Privacy and Data Protection: A Study on Awareness and Attitudes of Millennial
Consumers on the Internet - An Irish Perspective.

Saloni Lerisa Pinto

Master of Science in Management

National College of Ireland

Submitted to the National College of Ireland, August 2018

ABSTRACT

This study aims to understand the awareness Irish millennials have with regard to their data privacy online and data protection laws. It also looks at deciphering millennial attitudes towards their data- are they concerned about their data privacy, do they indulge in risky behaviours online and are they willing to trade data for benefits on the internet. The study fulfilled the objectives by the way of a inductive, mono method qualitative design using semi structured interviews. The findings were analysed using thematic analysis.

The primary findings were that millennials had a surface level awareness of data privacy and data protection. They seem to have a nonchalant attitude towards data privacy yet displayed concern over their data online. They also indulged in risky behaviours despite their concerns. Millennials seemed to be willing to trade data for benefits, but showed resignation about certain exchanges, especially where money was concerned.

Key words –Privacy, Data protection, Millennial attitudes, Data Protection Awareness

DECLARATION

I hereby certify that this material, which I submitted for assessment of the programme of study leading to the award of Master of Science in Management, titled "Privacy and Data protection: A study on Awareness and Attitudes of Millennial consumers on the Internet: An Irish Perspective" is entirely my work and has not been taken from the work of others.

Signed: ....

Date: 29th August 2018

Student Number :16135351

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to, first of all, Karen Murray, for the assistance, support and guidance during the development of this research. Secondly, Shannon and my parents, for all the love, understanding and help. And finally, for all the participants, thank you for your patience!

Contents

List of tables

List of Figures

List of Appendices

INTRODUCTION

The internet has revolutionized the world of communication with its world-wide broadcasting capacity (Leiner et al.,2003). Today, the Internet is the most preferred medium of communication. People shop, exchange photos and message, learn, work and even receive medical consultations on the internet (Kaplan and Haenlein, 2010; Pitkänen & Tuunainen, 2012). A report by the international Telecommunication Union (ITU), a United Nations body, states that out of the current world population of 7 billion people, almost 3.2 billion people use the Internet (Itu.int, 2018). In Ireland, almost 80% of people access the internet, with 91% of Internet users between the age group of 25-35 using internet on a daily basis (Central Statistics Office, 2017).

Unsurprisingly, most traditional brick and mortar businesses, who previously considered online presence optional are now adapting their value propositions to include significant online businesses (Sampler, 1998). Technological advancements have birthed organizations such as Facebook, snapchat and Spotify who are known as "pure play digital companies" and provide services only through the internet (Bharadwaj et al., 2013). These businesses collect and store consumer data, in digital format, in the course of business operation (McAfee and Brynjolfsson 2012). This Data consist primarily of personal information such as what type of products people buy, what are their likes and dislikes and behavioural patterns has business value, as it can be utilized to tweak the company's business processes, product offerings and business strategy (Mitchell, 2016). Almost 90% of this digital data was created in the last decade and is set to grow by 40% by the end of 2020 as the number of internet users rises (Eggers, Hamill and Ali, 2013).

While this data is driving efficiency and innovation on one hand, it is raising privacy concerns on the other(Tene,2010). As data grows, the job of protecting privacy and security online becomes more complex. Consumers, in order to avail of full benefits of online transactions, such as the ease and speed of processing an online order, trade off by allowing companies access and use of private data (Feldman, 2000) .The companies who hold this data, build vast data bases of consumer behaviour, mine this data to extract and create behaviour profiles (Rygielski, Wang and Yen, 2002). Most companies usually de-identify this data during analysis but over the last few years, findings have emerged that this encrypted data can be re-identified and therefore is a cause for concern (Ohm, 2010) .The issue of online privacy is aggravated

due to the structure of the internet with the absence of "Physical Indicators" of violation of privacy that are observable and apparent to human senses and as newer technologies emerge, weaving themselves deeper into people's lives, there is an erosion of the concept of "personal space (Bellotti, 1997).

These issues are raising regulatory concerns and governments around the world are taking action to protect their citizen. The European Union, in the light of this growing unease has enacted the GDPR (Regulation (EU) 2016/679) in order to protect European consumers on the internet and Ireland has a legal framework with regard to Data Protection in place (Dataprotection.ie, 2018a).

However, despite these measures to prevent the misuse of personal data, there are still questions arising if consumers are well and fully aware of how companies collecting and using their personal data (Barnes, 2006). A large portion of these consumers are millennials and as studies indicate millennials have different outlooks towards online privacy that vary from other generations (Pew Research Center, 2010). Academics state that millennial consumers permit the collection and storage of their personal data, if it translates to a certain degree of convenience and benefit for them (McDonald & Thompson, 2015). However, others argue that millennials are not willing participants in data transactions but hold cynical or resigned views towards the same (Giulia et al., 2018). Research claims that millennials have unique attitudes toward personal data such as lack of interest in data protection yet demonstrate concern over their data (National Cyber Security Alliance 2013). Some state that millennials generally tend to engage in risky behaviours that would compromise their control on personal data despite being the most technologically aware generation yet (Rainie et al. 2013). Most agree that millennials have only superficial level awareness of data protection laws but are aware of data collection and are willing participants to it or unconcerned about it (Timm & Duven, 2008). Since millennials are one of the largest segments on the internet, this study is undertaken to gain insights on their awareness and attitudes towards privacy and data protection.

This research examined the attitudes and awareness levels of Irish millennial consumers on the internet. The aims of this research were to understand how aware these millennials are of their being collected and used. It also looked at their behaviours and attitudes towards their data. The thesis is divided into 6 chapters. The literature review examined concepts like data privacy, data protection, attitudes and awareness levels of millennial consumers on the internet. The

next chapter, research aims and objectives - explained in detail, the need for this study and what it intended to find. The research methodology that followed this chapter identified and justified the methods used. Semi-structured interviews were used to collect data about the topic Following this a thematic analysis was undertaken to reach findings.

A few significant findings emerged - most millennials had surface level awareness of data privacy and awareness, were concerned about their data on the internet but didn't attempt to understand how to protect it and still indulged in risky behaviours online. It was also found that most millennials were willing to trade data for benefits but upon close observation, it was with a certain level of resignation when exchanging financial data. The study concluded with a discussion on the finding and recommendations for further research.

CHAPTER 1
LITERATURE REVIEW

This chapter discusses and critically assess the literature behind different concepts such as privacy, data protection, millennials consumers and the internet, their attitudes and awareness levels towards their personal data. The literature review with regard to Privacy and data protection will begin with an exploration of the origin of concepts of "Privacy" and "data protection" and trace the evolution of these concepts with the emergence of the internet. It will then outline the legal framework on privacy and data protection currently in place in Ireland for consumers on the internet. The literature Review on millennials as customers, will focus on defining and identifying millennials and consumers and explain why the study focuses on millennial consumers attitudes and awareness. Considering a millennial consumer's attitude and awareness level of data protection and privacy will give a good insight into the mindset of a millennial consumer and help in creating awareness programmes that target the millennial consumer.

1.1 Background of privacy and data protection

1.1.2 Privacy

The concept of privacy has had an important role in sociological, political, economic, religious studies from antiquity to the modern world. The concept of privacy can be found in Aristotle's books on politics, John Locke's works in the 1600's on public and private property , where the authors create distinctions between public and private spaces and denote the latter as an aspect of p privacy (DeCew, 2016). As civilization advanced, social and political changes to the society brought about the recognitions new rights, one of which was the "right to be left alone" (Cooley, 1879). Samuel D. Warren and Louis D. Brandeis stated that every individual was entitled to privacy of body and mind and this right came with enforceability, a right today known as the right to privacy(Warren & Brandeis, 1890).

Westin, considered to be the pioneer of the modern concept of privacy defined it as the claim of an individual or a group or organization to determine, when, how and to what extent can information about them be communicated to others (Westin, 1967). Altman's theories on this concept stated that privacy could be understood as a "Selective control of access of one's information" and propounded that privacy was not an absolute term in itself and could be

divided into desired and actual levels of privacy (Altman, 1975). These control centric definitions were unified and elaborated by Margulis (2003) who submitted that privacy signified a control of transaction between people, with the focus of the transaction being an increase in autonomy while reducing vulnerability (Margulis ,1977). Several academics in various field have attempted to provide subject relevant definitions of privacy that range from the subject of moral ethic to medical privacy, yet there is no agreed upon, universal definition of privacy in academic research (Dinev, Xu, Smith & Hart, 201; Goodwin, 1991; Nowak & Phelps, 1995) leading to the conclusion that the concept of privacy is multi-dimensional (Burgoon et al, 1989) and that the term privacy can be understood to be an umbrella term that covers a wide range of interest and can be broadly be divided into constitutional or decisional privacy which relates to a person's liberty to make his own choices on matters intimate or personal such as marriage or contraception and information privacy- which refers to a person being able to control the access to his personal data (DeCew,1997).In the course of this research, information privacy is being referred .

