I think privacy is very important and more people should be taking action to ensure their internet activity and social media posts are also private.

It depends a lot on the sites and what privacy criteria those sites have. If it's on Facebook, for example, where you can set privacy settings so that only your friends and people you know can see what you post, that's okay. If it's an anonymous internet forum such as Reddit I would be very wary of sharing private information to the masses, and I think there would be almost no benefits and many more risks. Sharing private information online would only be beneficial if I'm certain that it is released in a controlled environment around people I trust.

I weigh the risks depending on the sites. In an case, I think all online sites have risks when you share private information. If strangers will have access to this private information, it's a

huge risk and I almost never would do it myself. However, if it's a site where I can choose who sees my private information, this minimizes the risk a lot more and I'd feel much safer sharing private information in an environment like this.

Interview 78

I am concerned about my privacy, but I have come to the conclusion that I can't really avoid the dangers that come with the internet and the protection of my data and privacy if I still want to keep up with society, friends, coworkers, etcetera. I am concerned with how much they're figuring out about me and how that affects online biases as they're showing me personalized content, as well as the possibility that someone might be able to track me down though online connections.

There should be a specific breakdown of the data I am giving to all of those companies, and how exactly they would be using them. Personalized ads are fine, but selling my information to other companies would make me deeply uncomfortable, yet it probably is what they are doing anyways. As well, I would like to know if they really do have access to my conversations, camera, camera roll, microphone, etcetera. I think it is the bare minimum to have full disclosure of what those companies do with our data.

I honestly tend to ignore what kind of data protection some of the most common apps use because it would alienate me from the social part it provides in life, like keeping up with people who are far away, or instant messaging someone when you need it. It makes no difference if I protect myself there by stopping my use of certain sites, since it would have a worse outcome in my life. I at least check the kind of photos I give apps the access to with the iOS feature.

I think as of today benefits of using sites outweigh the benefits of not using them, but that might change in the future as we continue to let them in our lives. What they do with our data is not usually as transcendental or noticeable to us, while social media has a more immediate outcome and effect as we perceive it. I think human connection at this time, even if it is online, beats protection of privacy, although we should reconsider it sometime soon.

I try not to think or get very involved in the risks of using social media while sharing some private information, as it will worry me a lot. However I never share exact locations, and I only

post pictures after I have left a place. Personal accomplishments rarely make a post. I don't give sensitive information to sites that are not deemed trustworthy for me. I check site reviews before attempting to sign up or give information to them as easily.

When I go online I always think about my privacy, because I am very careful about the pages I use and the information that I have to give in some them, that is why I concerned about the how my information will be used or if someone is going to steal my identity or sometimes about buying online I worry about if is secure to give the information of my card.

Like not have to worry about that my personal information is being used by this social media or they can see all the things I do, and not to give my number for some of them, as well I don't want to worry about if my photos will be used for other purposes. I don't them to spy on my cellphone information and about the pages and apps I used during the day.

Not share personal information, about where you live, cellphone numbers

Not to post photos that can be used for bad purpose

Always be aware about what apps and pages I used and what type of information they asked

Not share information with unknown people

Don't give information about my family like where they work

Always be sure that the page is worth of trust

The only benefits I find about is because the social media ask for and I think give some information could help other to know a little bit of me, but I think some of the information they ask is not necessary and is only use for the companies to track us around all the apps and social media, but I think in someway is good because they need to have a control about who used their app

I weigh the risks of sharing private information by asking myself if that is really necessary to share it, and I have to know how may information will be used because if I not trust the

social media I decided not to share my information, and other reason because I share it is because they don’t ask to share a lot information but only the necessary like name, birthday, and that kind of stuff

Interview 79

When I go online i am a sometimes a bit concerned with my privacy, but I do not think about it too often. My concerns about my online privacy are that people might doxx my information, people might get my address or see my bank information. I am not particularly worried about companies using my searches to send me advertising though it is a bit disconcerting sometimes.

I would just like for these companies to keep my information safe and not use my information except maybe in the prospect of giving me targeted advertising because those do not disturb me too much. I would like for the accounts I have on these platforms to be as safe as possible. I do not personally share too much personal information online. I would like for them to take responsibility if privacy issues due to their platforms happen to me.

My values would be that I try my best to not share information that would be harmful to me or my family if someone online came to see it and I also do not share too much unnecessary personal business because it just isn't something that I usually do too much. I use an antivirus and I am careful of spam emails and suspicious websites. I am generally not too preoccupied about it.