However, the traditional definitions and understanding of the privacy, formulated before the advent of the internet aren't equipped to handle challenges brought in by technology (Austin, 2003). the introduction and accessibility of internet has furthered the scope of Information privacy or data privacy to include the digital environment and today, Information privacy deals with the interest of individuals in holding control over what information about them could be circulated on digital platforms (H. Jeff Smith, 2011).

1.1.3 Privacy and Control in the modern world

While Westin (1967) and Atman's (1977) theories developed the concept that privacy was control, some theorists claim that privacy can be termed as the ability to exert control (Culnan 1993). An Individual who is a consumer on a digital platform today, can say his privacy has been violated when he loses control of his personal data on that platform (O'Brien & Torres, 2012). However, while privacy theorists have established that control is integral to privacy and despite growing concerns about vulnerability online, a large number of internet users, especially users of social media platforms seem to be still sharing their personal information online, without expressing worry about the risks associated with the same and don't appear to concerned about the loss of control of their personal data (Rosenblum, 2007)

1.1.4 Data protection

Data protection is described as the legal control exerted against improper access and usage of an individual's personal information by a third party. This term was coined in Europe to initially refer to privacy protective legislation (Swire and Ahmad, 2012) . Data protection laws can be dated back to the 1970's when processing of individual data became widespread amongst business organizations and laws regulating this seemed necessary (Cate, 1995). The Data protection commission in Ireland outlines data protection in layman terms as process where an company or person handling a individuals personal data has a duty to keep such data private and safe (Dataprotection.ie, 2018).

1.1.5 Laws regarding privacy and data protection in Ireland

Privacy is a fundamental human right as outlined in several human right instruments including the Constitution of Ireland (1937) and Charter of Fundamental Rights (European Commission,2009) and European Convention on Human Rights (Council of Europe,1950).In Ireland, while the constitution doesn't explicitly carve out a right to privacy, the judiciary first recognized the "Right to Privacy" in the case of *McGee v Attorney General* [1974] IR 284 , where Article 41 of the Constitution was interpreted to guarantee a married couple a right against invasion of privacy by the state. This right was established as unenumerated personal right under Article 40.3 of Constitution (1937) in the case of *Kennedy vs Ireland* [1987] IR 587, where it was stated that "The right to privacy must be formulated in a manner such that it ensures an individual's dignity and freedom in a democratic and independent society".

On a European level, the human right to privacy is protected under Article 8 of the European Convention on Human Rights (Council of Europe, 1950) which provides or a right to respect for one's 'private and family life, his home and his correspondence' subject to certain restrictions. Ireland was one of the first countries to sign this convention and later incorporated it into Irish law by the passing of The European Convention on Human Rights Act 2003. The Data Protection Acts, 1988 and 2003 which transposed from Data Protection Directive 95/46 comprised the legal framework on data protection. The General Data Protection Regulation (GDPR) 2016/679//EU which came into effect May 2018, repealed and replaced these. It is complimented by the Data Protection Act, 2018.

1.1.6 Consumers, privacy and data protection

Consumers are traditionally known as buyers or goods or services. In today's technology driven world, consumers can also be end-users of an application or service on the internet. (Giese and Cote, 2002). Most studies on consumers refer to consumers as the final user of a product or a service (Spreng, MacKenzie and Olshavsky 1996; Mittal, Kumar, and Tsiros, 1999; Smith, Bolton, and Wagner,1999).

As most companies and consumers move online, the issue of privacy has begun to crop up. Consumer privacy can be defined as the consumer's capacity to exercise control over a) Presence of other participants within the environment at the time of such a market transaction or B) Transfer of information that was dispensed at the time of such transaction to a non-participant to the transaction (Goodwin, 1991). This definition has been upheld by privacy academics and researchers (Foxman & Kilcoyne, 1993) while this definition was made before e-commerce became common place, it still finds relevance in the e-commerce environs of today (Milne and Rohm, 2000). Before the age of the internet, consumer privacy issues revolved around companies extracting information from people them to target catalogues and promotional messages at them (Equifax, 1996).

With the introduction of the internet and the electronic marketplace, there was dramatic shift in the way retail and other business operated as most people began to use the internet to access, view and shop for products all over the world. The rise of the "Age of information" has caused about of this data privacy as the dynamic nature of web based technologies has made information privacy of individuals who access these technologies one of the most debated ethical issues today (Davies, 1997) .

Currently, there is a wide legal framework in place in Ireland on privacy and data protection. The ones that specifically apply to consumers on the internet are the GDPR (Regulation (EU) 2016/679) and the ePrivacy Regulations, 2011 (S.I. 336 of 2011). As The GDPR allows member states to give further effect to certain provisions, Ireland has enacted the Data Protection Act 2018 in pursuance of this.

The GDRP (The General Data Protection Regulation)

This Regulation applies to EU citizens and their personal data, irrespective of where such information is collected or stored. It stipulates that consent to processing data must be explicit and must be obtained by providing complete information about why it is being obtained. It defines EU citizens as "data subjects" and "processing" as an operation which includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations. Article 4 of the GDPR (Regulation (EU) 2016/679) defines personal data as "any information relating to a living natural person (known as a data subject for the purposes of GDPR)" who is "identifiable" or can be "identified, directly or indirectly by certain "Identifiers" , a list of which is provided in Article 4(1) of the GDPR as follows:

- Name
- identification number,
- location data,
- an online identifier
- physical, physiological, genetic, mental, economic, cultural or social identity of that Data subject.

The GDPR also states in Recital 30 that online identifiers can be created by tech devices, apps, IP addresses, cookie identifiers since they leave evidence that can be combined other server information to identify data subjects (Vollmer, 2018).A data processor under this regulation can refer to an individual or an organization which "processes personal data" on behalf of "Data controller". Data controllers means a natural or legal person that determines the objective or methods of processing personal information.

To ensure that the data subjects have complete control over their personal data when such data is being held on a computer, manual filing system or via photographic or videography recording the data subjects have been given 8 fundamental right which are as follows;

 The Right to access information(Article 15 of GDPR) , *Right to rectification*(Articles 16 & 19 of the GDPR), *Right to erasure* , also known as the right to be forgotten (Articles 17 & 19 of the GDPR) , *Right to data portability* (Article 20 of the GDPR), *The right to object to processing of personal data* (Article 21 of the GDPR) *The right to restrict the processing of personal data* (Article 18 of the GDPR) and *Right to be informed* (Article 13 & 14 of the

GDPR). The data subjects also have *rights regarding automated decision making and profiling* (Article 22 of the GDPR). Data subjects may object specifically to any processing of data for direct marketing purposes and have right to have their information used in compliance with the GDPR. These rights are enforceable and in the event of a violation, data subjects can file a complaint to the Data Protection Commission under Article 77 of the GDPR and can also authorise certain third parties to file such complaints on behalf of them under Article 80. (Regulation 2016/679/EU) .

The Commission may take several actions in the event of a complaint such as conduct inquiry, issue enforcement notice to the violating party and impose fines for certain violations of the provisions of GDPR. These fines can go up to 10,000,000- 20,000,000 euro or 2%- 4% annual turnover worldwide of the previous fiscal year. Alongside this, data subjects are permitted to sue data controllers via tort law for compensation and may even file criminal cases in certain special events.

ePrivacy Regulations (S.I. 336 of 2011)

This regulation governs personal data protection in relation to unsolicited communication made via telephones, emails, SMS. After GDPR came into effect, these types of communications are governed by both the GDPR and certain specific rules set forth within the ePrivacy regulations (Dataprotection.ie. 2018b).

1.2 Millennial Consumers and Privacy attitudes:

1.2.1   Defining millennials

Defining and exploring generations can be based on two perspectives: sociological or cohort perspective. this study will consider the former perspective. Sociologically speaking, a generation is often considered to consist of a class of people who share a similar time range of birth and similar socio cultural experiences (Aboim & Vasconcelos, 2013) . Each generation has been found to have unique experiences, a differing history, lifestyle patterns and value system which impact their behavioural patterns and decision making especially with regard to buying (Williams & Page , 2011) research shows people who were teenagers during the 1980 were more likely to purchase the period relevant pop culture centric merchandise in the 2010 . The focus on this research is on the millennials or generation Y as this generation is often considered to be first native speakers of the digital language and is a generation that was raised in a world of technology (Lyons & Schweitzer, 2012) .

However, there are contrasting viewpoints on the timeframe of where this generation begins and ends. Some state the accurate range of time for gen Y is 1981-1995 while Black describes Gen Y the generation being born between 1980-2000. Some academics believe that time frame to be considered millennials should be longer, ranging from1977- 1997 (Meister & Willyerd, 2010) or from 1982-2005 (Howe & Strauss, 2007) while others argue that millennials should only include people born close to the millennia and that anyone born after it would fall into a different generational categorization (Kaifi et al., 2012). While there appears to be no consensus amongst academics on an absolute time range to define millennials, most subscribe to the time frame of 1984-2000 in their research (Black, 2010 ; Smith and Nicholas, 2015) and this time frame is used in this research as it subscribed to by most authors in defining millennials.

Millennials are considered "digital natives" according to Prensky (2005) and are quick in grasping new technological tools and processes, with an intuitive knowledge and ability to understand digital knowledge often appear to use these tools as an extension of their mind and are so accustomed to the digital environment, that they cannot image a world without it (Frand 2006) . Most research indicates that this generation's brain has been rewired by the exposure to digital technology, creating changes in the way this generation perceives things that might impact they see the value of their data (Woods 2006).

1.2.2   Millennials in Ireland

 Internet use in Ireland at its peak with 8 out of 10 adults accessing the internet on a regular basis. Almost 98% of Millennials in Ireland used the web in 2917 and 92 % accesses the web everyday (Central Statistics Office, 2017). Most of these used the web for shopping or sharing data. The numbers indicate that there is a huge segment of millennials on the internet. As the government is creating awareness about data privacy and protection, it is important to know where millennials stand on this topic in Ireland.

1.3. Consumer attitudes in general

An attitude can be defined as a mental state of being, caused by experience, imparting an directive influence on a person's response to any situations or objects (Allport ,1935). It is lasting set of beliefs, emotions and behavioural patterns in connection to socially relevant

objects, groups, events or symbol (Hogg, & Vaughan 2005). Attitudes are usually expressed by evaluating an entity with a level of favour or disfavour (Eagly, & Chaiken, 1993) An attitude contains 3 factors a) a feeling, B) Cognition C) Behaviour. A knowledge of Attitudes helps in forecasting the person's reaction and behaviour towards a situation. (Debasish and Muralidhar, 2013). In the world of business, an organization can benefit greatly by being aware of the attitudes of their consumers and shaping decisions in line with positive attitudes of consumers. As attitudes are useful to predict behavioural patterns (Daniel Katz,1960) they are used in formulating business strategies. Attitudes can be shaped by family, lifestyle, media age and gender amongst others (Solomon et al. 2013). As data indicates that since consumers attitudes often differ by generation, most business tactics developed for middle age and older consumers don't have the same effect on millennial consumers (Gehan and Yamamoto, 2017)

As millennial consumers have significant spending powers, they are an attractive segment. Most millennials use the internet to accesses goods and services and companies are clamouring to have an online presence to capture this segment. In the light of these issues, it is important to know what attitudes these millennial consumers hold, with regard to the internet from a business perspective. Alongside this, awareness of millennial attitudes is beneficial for governments and authority bodies to formulate more effective awareness programme and educational policies in this regard.

1.4 Attitudes of Millennial consumers on Privacy and Data protection

1.4.1 Privacy Concern amongst millennial consumers:

Concern is defined as worry about a situation (Collins Dictionary 2012). The Concern for privacy has been a fundamental part of the debate on the concept and theories of privacy since 20th century when inventions like cameras and moving pictures caused worry amongst law makers and academics that a person's actions could be permanently captured and stored in a accessible and distributable format (Warren and Brandeis, et al). Privacy concerns amongst consumers before the internet revolved around being subject to unwanted marketing via mails or phone calls. Today, most consumer privacy concerns are centred around how personal data is handled by third parties on the internet.

Privacy of personal information was ranked 3rd in the list of key issues in Ireland with 84% looking it as a very important issue in the Public Awareness Survey 2008 carried out on behalf of the Irish Data Protection Commissioner (Lansdowne Market Research, 2008). Research

shows that millennials are concerned about their personal information online (Youn, 2009) A study led by Olivero and Lunt (2004) on consumer privacy concerns in the e-commerce environment reported that as the awareness levels of consumers on the internet on how their data was being processed increased, so did the demand for better control over personal data . Privacy concern was also linked to the nature of the transaction, the type of data being extracted and its use((Malhotra, Kim and Agarwal, 2004) with studies indicating that most consumers including millennials are more concerned about financial data such as credit card information, income, personal credit score over relationship and demographic data such as age, location, address and marital status (Cranor, et al., 1990 ;Phelps, et al., 2000). Some research states that millennials seek control over their data online based on privacy concerns (DMC, 2018). Millennials are found to be concerned about their privacy online and privacy rights (Salazar and Woodward, 2017). Surveys show that while less than 40% of millennials participated in safety procedures such as installing security software on a regular basis, they still agreed that they had concerns about their data and stated there was need to create more awareness on data privacy (National Cyber Security Alliance 2013).

Conversely, Fleming and Adkins (2016) argue that data privacy and security aren't big concerns for millennials. A study conducted by University of Southern California's Centre for the Digital Future in 2013 found that millennial's concern about privacy was low (Reed, 2013). A similar survey in 2015 found only 20 %millennials worried about online privacy (American Press Institute, 2015). Findings from both the studies indicated that as digital natives, millennials seemed to have acclimatised to the digital environment and suspicion or concern was not default outlook about the internet, unlike the other generations. Millennials seem to have a laid-back attitude to privacy on the internet with almost 46% of the participants in a study on data privacy on the internet stating that they weren't too bothered about how their data was protected online (MIP, 2015). This study also cited the reason for this attitude to be the extent of digital integration in their lives. Research indicates that the number of consumers who are not interested to know about how their data is collected or used is on the rise and almost 30 % of these consumers are millennials (Ridley-Siegert, 2015) . Due to the contrasting nature of literature on privacy concerns amongst millennials consumers and the lack of information on an Irish perspective, this study has been undertaken to shed light on the issue.

1.4.2 Attitude to risk:

One of the drawbacks of the internet, is exposure to risks online. Risk, in this context can be defined a high probability of loss of control over personal data on the internet and risky behaviour is any kind of behaviour on the internet that leads to unintentional or intentional loss of control over personal data (Zimmer et al, 2010). A Consumer's perception of risk is understood to feelings or emotions toward any probable negative outcomes of transactions on the internet (Hsu and Chiu, 2004). Studies show that many consumers online are risk aversive, especially with regard to online payment methods, frauds online, theft or misuse of personal information by third parties (Miyzaki and Fernandez, 2000 ; Fischer and Arnold, 2006).

However, people, especially younger generations aren't demonstrating sufficient reactions to this "risk" factor (Levin & Abril, 2009) Most millennials have confessed to risky behaviours online such as emailing sensitive documents from personal accounts, save on easily accessible locations and lose company devices that haven't been encrypted (Carmichael, 2014). A study on millennial consumers shows that almost 30% of millennials share personal data such a phone numbers and social media profiles with third parties (Mintel,2015) and study indicates that 44% millennials think that companies who they transact with keep their information private all or most of time(Flemming and Adkin, 2016) Millennials are found less likely to be aware of "opt out options" in tracking via websites and most don't express any interest in enabling privacy options on websites (Levine, 2011; Tablante, 2013).

Research indicates that while millennials have appropriative values regarding privacy, they simply aren't fully tuned toward risks involved (Hazari and Brown, 2013). Despite being the most tech savvy generation, millennials are posing security threats due to their unsafe online practices (Palfrey and Gasser 2008). Millennials, while more aware of hacker threats, were more likely to indulge in activities that would enable these hackers (Rainie et al. 2013) . Most millennials don't read privacy disclosures and consent forms (Kelley et al. 2009).

It is believed that these risky attitudes of millennials towards their data privacy online stems from being "digital natives". Since millennials have never known a world without technology, they have lower expectations about data privacy, knowing that all their data is online, even if isn't vulnerable (Moqbel et al., 2017) Another school of thought argues the contrary, that since millennials are digital natives, they must have higher expectations regarding data privacy on

the internet, as the generation as a collective has a better understanding and adaptability to technology (Lulsoli and Miltgen, 2009) and has seen first-hand cases of massive data breach and data misuse like Facebook.

Several academics state that millennials exhibit such risky behaviours or hold such attitudes towards risk online due to trust on websites (Obal, 2015). Trust is defined as "A psychological state of mind , where vulnerability is accepted based on positive expectations of behaviour by other person" (Rousseau et al. 1998) . Trust plays a key role in online interactions, as people have more difficulty understanding a third party's positive or negative interaction (Friedman et al. 2000) Lack of trust is the primary cause of most consumers online not using a service/ website (Monsuwé et al., 2004). Millennials , unlike the previous generations, have very little trust on establishments such as companies or the government and believe that most companies try to manipulate them (Nimon, 2007) However, while they shun such traditional systems, millennials demonstrate large amounts of trust on the internet by preferring to receive news via the internet as opposed to traditional newspapers or obtain information about products over the internet rather than enquiring at stores and (Bolton et al., 2013) This observation is contrary to several research paper findings that state that "people trust people, not technology" (Friedman, Khan and Howe ,2000) . Most millennials don't appear to take personal responsibility to educate themselves on the avenues open to them, in lieu of protecting their personal data as they don't see online safe as their personal responsibility (Lee and Kozar 2005). Millennials believe that the government must create more awareness of data protection (Davinson and Sillence ,2010; Larose and Rifon , 2007).

1.4.3 Are millennials willing to compromise privacy on the Internet for benefits

Consumers base their decisions by comparing benefits to risk during transactions (Metzger, 2004). Most Research indicates that while there is concern over how personal data is treated in such transaction, a significant number of consumers on the internet are willing to exchange their personal information as long as the benefit received is larger than the risk involved (Awad & Krishnan, 2006) This behaviour has been referred to as "privacy calculus" (Kobsa , 2007) where in a consumer begins to see his information privacy as a sort of entitlement which can be transacted for a kind of benefit as long as the risk involved are not larger than the benefit . This theory model has been tested by Xu et al (2001) and confirms that willingness to trade privacy for benefit exists.