If I think an information is probably not ideal for other people to know about, think it is unnecessary or reveals too much about myself I will probably not post it, unless it can only be seen by some friends. I do try to filter what I say. If sharing information with websites I will ensure the website is safe and if it is I will probably share information to a reasonable limit/amount.

When I go online I will wonder if the information I am about to share could cause me harm in some way, if I truly wish for people to see it or even know that about me and I will then decide if I still wish to post it. If a website is asking me personal information I will probably ensure that the said website is safe before I proceed to give my information.

I am very concerned about my privacy, especially when talking to people I don't know, for example on platforms like Steam or generally speaking some in-game chats. I try to never reveal what my true identity is, like name, surname and my address. I only use trusted websites to do shopping online and never go to some sketchy, unknown ones to buy anything that needs to be shipped to my address or requires me to reveal my personal info. I also very rarely use my credit card and tend to buy things through PayPal.

On Facebook it is already quite nice because I can choose who can see information about myself, such as school, city I live in and things like that. I would love to entirely hide my profile information entirely (except my name of course) from people who are not related to me in any way and those that I have no mutual friends with. It would be nice to have easier way of blocking ads or sites I don't like and choosing who can DM me.

I value any kind of privacy that a site gives me, but for me the single most important thing is my personal data like name, address and contacts. I also don't like to reveal my nicknames on different sites because I would like to keep what I write on those sites only to the people who I address there. I am also very concerned about all the payment methods such as using my credit cards or PayPal and generally refrain from using it too much.

I choose my personal safety over everything, I don't want people on the internet to know much about me. If I can get some financial benefits I'd first have to know if its safe for me to reveal my information, then decide whether the benefits are worth revealing it. Most of the times I know I'm safe because it’s not my first day on the internet and I know how to protect myself.

First of all I check whether my information can be shared or leaked to any people I wouldn't want to, then I decide if it’s even worth it. It’s never too much precautions for me and I'd like to be 100% sure I won't get harmed in any way. If something seems too good to be true then I'd probably turn that offer down, especially when it comes to financial matters.

Interview 80

When I go online I know that I'm being "watched" in some way, but generally I don't have any concern at all, that said, sometimes I don't like when they the site I'm visiting tells me my exact location and everything, although it doesn't even mean to be something bad, sometimes they just want to see where I'm accessing their site from for research reasons or something. I have a little grasp when it comes to internet data and how sites gather data without you knowing it and then sell them to companies to give you ads on sites.

When it comes to social life and everything, it would be good to only show it to your friends and nobody else, but when it comes to things like the place that I live in or the school that I attend to or in general stuff that could give a hint that where I could be, I wouldn't like it to everyone who can see my social profile can know those things, actually there exists one option to change your privacy settings and with that I think that it works fine for now.

The simple things, like where I live, what I do, where do I study and those kind of things first, then it comes other values like personal documents on my PC or documents that involves personal projects that I'm currently working on and would be very bad to lose them, then I have social media accounts, not only Facebook or Instagram, other social media like Twitch or YouTube and finally the sites where you can buy things online, like Amazon, which at the same time have billing information.

It depends what I share, sometimes I share stuff I don't lose anything by sharing it, but when it comes to personal information, even when I don't do that, I don't think that it could be good to share it with strangers on the internet and in the grand majority of cases, I don't see benefits of doing so, but you could share information with reliable sources, like banks.

They are a lot of risks doing so in a lot of sites or social media. Sometimes you could give more information that you would like to do and it could get in the hands of the wrong people,

but the chances of that happening depends on the site or people that you decide to share your information, you should always share things with people that you trust or sites that you trust.

Interview 81

When I use the internet, I use it mostly for leisure and research. The concern with my privacy is not much, maybe because I have nothing to hide anyway, but I always take care to not happen something bad. What worries me most is someone being able to have access to my camera and see what I am doing the rest I am afraid of the most normal things, such as stealing confidential information and information about my credit card, but I believe that if I am are careful, the chances of this happening are minimal.

When I'm visiting any social media site, first of all I never put my original information, about my age and where I live I always use fake information on those parameters, second if someone sends me a message asking where I live I don't say It I only say it if that person is my friend, and third I never post anything, mostly because I don't like to post pictures of me and second because I don't want other people to see what I'm doing or have done.

My individual values pertaining to protecting my privacy online, well I don't answer messages from people that I don't know, I never open links that I get from unknow people, I always try to hide my personal information, I don't post pictures all the time of what I'm doing, when someone asks for my credit card information I never give it as well as information about my family and friends and last but not least I always try to make my profile pages private.

Well its very rare for me to share my personal information online, but when I do it I weight the benefits of it by seeing if that share of information will bring me gains in the future for example giving information to a company that is trying to hire me. At the moment must of the private information that I shared online was with my friends so I guess I don't have a problem most of that information where accounts that my friends needed.

Well its very rare for me to share my personal information online, but when I do it I weight the benefits of it by seeing if that share of information will bring me gains in the future for example giving information to a company that is trying to hire me. At the moment must of the

private information that I shared online was with my friends so I guess I don’t have a problem most of that information where accounts that my friends needed.

Interview 82

In part I am, yes. I strongly believe that privacy is a right that should be strictly respected and protected, not only on the internet, but in everyday life too. Specifically online, I am afraid that my data is being sold to powerful corporations all over the world, without me knowing what are they doing with this information. Also, hackers could get into my private stuff, for example. However, I feel that there's not much more of my online information that is not already in hands of other persons/institutions.

I would really like to be asked, firstly, if any information of mine is being shared with other entities. I would like to have total control of what is being kept private, and what not. Social media should keep total privacy of conversations, without even the site knowing what is being chatted in those conversations. If I decide to share some information, I need to know what information of mine is being given to other entities, and what are those entities, and what are the purposes of getting that information.

Privacy should be total. No entity, whether it is private or governmental, should have access to private information without consent. We can not accept to live in a police state that controls and knows everything about us. If something like that was a thing, we could not live free to say what we want, denying our most basic freedoms. In an ideal world, I am going to share exactly what I want to share, nothing more, and nothing less.

I mostly think about what would the benefits of sharing that information would be, compared to what the negative outcome of it would be. I could know that I am sharing somewhat important information on the internet, but if it helps substantially to others, persons or institutions, or if it gives me a reasonable financial compensation, I could decide thus to give that private information.

The risks of sharing private information online can be thought about, in my opinion, in two big groups. The first group is somewhat inoffensive: I think of, for example, the information

that is collected to target ads to me. This is, however, not completely inoffensive, as entities are still gathering massive amounts of information that is being sold by all kinds of sites, and that could help to build a fake-internet-persona of myself. The other kind is more personal information that compromises more myself, like private events of my life, private media (photos), etc. This kind is the type I hesitate most to give online, because of the risks that it could give to me.

Yes, when I go online I am concerned about my privacy, because I could never know where is going to end up my personal information and there is always people that uses it for their convenience and its not always in good hands, I am concerned about being under vigilance, or being robbed from my bank account when I buy things on Internet or something like that.

I never share my personal information like my location, phone number, actual pictures or information about my loved ones on those sites to protect my privacy, it would be great for everyone that those sites stopped asking for that kind of information about us because it makes us vulnerable of being extorted and that kind of things that are actually very common.

To protect your online privacy, ignore the, About Me, fields in your social media profiles. You don’t have to let people know what year or where you were born ‚Äî which could make you an easier target for identity theft. Explore different privacy settings, too. You might want to limit the people who can view your posts to those you’ve personally invited.

Create strong passwords, too, for your social media profiles to help prevent others from logging into them in your name. This means using a combination of at least 12 numbers, special characters, and upper- and lower-case letters. And never use personal, easy-to-guess information, such as your birthdate or pet’s name, as your password.

To start, make sure to use a passcode to lock your phone. It might seem like a hassle to enter a code every time you want to access your phone’s home screen. But this passcode could offer an extra layer of protection if your phone is lost or stolen. Make sure your passcode is

complex. Don’t use your birthdate, your house number, or any other code that thieves might be able to guess.

One of the ways in which hackers compromise your online privacy is through phishing attempts. In phishing, scammers try to trick you into providing valuable financial or personal information. They’ll often do this by sending fake emails that appear to be from banks, credit card providers, or other financial institutions. Often, these emails will say that you must click on a link and verify your financial information to keep your account from being frozen or closed.

Interview 83

Yes, I'm concerned about it. I refrain from posting too many pictures online, especially the ones showing my face. I also want to leave as less information on me on websites as possible. I'm worried that any person can get to know too much information about me just from social media, I do not like to comment on anything neither not to make an impact. I also do not like giving away my phone number or sharing my location with aby website or apps, I feel that I'm tracked.