A study conducted by The Direct Marketing Association in the UK in 2012 indicated that almost 31% of the population of consumers were not willing trade data for free services. However, a similar study conducted in 2015 showed that this number had dropped down to 24%, while the percentage of people who were ready to exchange personal information had risen up to 54% and almost 60% of this set were millennials (Ridley-Siegert, 2015).

Another study conducted by Mintel Research stated that almost 60% of Millennials were ready to share personal data and 30 % of the millennials who refused to share data, agreed to share data when incentives like discounts or coupons were offered. These numbers were in direct contrast to other generations with only 13 % of the preceding generation opting to share their data for benefits (Mintel,2015). There have been indications about the nature of data consumers are willing to share, with most opposed to sharing financial information and willing to share personal/ location information. It appears that currently, most consumers see their data as having value and are willing to transact it for services or benefits (Myerscough, et al., 2006).However, there are contrasting views stating that some millennial consumers are resigned about sharing data. They are often cynical as opposed to willing to trade their data but not ready to give up the services or benefits that result from such transition. A key reason behind this resignation was that as the world become more technologically connected, data exchange for benefits or services was inevitable and beyond their control (Giulia et al., 2018)

1.4.4 Millennial consumers awareness of how data is collected and used on the internet

Technological advancement in data mining and analytics have expanded the potential of consumer data (Dwyer et al, 2007). However, some studies claim that most millennials aren't too sure of how exactly their data is collected and stored on the internet by companies (Salazar and Woodward, 2017) and exhibit low levels of understanding of how such data is used (O'Brien and Torres ,2012; Sciencewise, 2014) Most companies do provide privacy options, security guides and detailed disclosure for users. These require the users to read and understand this information on their own and manage their data setting (Giving consent to having their data used or not) (Timm & Duven, 2008). However, many consumers including millennials seemed to not understand implications of their current behaviour on future security and often don't go through this information (Milne , George and Culnan 2004).

Some sources argue that on contrary, there is awareness on data privacy ,especially amongst millennials (Dommeyer & Cross, 2003).Research attributes the awareness to gradual acceptance of regulated of data exchanges with companies to a growing understanding of how data is collected and used, with studies showing that almost 2/3rd consumers understand how data exchanges worked (DMC, 2015) .Increasing transparent behaviours of business that engage in data collection are said to have contributed to this awareness. However, there is a gap between what consumer think they know and what they should know (Karvonen, 2007). The opinions amongst academics with regard to millennials awareness of how their data is collected remains divided, with most suggesting that millennials don't understand how their data is collected and used while the others believe that there awareness amongst millennials due to transparency amongst companies and better understanding of technology.

1.4.5 Millennials consumers awareness of the current data protection framework

According to Salazar and Woodward (2017) millennials have low levels of awareness about their privacy rights under data protection law. A study on privacy rights concluded that awareness of privacy rights and data protection laws generally low with almost 63 % of participants unaware of their rights (Phoenix Strategic Perspectives Inc., 2013). Academics recorded similar findings that knowledge of data protection laws was poor (Peifer, 2014). However, some say that people who had a university degree have more awareness of these rights (Salazar et al 2017) The GDPR Awareness Index, published by Kantar TNS shows that only 34% percent of the people were aware of the GDPR and most dialogue on this was professional than personal (Kantar TNS UK, 2018).

However, on the contrary, surveys conducted by the then Data Protection Commissioner (DPC) in Ireland demonstrate that legal awareness was increasing amongst about data subjects (DPC, 2013). Awareness of data protection appears to increase in millennials under certain circumstances such as cyber threats (Milne, Labrecque, and Cromer ,2009). A Recent study by the DMA (2018) shows that millennials are becoming increasing aware of their rights under the GDPR. However, there is no indication about the depth of awareness. There is contrasting literature on millennial's awareness of data privacy rights and this study intends to develop an understanding of awareness levels of data amongst millennials.

1.4.6 Need for study

Studies indicate that the number of internet users in Ireland is growing, with millennials leading the usage. Almost 98% millennials logging into the web on a frequent basis (Central statistics office, 2017). They also demonstrate that while most millennials, spend most of their time on the net, they aren't fully aware of who and what monitors/ saves/ uses their activities on the net. The government and the Data protection commission have taken several measures to protect Irish' population's data on the internet by creating awareness programmes (Dataprotection.ie, 2018b). However, there are no studies indicating if these measures are successful. There is gap in literature about the consumer's awareness on what is created specifically for them. Millennials, are the largest group of users on the internet and are therefore most likely to suffer violations of data privacy. Yet there are no studies that specifically address their awareness levels or target their understanding of these concepts. Understanding their awareness levels and attitudes data will enable the governments to formulate better strategies to improve awareness amongst them. Millennials are digital natives and there is significant evidence that indicates that they learn differently, understand privacy differently and have unique world views (Taylor, 2012). Traditional methods of generating awareness wouldn't work on them. Therefore, to address these gaps in literature, this study is undertaken.

1.5 Conclusion

Data is touted to be new currency of the business world with several businesses running based on data mining. Consumer data is valuable and a company holding personal data, under their control can have far reaching consequences in the coming decades. As the millennials enter their late 30-40s during this decade, their data on consumer- buying patterns, behaviour patterns and relationships can be profiled to sometimes have detrimental effects. Therefore, it is important to ensure that this data is under the control of the individuals. Governments are attempting to regulate this data and protecting their citizens, by passing various legislations that limit the gathering, storage and use of such data. Academics are critical of organizations that access/ distribute their consumer's data. However, the question that is particularly important to this debate is if millennial consumers are concerned about their privacy online and if they are aware of data protection rights available to them.

CHAPTER 2

RESEARCH QUESTIONS AND AIMS

2.1 Research Question

The previous chapter sought to highlight how data privacy is an issue amongst millennials consumers in Ireland today and why the awareness of data protection is required. A critical investigation of different issues surrounding data protection awareness and attitudes amongst millennials in Ireland and the recommendation for further enquiry and research, keeping in light this the central research question will be

What are the levels of Awareness with regard to data protection and digital privacy of Irish Millennial consumers on the Internet and their attitudes to the same?

2.2 Research aims and purpose of the study

This study seeks to understand how millennial consumers on the internet view their digital data. As highlighted in the literature review, there appears to be arguments supported by evidence for both sides of the spectrum, with some studies indicating that millennials consumers are increasingly aware and concerned about data privacy and protection and are actively seeking to enforce the same, while other sides show that there is a merely prima facie awareness of these concepts amongst millennials Irish consumers.

As the research intends to gain insight on the current situation in Ireland amongst millennial consumers on the internet, the following objectives have been set out to answer the primary research question based on themes identified within existing literature on the subject.

1)To determine the extent of Millennial consumers awareness of how their personal data is collected and used on the internet

2) To investigate their knowledge levels of data privacy rights and data protection measure available to them

3) To understand their attitudes toward their personal data-

- Are they concerned about their data?
- Do they take risk with regards to personal data on the internet?

- Are they protective of their personal data or are they willing to compromise this for perceived benefits?

Alongside this, the research also hopes to develop an understand how millennials' awareness levels can be improved.

To begin, it primarily looks at finding out if millennials are concerned about their privacy online and then to gauge the awareness levels they have over how their data is collected and how they can protect their data on the internet. Lastly, it looks at mapping the attitudes of these millennials toward their data, by deciphering their attitudes – Do these millennials consumers have an interest in protecting their data or are they willing to compromise or exchange their digital privacy for benefits.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

This chapter outlines the methodology followed to answer the central research question and fulfil the objectives outlined in the previous chapter. According to Saunders et al (2012) answering a research question by way of data collection and analysis, requires a systematic process. This process can be in the structure of a "research onion" as developed by Saunders, Lewis and Thornhill (2007). The research onion as visible in the below figure lays out an methodical chain of progression that leads to the creation of an effective and comprehensive research methodology by tackling each vital step in the process (Bryman, 2012).
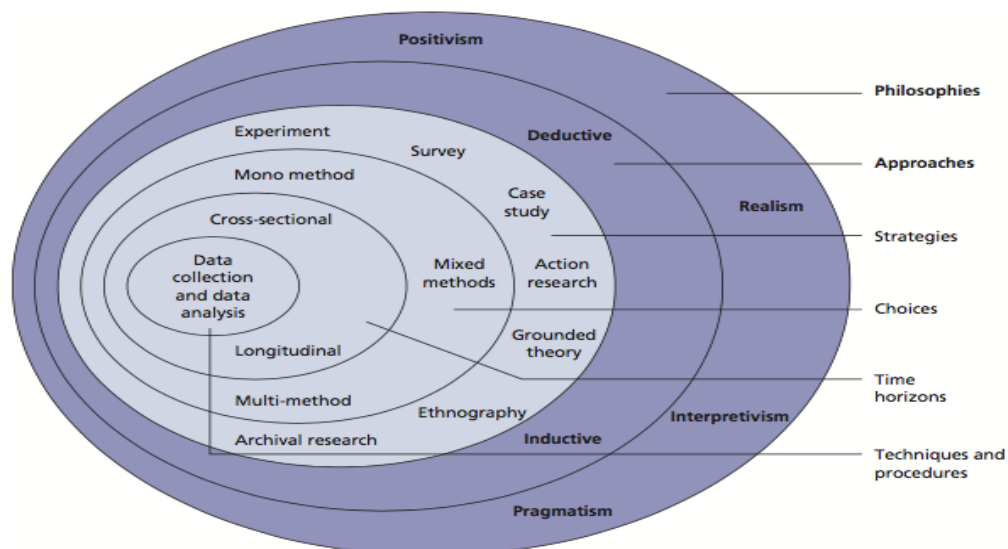
Figure 1: The Research Onion (Saunders, Lewis and Thornhill, 2007, p. 139)

In accordance with the research onion structure, primarily the philosophy behind the research will be discussed along with the approach to the research. After this, the design of the research, methodology choice, , time horizon, techniques and procedure will be dealt with.

3.1 Research Philosophy

Research philosophy is the beliefs or logic upon which a research would base and formulate the investigation into the subject (Goddard & Melville, 2004) and the choice of philosophy

being followed would be justified by the matter under investigation. Academics believe there are 3 reasons why it is important to understand philosophy (Easterby-Smith, Thorpe and Jackson, 2008).

- To validate choice of research methodology
- To develop an understanding of different methodologies available
- To delve from the path taken and be creative in use of methods

Research philosophy is shaped by ontology and Epistemology. Saunders et al. (2012). These paths outline the thinking behind how research questions are formulated (Bryman and Bell, 2007).

Ontology is broadly refers to the nature of reality and had two sub sections under it which are objectivism and subjectivism. Objectivism believes that social entities present in the environment are independent and not influenced by factors while subjectivism states that social factors influence social entities and understanding these factors helps in deciphering social phenomenon. this research has chosen subjectivism as it is attempting to decipher a social phenomenon by understanding the factors that influence it

Epistemology is related to defining what acceptable knowledge is (Saunders et al.,2012) but Epistemology is further divided into Positivism and Interpretivism. In this research, *interpretivism* will be subscribed to, as the fundamental idea of interpretivism is to work with the existing independent meanings within the social world by understanding and reconstructing them to use as the base of the theories (Goldkuhl, 2012) . Interpretivism is in contrast to the other main philosophy used to influence the research process – Positivism, which believes that factual knowledge can be obtained only via observation and measurement, without any scope for the human-interest element. Due to the nature of its views, positivism is generally used to study phenomenon in pure sciences and wouldn't be able to do justice to a study focusing on human social attitudes and awareness characteristics.

Unlike positivism, which operates on the ideology that people are merely social actors who react to external forces, interpretivism focuses on deciphering the causes of human behaviour. It opines that people are unique individuals, each having a distinctly different experience of the same objective reality and therefore have different responses to external forces (Collins, 2010) Therefore, this philosophy is apt for the research undertaken as this research also looks

at understanding millennial consumer's perception of an series of events online, instead of attempting to identify different variables that explain these consumer behaviours and map a relationship between them.

3.2 Research Approach

The most relevant research approach can be identified based on the most appropriate philosophy followed to answer the research questions and objectives laid out in the study. The choice was between two approaches, the inductive approach and the deductive approach.

The inductive approach is usually used when the study at hand is attempting to understand human beings and their relationship with the external world and is suitable for studies with a small number of participants. The deductive approach on the other hand is appropriate when the study is concerned with looking into if the observation fits with the theory present (Wiles et al., 2011) and usually, in this approach, the general theory is identified and the information obtained from the data analysis is compared and validated against it(Kothari, 2004) This research adopts the "inductive approach" . A primary characteristic of this approach is the movement from specific to general and usually, in this approach, observations are made first and then patterns and themes are identified from the observations (Beiske, 2007).

As the research at hand is looking to understand how humans react to certain situations and has a small number of participants, an inducive approach is deemed more suitable than the deductive approach. Unlike most research undertaken around data privacy and data protection, which follow deductive approaches, by looking into practices amongst vast number of participants, this study is using a inductive approach to understand how a small number of participants look at concepts such as data privacy and protection in depth. As an inductive approach guides the researcher to observe the environment, draw inferences, by identifying patterns or trends which lay base to the formation of theories, this approach is considered most appropriate in the current research setting, where the objectives are to understand attitudes of millennials towards a certain occurrence.

3.3 Research Design

The Research design encompasses the strategies, the choice factor and the time horizon of this project. It is the framework that covers the suitable methodology to be applied, the process of

selection of participants in the study and includes how the data will be collected and analysed (Flick, 2011). In this segment, the most appropriate strategies, the research choice and the time horizon will be identified by the researcher and the choices will be justified.

Research choices- This deals with the type of approach chosen, with the choices being mono method which refers to using only one particular approach to answer the research question, the mixed method which as the name suggests is a blend of qualitive and quantitative approach and the multi-method which include both approaches, separately to arrive at conclusions. (Saunders et al., 2007). The research choice for the study at hand is a mono method of qualitative analysis, where the data is collected and analysed through a singular qualitive approach and this is justified in the following paragraph.

3.3.1 Mono Method Qualitative Approach

This line of enquiry focuses on developing concepts that help decipher and identify meanings of social phenomenon in natural settings and relies on experiences, beliefs and outlooks of the respondents (Strauss and Corbin, 1990) . It is a approach to research where findings are made based upon observations and inferences from "natural environmental settings" where "phenomenon of interest occur in an organic, natural manner" (Patton, 2001). Qualitative research seeks to not merely determine an answer but also understand the reason for the answer, unlike quantitative research which only concerns itself with mere facts, data and uses these for predictions and generalization of findings (Hoepfl, 1997).
While quantitative researchers look at breaking down a phenomenon into fragments that can be understood and applied across similar situations (Winter, 2000) qualitative researchers study a subject deeply, by isolating all concepts related to the study, examining them in detail and then drawing conclusions (Glesne & Peshkin, 1992) . Quantitative research methods are highly reliable as they use standardized tools such as questionnaires and are useful to arrive at statistical or numerical answers whereas qualitative research often produces more valid answers, as it emphasizes on people real behave and what people actually mean when they describe their experiences, attitudes, and behaviours and therefore more useful to understand behaviours and Attitudes (Pope and Mays, 1995).

 Most research on privacy awareness amongst consumers has been quantitative research, that has arrived at percentage indications of awareness and attitudes, showing what percent of the

population held what belief towards personal data and what number of participants were aware of their rights (Phoenix Strategic Perspectives Inc., 2013; Kantar TNS UK, 2018)

However, the study at hand is not looking to arrive at numerical conclusions on awareness, by identifying the percentage of millennials who are aware about data protection and Privacy in Ireland. Rather, it attempting to develop an understanding of ***What do*** millennials know and ***how they behave*** towards a social issue – Data privacy and protection. Since the study is focusing on deciphering behavioural patterns amongst millennials towards their data quantitative analysis would be discounted as it tends to emphasis on measuring a phenomenon rather that developing an understanding of it (Michell, 2005)On the other Qualitative research approach is flexible about how data is collected and allows for a host of data collection methods such as document analysis, interviews, observations amongst other .As qualitative research is most commonly used for understanding the meaning of social occurrence , rather than forming links between established variables (Feilzer, 2010) it is deemed most appropriate for the study at hand. Due to time limitations, the mono or single method of qualitative research was chosen.

3.3.2 Time horizon

 This is the duration or the time frame by which the study or research should be concluded. The research onion lays out two kinds of time horizons namely the cross sectional and the longitudinal (Saunders et al. 2007) The former stands for data collected at a certain point in time and the latter relates to data collected over an extended duration of time.

The longitudinal study is particularly useful to study a occurrence with a factor that changes with time. While this study would benefit from a longitudinal time horizon, to correctly understand, if major changes in technology would impact a millennial's perception and awareness levels of data privacy and protection, time limitations have led to choosing cross sectional time horizons.

3.4 Data Collection and Analysis

Focused data collection is an essential part of qualitative research. Selecting a appropriate method of data collection has significant impact on the validity and the reliability of the study. Qualitative data collection is three-fold in nature 1) Augment a clear plan of collection 2) Locate and sample the population of interest 3) Obtain the relevant data (Ranney et al., 2015). The nature of the subject to be researched drives the method of data collection. Qualitative research offers a variety of methods for data collection such as observations, textual or visual

analysis (eg from books or videos) and interviews (individual or group) (Silverman, 2000). The most common method used is interviews and or focus groups (Britten 1999). In this case study, Interviews and focus groups were considered for data collection. While interviews and focus groups do share many similar characteristics, the former are conducted usually with one respondent at a time and the latter are usually conducted in a group setting. Interviews are the most appropriate methods in cases where there is scanty information about the research topic or where in dept information is individual participants. They are also considered most effective when investigating a sensitive issue, especially issues where respondents would prefer to talk in private than in a group (Gill et al., 2008). Focus groups on the other hand are very useful when the research intends to figure out collective views on a phenomenon and can produce rich, contextual information about participant's views and beliefs (Morgan,1998). However, due to the interactive nature of a focus group, the interactions will often be based on group dynamics which generate biased or inaccurate data that doesn't reflect a person's personal view. In Interviews, unlike focus groups, it is easier to learn the personal views of a participant via face to face, one on one exchange (Robson, 2011). Therefore, interviews were chosen as the most appropriate method of data collection as they provide more in-dept information about the topic and issues being investigated, despite the ease of a focus group.