I have a feeling that just going on Facebook means no privacy, as it is mainly used to share things for them being publicly seen. I would only like to ensure my chats are safe as well as any files I share with my friends in private. Also I really dislike the fact that Facebook and for example Instagram are owned by the same company and it seems it is impossible to have separate accounts, because they use their data to see it's the same person.

In the first place, being rational with uploading stuff online. Not sharing very private things with people, not giving it away to any other website. Not sharing your location neither. Simply restraining yourself from using social media, keeping track of cookies used on websites you visit. Having an anti-virus that helps checking suspicious websites. Not having your passwords saved on your browser.

I do not think there's many benefits of sharing your private information online, I'm really against it. I feel bad thinking of my data (pictures, artwork, texts) being used without me knowing it. I can think maybe of trying to find a job through a website online - that could be quite beneficial. Or to sell some things online (either artwork or just a few things at home you don't use anymore). Other than that, I'm okay with buying things online on websites like Amazon, which also requires personal data, but that's already a need in daily life I think.

They can be used without my knowledge in a wrong way, if it's artwork - it can be stolen and uploaded somewhere else. Cyber thieves can use your data to mislead you, like with using

your number to send you misleading messages to pay something, things like that. Also sharing your location online can be dangerous, as you never know who is on the other side of the screen getting to know all of this.

Interview 84

Yes, sometimes when it comes to things I want or do not want to share with others. I usually use Instagram as my main social media source where I mostly share posts to the public. When there comes a time when I decide to share something on there, I get very indecisive because I do not like sharing too much of myself or my life. So I would try to narrow down the amount of pictures I would like to post. Also my account is private which means that if people want to see my posts they would have to request a follow from me which I like very much because I do not like random people following. I get very uncomfortable when my pictures do get in the public eye because those are my personal posts. If my account if public, I would not know who are looking through my page and people could possibly know where I live.

I would immediately private my account so I can take control on who and who cannot see my page. I would try to also avoid giving out my location and where I am from. And on Snapchat, I would be on Ghost mode so no one can see where I am currently at. When I am about to post on any story, I would try to avoid putting on a filter that contains my location, instead I would put emojis. I would definitely not put any important information on my bio or status such as where I go to school and where I am from. For me, I would post less.

My values are to not share important and very personal information to others on social media. Like my location, my school address, and work address. For me, I choose not to show my face a lot, instead I would mainly show my outfits in which my face is not included in pictures. I prefer my friends to ask me if they can post pictures with me in them. I try not to post pictures of me in an obvious where people can tell where I am specifically. For example,

in the picture there could be a street sign and a local restaurant next to it. Therefore, I try to avoid posting pictures with obvious settings.

The things that are okay to share are my age and nationality. I believe those are harmless information that you can share with anyone because no one can do anything with that information. Basically when I decide I want to share something I usually weigh out the pros and cons, if there are physical signs involved, I would try to remove it or not post it at all, if it's just the inside of my room, it is permissible to me. As long as there are no serious information shared that anyone can use, then that is a green light for me to post and share.

If it includes my home address or even the town I live in, that is what I consider to be a risk when sharing my private information online because people can use that information and probably come to my home randomly without me knowing. And I even get anxious when sharing my face because if my page was not private, anyone can save my pictures for anything, it can be to use my face to access anything or to pretend to be me.

Interview 85

My privacy concerns are mostly about sensitive data, the likes of home address, my college, my name, my phone number, my family members names, etc. I don't want to be a target of harassment or exposing a family member or friend, I like my anonymity, and I think that people on the Internet can be harsh, hateful or harmful, because they don't see the potential harm of their actions or they just don't care. I try to avoid being doxxed.

Ideally, I like to make my accounts as unrelated as possible, I sure do use the same email to create all my accounts, but I avoid using the same username and I always enter into the privacy options to configure them to my liking. I also put just one name or I write fake ones, or pseudonyms. All my accounts seem unrelated, and obviously I never link them if that's possible.

My personal view is that everyone has the right to maintain their anonymity and privacy while using the Internet, being an irrevocable right that should not be limited by governments, however I believe that this right comes with a responsibility, especially about the anonymity. This idea that anonymity should be treated responsibly is due to the fact that anonymously people on the Internet participate in acts that can sometimes be highly questionable

I'm feel that the cost of using social media today, whether it's Reddit, Twitter, Tiktok, YouTube, etc., is to sacrifice, whether we like it or not, part of our privacy, but it's a cost I'm willing to pay, However, this does not mean that I am unable to control my digital fingerprint and privacy to some extent, whether with respect to my sensitive data or my personal interest profile for advertisers.