3.4.1 Selecting type of Interview

Interviews are broadly categorized into structured, semi structured and unstructured interviews and are useful in different scenarios and for different data collection requirements (Punch, 2005). Structured interviews are where the questions to be asked are predetermined and the answers obtained fall into clear category of answers, which can be quantified and assessed using mathematical modelling, while unstructured interviews are flexible and open ended, intending to collect data on personal reflections of participants. Semi structured fall between the both, with a clear set path for the interview, via prior formulated questions, while incorporating a certain flexibility to peruse any leads or paths that emerge in the process of the interview, that has not been previously anticipated and may lead to valuable data (Silverman, 2004).

Semi structured interviews, were chosen due to their flexibility. These interviews include several pre-determined questions but make allowances for divergence to peruse an idea and are ideal to chart out new lines of inquiry (Ward, Legard and Keegan, 2003). These interviews will be used to collect primary data. While semi structured interviews consume more time than

structured and lack a verified standard, which raises questions about their validity (Creswell, 2009) they are deemed most appropriate for the current research as they are in line with the research philosophy. The interview question was based on questions formulated and verified by a similar, previous study (Salazar et al, 2017).

3.4.2 Population and Sample

A sample size is the number of respondents chosen to represent the population being studies and the sampling technique is the method used to pick up these participants (Newman, 1998). The technique used in this study is **non- probabilistic sampling,** which doesn't rely on random selection bur depends upon researcher's approach (Tansey, 2007) . This classification is broad and has several types of techniques under it amongst which Purposive Sampling will be undertaken. Purposeful sampling is special to qualitative research. It entails interviewing a pre-defined group of participants, who are identified by the research as most appropriate for the study.It provides the appropriate set of people with specific characteristics (Kidder, Judd and Smith, 1991). The respondents chosen for the study must represent the population being studied and this must be verified by a statistical study that validates the choice (Graziano and Raulin, 2009) However, due to lack of time, this validation hasn't been possible and is identified as a limitation to the study.

As per Non-probabilistic purposive sampling methodology, the researcher has selected 7 participants based on their educational levels and occupations so that there is wide spectrum of influences on awareness and attitudes. Literature review indicates that awareness levels amongst graduates was higher, so the sample includes both university graduates and non-graduates. Research also states that most awareness is on a professional level rather than a personal level, so the sample includes employed people and non-employed people.

3.4.3 Choosing Interviewees

The key factor in obtaining in-depth knowledge about an issue, through semi-structured interviewing is the number of interviewees and the relevance of the knowledge they possess to the issue being researched (Kvale, 2008). Some researchers state that 12 participants must be interviewed to obtain sufficient data while others opine that size isn't the main criteria to obtain rich data but depends on how the process is carried out (Baker and Edwards, 2012; Ruane and Wallace, 2013).

As there were time constraints, interviewing many respondents wasn't feasible. 7, participants were interviewed as part of the study. In accordance with the topic being studied, it was critical that only millennials living in Ireland should be interviewed. The participant birth date range, based on the literature review had to be between the years 1984-2000. Since the research was being guided by the purposeful sampling technique, the respondents chosen had to be able to be able to provide information that would answer the research objectives. The 7 participants were identified by their occupational and education levels. Convenience sampling came into play as certain participants were chosen based on their availability and accessibility to the researcher. The people who took part in the interview were from different backgrounds and at different stages in life to ensure there was diversity of people. 6 of the 7 participants were from county Dublin and 1 participant was from Limerick.

Table 1: Contains the profile of the participants. the identity of the participants has been protected by anonymisation.

Name	Age	Occupation	Education Levels
Participant1	26	Software engineer	Masters level
Participant 2	23	Childcare worker	bachelors
Participant 3	20	student	Leaving cert
Participant 4	25	engineer	masters
Participant 5	22	maintenance	Leaving cert
Participant 6	28	student	Masters
Participant 7	27	Technology implementation analyst	masters

While the interview conducted was of a one on one nature and note taking was the primary record of data collection, to maintain the authenticity of the data, audio recording was undertaken alongside the primary method for assistance in transcribing data.

3.4.4 Pilot study

A research instrument or technique developed for a study must be "pre- tested", to identify any shortcomings or drawbacks (Baker, 1994). To iron out such issues, a pilot study was conceptualized and conducted. A pilot study, is essentially a "trail run" (Polit, Beck and Hungle*.,* 2001) and helps in testing the feasibility of the research and identifying issues. Ideally, pilot studies must be conducted, several times during the research process, primarily at the outset of the study, to identify potential issues of the topic being studied and at a later stage, to examine the research process (Van and Hundley, 2002). However, due to time constraints, the pilot study was conducted at the initial stages of data collection, with a Irish millennial, who was not a respondent in the main study. The pilot study led to the following observations and modifications.

Recording of interviews- The interview was recorded via phone and led to the observation that certain parts of the interview weren't audible due to background noise (music played in the location). The location was thus changed to a more private location and the recording instrument had to be held in the hands of the speaker.

Time duration- The researcher had allocated a duration of 1.5 hours to the interview process, but as the semi- structured interview unfurled, it was noticed that a duration of 1 hour was sufficient for a full-fledged interview. The time duration per interview was thus changed.

Interview Questions: The interview had 20 questions. During the pilot study, 4 were identified as similar questions and were eliminated. Another 5 questions were added by the researcher based on the certain comments made by the interviewee, which were deemed important to the study at hand. These can be found in the appendix 2.

Development of the interview schedule:
It has recommended that an interview schedule should be constructed keeping in mind the p0articipants and due importance should be given to them, since he or she will be doing the

work by supplying the answers to the questions' (Mann, 1985). The participants were given flexibility of time and place. All interviews were done face to face at the time and location of the participant's convenience. The researcher also avoided probing issues that were sensitive to the participants.

3.5 Data Analysis

In this study, the data collected was analysed using "thematic analysis". Thematic analysis is a method of data analysis, where data is systematically studied and common reoccurring ideologies relevant to the research topic are identified and interpreted. (Fereday and Muir-Cochrane, 2006). This process revolves around identifying a pattern amongst the data and interpreting it (Rice & Ezzy, 1999).

The reasons for this choice are threefold. Primarily, Thematic analysis has been commonly used in studies based upon inductive approach, where "attitudes and beliefs" of people are examined (Attride-Stirling, 2001), much like this study. Secondarily, thematic analysis is accessible and flexible, simplifying the complexities of qualitative study by laying out a charted course of data collection, theme identification and interpretation (Braun & Clarke, 2006). Lastly, thematic analysis compliments the research strategy used in this study – a stratergy based on certain grounded theory principles which much like thematic analysis method are built around using raw data to form themes and subsequently form a theoretical framework.

The thematic analysis is carried in via procedure laid out by Braun & Clarke (2006) which has been segregated into 6 phases which are as follows

- Become familiar with the information collected via through reading and re-reading of the same.
- Generation of primary codes
- Looking for themes
- Identification and review of potential themes
- Defining and naming themes
- Producing reports

The first stage of this analysis is not unique to thematic analysis and is common amongst all qualitative research methods. In this stage, the data collected was gathered, transcribed into

word and read and re-read thoroughly to develop a familiarity with the information (Braun et al, 2006) recommend that the data not be merely read as data but be read analytically and critical.

3.5.1 Coding

Coding is predominantly identifying and labeling features of data that is important to answer research questions (Tuckett, 2005.) In this initial stage, every time some information appears to be related to the issues, it is coded. Primarily, the data collected was transcribed into MS word. It was then studied in detail and then coded. The initial coding was done manually on MS word. the coded data was then categorized and organized under each code and potential themes were identified. the following ideas were used to create and segregate data into codes as advised by (Bruan et al,2012).

- Meaning: what do people feel about things, how do they process certain information
- Participation: what measures are taken, choices made
- Causes: what leads towards this
- Consequences: outcomes of choices, attitudes, behavioural patterns

3.5.2 Themes

In the 3rd stage, themes are hunted by the researcher. This stage requires looking at codes and locating overlaps and similarities. Following this, themes are spotted and examined. These were evaluated again to bring coherence to the data and since it isn't an exploratory study, certain codes that weren't relevant to the research subject were discarded. The final code-theme was generated by removing reoccurring themes. All themes were then viewed form the research question and objectives point of view and irrelevant themes were removed. masdaq 2018 software was used to organize data at this stage. Four themes emerged which were analysed. Generating themes requires primarily creating an explanation and then comparing this to ensure there is consistency between it and the data and the theory (Vaismoradi et al, 2016).

A subsequent comparison of the codes, will enable to highlight patterns and themes within the data sets, which will be used to draw conclusions. While most of the coding and theme identification was done manually, MAXQDA 2018, A software for qualitative data analysis was used to manage data ((MAXQDA - The Art of Data Analysis, 2018).

3.5.3 Validity

Despite the developments within qualitative methods of research and growing popularity, there have been certain drawbacks within these methods such as lack of accessibility to research notes unless uploaded properly, doubts regarding the accurate representative value of the sample used, research bias amongst others(Huberman and Miles, 2012) This in comparison with quantitative analysis where mathematical accuracy is assured leads to academics leaning on studies conducted via quantitative methods over qualitative methods. Keeping this in mind, the researcher has followed a validity method of member checking **to** ensure validity of qualitative analysis (Creswell and Miller, 2000).

3.6 Ethical Considerations

As the research includes interviews and inferences from such interviews, there might be potential violations in privacy of thought and beliefs of individuals who will be interviewed. Participant's names shall be anonymizing, Due care will be taken to ensure that all participants will sign a consent form that permits the use of their data for the research specific purposes which is enclosed in Appendix 1. All data will be anonymized, stored securely and disposed at the end of the research.

CHAPTER 4

FINDINGS AND ANALYSIS

In this chapter, data obtained from the interviews conducted has been analysed using thematic analysis as outlined by Braun & Clark (2003). The analysis was conducted in the manner discussed in the previous chapter. The findings that emerged from the interviews will be presented and will be used to answer the research question and fulfil research objectives.

The following Themes were identified to fulfil research objectives

Theme 1: Millennials awareness about data privacy and data protection is surface level

Theme 2: Millennials are concerned about their personal data online

Theme 3: Attitude to Risk- Millennials indulge in risky behaviours on the internet

Theme 4: Millennials are willing to Compromise data privacy for benefits

4.1 Millennials awareness about data privacy and data protection is surface level awareness

This research set out to answer the main research question by identifying 4 objectives amongst which the first objective was - To determine the extent of Millennial consumers awareness of how their personal data is collected and used on the internet. Keeping the first and second objective in mind, the first theme was constructed:

Within this theme awareness of data privacy, data protection and attitudes towards these were included, as data obtained was linked. Findings were as follows - ***All participants were aware that companies collect data online*** Participant 1 said "Yes I am aware that my data is collected on the internet. I know that it is collected by pretty much all the services and applications I use" Participant 3 said " Yes, I am aware that companies collect data and sell it".

However, most participants didn't know how the data was collected and used - Participant 2 said- "Yes, I know data is collected not too sure how it is collected or used" Participant 3 said "I often hear about how companies collect our data but I have no clue what happens to it" Participant 1 said " I do know the basics of how companies use data, but not fully aware of the technology behind it".

All participants exhibited some knowledge of GDPR. Participant 2 said "Sure, I do know what GDPR is, it's that European regulation that is related to our privacy" Participant 7 said" I do

know it's for data protection in Europe." Participant 5 said "I think it has something to do with the stuff we post online".

However most participants had little to no awareness of their rights under GDPR with 5 participant having no awareness and 2 participants having superficial awareness . Participant 2 said " I had no clue that there were rights! Sure, I know someone cannot touch or miss use your data, but I didn't know these were like actual rights" Participant 5 said "I do know that now companies cannot hold data without your permission but I don't know what kind of data this is" Participant 1 said "Yea, I do know that the I have some rights, not in detail though"

Most awareness of GDPR stemmed from work and some from changing policies. With only Participant 1 said "I know about the GDPR due to seminars and policy changes at work" while Participant 4 said "my company conducted awareness programmes about GDPR" Participant 7 said " My boss wanted us to all go through GDPR impact assessment" Participant 3 said " I noticed most sites had begun to ask consent and though I didn't read it in detail, I saw something about GDPR on a US page".

Education didn't seem to bring better awareness of data protection as university educated participants and non-university participants seemed to have some awareness of GDPR. The non-university participants had less depth of awareness nevertheless.

All participants didn't feel the need to voluntarily educate themselves about GDPR. Participant 2 said "ah it's a hot topic now isn't it, but I honestly wasn't bothered to figure what the fuss was about". Participant 6 said "I've come across a few articles on the net and heard a lecturer mention it. I'd probably say that my knowledge level is minimal, however I do attempt to educated myself, but it isn't an active conscious decision".

All participants agreed that governments and companies had major responsibility of bringing awareness. Participant 3 said "government must do fun posters to make sure our generation watches it" Participant 2 said "Governments bring these rules, so they must make sure we know" participant 5 said "I mean I can hardly understand the law words, so its government's job to inform us."

The findings indicated that millennials were aware that companies collected their personal data on the internet but didn't understand the intricacies of how it was collected and used. Some participants knew cookies were used to collect data but could not explain how they worked. This implies that while there is surface level awareness of data collection, there is a poor awareness of the how the data is used. Only 2 participants stated that they knew companies-built profiles based on consumer data. These participants worked in the software industry so

there is a bias in findings and might not reflect the awareness levels of millennials in Ireland in general.

The awareness of GDPR was primarily due to work and only 1 participant stated that their awareness was due to consent forms on the internet. Participants who were aware of their rights had only surface level awareness as they could not name their rights in detail. This implies that there is superficial awareness of GDPR and that awareness measures from the government have limited reach. Participants are not fully educated about their legal rights and remedies under the GDPR and don't know when their rights are being violated. This situation can lead to companies taking advantage of these consumers.

All participants stated that they wouldn't voluntarily attempt to change their awareness levels, and several indicated that it was role of the government and the companies to create awareness as these subjects were "too legal" for an ordinary person to understand. This behaviour could be linked to the complexity of legal and technical jargon around these issues, which make learning about it less appealing to millennials. This topic requires more research to understand how millennials can be motivated to improve their awareness.

The idea that they weren't responsible for awareness and that government and companies had a duty to create awareness was re-occurring, implying that millennials in Ireland didn't feel obliged to understand the current legal framework on Data Protection. This lack of responsibility could be attributed to how millennials perceive the world and the government. This attitude can be also attributed to the complexity of the legal issues around data privacy.

4.2 Millennials are concerned about their personal data online

The research objective 3 was to understand if millennials are concerned about their personal data. Theme 2 was constructed to answer this question.

The participants all stated that they were concerned about their information on the internet Participant 1 said "I am thoroughly concerned about who accesses my data". Participant 2 said "I am concerned about what happens to all the data I put on the net without thinking". ***Concern was largely related to financial information on the internet*** with 6 out of 7 participants stating that their concern was at its peak when they used financial information online with Participant 2 stating "I am often very worried about my credit card details and their security on the internet"

. Participant 6 echoed this statement stating " I am not too aware of how data is collected or protected by I sure am concerned if my bank details and transfers are safe on the internet" .*Concern was less with regard to personal data but was still present and seemed to be growing with growing awareness of privacy issues* as evidenced by the statement of Participant 4 who said " when the Facebook scandal came to light, my concern for what was happening with my data also increased. Sure, I was concerned before, but it wasn't anything major until this incident" and Participant 3 said "I often feel that someone might steal my information online. Am also concerned that even simple data about me can be used for a malicious purpose against me".

Findings indicate that concern levels amongst millennials appear to be quite high, despite lack of awareness and understanding about privacy and data protection. This is a rather paradoxical situation because participants don't seem to be bothered about learning how to protect their data online but still express concern over their data. Concern levels seemed to be linked with the nature of information and highest concerns are toward financial data. This implies that millennials prioritise money over privacy of their other data. Growing awareness of privacy issues online seems to be causing concern levels to increase which implies that awareness is often motived by a threat to security. The awareness of privacy issues online can be linked of concern as participants as most don't really understand the implications of a third-party accessing their data until it becomes clear to them. When they do see what can be done with their data, their worry increases. However, concern didn't seem to trickle into action towards improving awareness.

4.3 Millennials indulge in risky behaviours on the internet

Research objective 3 was to understand millennial's attitude toward risk – theme 3 was constructed to fulfil this. The theme millennial attitudes to risk emerged. The findings under this theme are as follows *All participants exhibited risky behaviours with regard to their personal data on the internet.*
6 of the participants stated that they never changed their passwords on a regular basis and saved their passwords on an easily accessible location unless it was financial data. All of them did not read the terms and conditions of consent forms unless it was financial data. Most of them didn't check if the sites they were using were secure sites. 5 out of 7 participants didn't review or update their privacy options on sites. Participant 1 said " I am cautious about what I reveal

on the internet and have set difficult passcodes for most of my online presence" . Participant 4 said "I did try to read terms and conditions several times, but got bored midway and just clicked accept" and participant 3 said " I use a fair bit of online site to upload and edit my photographs and while I do this via a secure account, I've never thought of it until the site began to suggest names for my albums, based on my location" participant 5 " I constantly check in on various applications, upload my location and review places- it's how my gang moves" However, *all participants seemed to take precautions online when it came to financial information*. Participant 2 - "I am kind of cautious about my financial movement online and don't log in using WIFI but use my personal network for financial transactions" . Participant 4 said "I don't give my credit card details online unless it is absolutely necessary.