Returning to my initial response, my main personal concern about the risks of the Internet in terms of privacy is the possibility of being exposed to harassment, violence (whether physical or psychological) by myself or my family and friends. It's something that worries me a lot and I want my privacy decisions to limit this risk as much as possible.

Interview 86

My biggest concern with online privacy is people and entities breaking the law when they partake in data sharing. Today, countless privacy policies are put in place by companies to protect people's data. They specify how people's personal information may and may not be shared when they sign-up for a company's services on the internet.

When visiting any social media site I would manage my privacy by following some steps: Using a strong password, Using a different password for each of my social media accounts. Being selective with friend requests, Being careful about what I share and not revealing any sensitive personal information (home address, financial information, phone number etc.).

I think that online privacy is important for numerous reasons and I personally try to protect it as much as possible because you never know for certain. For example you don't want to share details of your personal life with strangers and it's hard to be sure what personal information is gathered and by whom: information collected by one company might be shared with another. This why I believe that protecting my privacy is something very important.

I personally do not believe that there sharing your private and personal information online for everyone to see, is going to do any good for you... So I think that there are no real benefits in sharing your private information online.

I believe that everyone needs to be careful with how much personal information they reveal online. For example sharing your address, phone number, birthday and other personal information on social media can mean you are at a greater risk of identity theft, stalking and harassment. Those are just some of the risks of sharing your private information online.

Interview 87

When I go online I am concerned about my privacy because the internet is a dangerous place. I am concerned about my personal information becoming available to people that intend to do bad things whit her. I always think about blackmail when I go online, because nowadays, although the security is increasing, so is the danger.

I get worried about someone getting access to my personal accounts like Instagram, and I often change the password. When visiting social media sites like Facebook, Instagram or Twitter, my ideal situation to manage my privacy would be getting to manage the things I would like to share with the app. I also like to keep all the accounts with the security codes when accessing through another laptop or phone. In order to manage my privacy it would also be interesting if I could see all the data that is really important to the sites and what for they are used.

I ensure my computer privacy with virus protection software, and I also try to use strong and unique passphrases or two-factor authentication. I am aware of scams like phishing scams and email scams, which attempt to collect personal information. I am cautious about requests of personal information online. I am careful about who I hand my private payment details over to.

The potential benefits of sharing personal information include saving money, gaining access to useful services or information, and facilitating commercial and social encounters. It can also provide better experiences because organizations use data to understand us better. This helps them provide great customer service and build trust in the way our data is used. This can involve making sure their brand resonates with me, or designing websites that are easier and simpler to navigate.

I think about people who revealed they were traveling and their house and were robbed. Investigation showed the culprit was a Facebook. Social media is a time drain. Hours pass and

people don’t know where the time went. We spend to much time on social media. We spend money on social media. And if I bought a shirt I will keep getting shirt ads.

Interview 88

When I go online, I always think about safety, because I know there are a few risks about exposing our private life on social media. Some of them can use it or sell it, so I try to give few details about my life in order to be safe. Besides, if we are care enough we can navigate safely. To make this possible we should watch out for scammers that can and will use your private life for their benefits.

Regarding social media, in my case I only give my name, e-mail and sometime my phone number, but I don’t put my credit card details for example. I don't know if I'm being paranoid, but at least I feel safer.

In other words, I only put some ways to identify myself, but try to protect myself at the same time not giving any monetary information, even though these are secure social medias, you will never know.

As I said before, not giving crucial information about you, like exposing every detail of your citizen card and your credit card is very important to protect you from online scammers. You can use VPN to hide your IP address and be safer. Besides that, just try to not give all information and research about specific websites and see if they are safe in order to give this information if asked to.

I think that if it benefits me in some way, I must be cautious and do a quick search to see if benefits me. If it is an online shopping and I need to use my credit card, then I need to be sura that the website is safe and I'm not going to be scammed. If it is a social media, because I don’t buy anything there, I won't put my credit card information, only the minimum they asked for.

I try to give the minimum information I can give. If it is a online shopping website and I need to put my credit card information, I will research about the website and if I end up seeing as safe, I will give my information, but if it is a social media, where I don’t do any shopping, I

won't put any details about my credit card just for safety measures. So I only try to give the bare minimum in order to keep me safe.