Most Risky behaviour stemmed from trust on websites with participants opting to give financial and personal information to websites they trust, not reading any consent forms of trusted websites and not monitoring what personal data these sites accessed.
Participant 7 "I usually make sure I make credit card information to trusted websites like amazon, spottily and Netflix" and participant 5 saying "if they are reputed brands, I allow them to access my location, my personal details, I mean like everybody does it bro"
participant 6 "I don't check the terms and conditions before accepting- I mean they cannot steal money or my identity, right?" Most of my health data / college data is saved on the internet, on various apps whose terms I haven't read".

However, another finding for cause of risky behaviour emerged – *All Participants were aware of risk but didn't take it seriously-* most participants were aware that by losing control of data could be nasty, but nobody took this seriously or saw it as a cause to worry. Participant 3 said " I often become concerned about what happens to my behaviour online but I eventually get out of that zone and forget it" Participant 7 " I try to engage in safe behaviours but often than not , I fall prey to laziness".

The findings show that all participants, despite being concerned about how their data was handled online and knowing that there were risks, still took risks with their data on the internet, by engaging in behaviours that could potentially lead to loss of control over their data. This contradictory behaviour seemed to stem from trust in certain websites but was not explanatory enough understand behaviours like saving passwords in easily accessible places or not reading consent forms. The finding that millennials are not taking risk seriously could be a plausible

explanation for this type of behaviour. However, when it came to financial information, risky behaviour amongst participants reduced , highlighting a trend that money motivated millennials to act upon their concerns online.

Another finding was that participants usually didn't read privacy notices or consent forms due to language and length. This lack of interest was predominantly due to "legal language explanation" and "long boring explanation" and tricky "web designs", as evidenced in theme 1 where millennials seem put off by complexity of legal issues surrounding data privacy.

4.4 Millennials are willing to compromise data privacy for benefits

Most Participants seemed to be willing to compromising data privacy for benefits with 5 out of 7 that they were accustomed to trading their data for benefits to a point that they didn't examine such behaviour. participant 3 said– " I often sign up on random pages, for freebies" Participant 6- " I've saved loads of personal information on webpages due to the ease online of accessing it".

Some participants were ready to exchange data when risks involved weren't high - 6 out of 7 participants said they exchanged data when they were sure the risk involved wasn't high, with participant 1 saying– "No, my data is very important to me and I would never exchange it for benefits unless it is some minor information like name and fav brands etc" " as long as the transaction is with reputed company and it's a small set of information, I'm game*." Most participants seemed to view their data as having value, that could be exchanged for gains like services.* Participant said 60

. "most companies have this offer – they get you to create an online account and they offer you discount, I've done that lo

ads of times for the crazy insider online sales". Participant 2 " due to financial constraints, I use subsidized versions of software online, in exchange for personal information".

However, *some participants seemed to be resigned to sharing their data,* with believing that "that's how things work now" as evidenced in participant 1 "initially I was uncomfortable with sharing my card and home details with apps like my taxi but I later learnt my friends would get amazing deals, so I gave in as it's an app everyone uses " and participant 4 said "I hate saving credit cards but I don't want to buy things via the guest user option as most companies process these orders slower than member and like millions use this site to shop and their information is intact right ".

The finding indicated that all participants were willing to compromise with privacy for free services at some level, with most participant saying that they did consider the risks occasionally and made sure that the risk involved didn't seem to overweigh gains as evidence in the literature There was common belief that personal data was of value and could be exchanged for gains, Participants were ready to barter their data for returns online. Another finding emerged that a portion of participants weren't eager to share data for benefits but did so out of resignation as the services that they were exchanging such data for appeared more important. This finding shows that despite all participants willingly trading data for benefits, there was certain data that they were slightly concerned about, which as identified in theme 2 as financial data. However, they still participated in such data exchanges, especially with "trusted" websites, because otherwise they would lose out on gains. They seemed to be resigned to the new systems, despite their lack of willingness. This finding, seemed to re-occurring when data was shared for benefits like medical or financial history on the internet, with most participants seeming resigned to giving up credit card/ bank account / purchase history information online because of benefits such as ease of transaction, faster processing of payments, saver deals such as free trips on taxis apps, cash back on cards and better services such as reduced prices on most ticked booked online at within the entertainment industry and holiday industry.

CHAPTER 5

DISCUSSION

5.1 Discussion

This chapter will interpret findings of research and link with the existing literature on data privacy and attitudes of millennial consumers.

Contrary to the literature (Dommeyer & Cross, 2003) findings indicated that Most millennial consumers are aware that their data is being collected. However, there is poor knowledge of how this data is used by companies, which is consistent (Salazar and Woodward, 2017; O'Brien and Torres, 2012) with the literature on the subject. This lack of awareness of technical aspects of data mining is often cited as a major issue in today's technology world. Most academic research on the subject doesn't make a distinction of nature of awareness - how data is collected and why it is collected. This observation draws out the limitations within current research that often assume consumer's awareness of data being collected also implies knowledge of how this data is being used.

Since millennial consumers in Ireland have poor awareness of the technical aspect of data collection, awareness measures conducted by should include how third parties collect and use data. Technological jargon must be simplified to laymen's terms so that technical understanding of this issue improves.

Findings also indicate that most participants are aware of the GDPR, opposing the literature on the subject that there are low levels of awareness of GDPR (Kantar TNS UK, 2018) and supporting to a certain extent, the survey conducted by DPC in Ireland that showed that there was awareness on data protection (DPC, 2013). However, it is drawn out that Millennials have only a surface level understand of GDPR and are not aware of what rights and remedies are available to them under the GDPR. Studies on awareness of legal rights provides similar statuses of legal awareness (Phoenix Strategic Perspectives Inc., 2013) and literature collaborates these findings (Peifer, 2014). Since millennials aren't aware of their rights, they might not report violations online and companies can take advantage of this situation to harvest data illegally. As the Government in Ireland is actively working towards improving awareness

levels, this finding indicates that focus should on creating in-depth awareness of rights and remedies available to data subjects under GDPR, in a manner that millennials find appealing.

It was determined that most awareness stemmed from work related situations, which is in line with previous research on this subject, undertaken by Kantar Uk indicating that most discussions on GDPR are work related and very few people actually talk about GDPR outside of work (Kantar TNS UK, 2018). Since millennials don't find talking about GDPR interesting, awareness programmes must be centred around what appeals to millennials like videos or posters rather than meeting or seminars. Awareness measures taken by the Government should incorporate basic, simplified explanations of the law and technology around this issue. Language used in such measures must be customised toward millennials.

Surface level awareness on data protection and privacy seems to go hand in hand with Irish millennial's nonchalant attitude toward ensuring their data is protected, as per the findings. They don't seem to be bothered about data protection and have a rather laid-back attitude towards online privacy, which has been highlighted in previous studies. (MIP, 2015). They don't take responsibility to increase their awareness levels, by educating themselves on current data protection laws and security methods. This pattern has been backed by literature verifying that millennials didn't believe that updating themselves about privacy online was their personal responsibility (Lee and Kozar 2005; Larose and Rifon , 2007; National Cyber Security Alliance 2012).

This is a worrying trend because while the government in Ireland is taking measure to create awareness, it cannot force awareness on millennials. There must be an initiative from the millennials to learn about their rights. Companies must also be legally bound to educate consumers on how they use their data in the simplest way, customised to facilitate learning amongst their user base. More research must be undertaken to gather clear insight on how millennials can be motivated to improve their awareness levels. It has been observed in the literature that millennials' awareness on this topic increases when exposed to threat (Milne, Labrecque, and Cromer, 2009). Education on threats online can be a starting point towards motivating millennials to improve their awareness.

Despite a lack of inclination to improve awareness, millennials still express concern over their personal data especially financial information as evidenced in findings. This behaviour has

been identified in literature (Malhotra, Kim and Agarwal, 2004) and indicates that millennials care about their personal information. It also shows that money is an important aspect of a millennials life. Millennials still hold on the belief that the worst thing to happen online is financial loss. It was observed that, when awareness levels increased, concern was higher, with previous studies supporting this co-relation (Olivero and Lunt, 2004). Increased awareness translates to understanding the implications of privacy issues. This observation that when millennials understand what happens to their data online, they actually care more. This also show the importance of awareness programmes. Programmes customised towards millennials can go a long way in creating more awareness.

One of the most worrying findings of this study was that despite high concern levels, millennials still engaged in risky behaviour online, echoing literature on the subject that identified this behavioural pattern (Mintel, 2014 ; Levin & Abril 2009; Carmichael, 2014; Fleming and Adkins, 2016) .This attitude as observed in the literature review and findings, could be attributed from millennial's ack of awareness of data privacy protection, that made them care less about personal data .This behaviour could also be partially attributed to trust, as most millennials showed risky behaviour with trusted websites . Most millennials didn't read consent forms or privacy notices due to a mix of these attitudes- they didn't care enough and trusted the websites to safeguard their interest. Another observation that millennials did show less risky behaviour when the activity online was related to money. This was a reoccurring theme within the study, similar to millennials concerns about financial data showing that money was a priority amongst millennials and motivated them to act on their concerns.

Millennial consumers were willing to compromise with privacy for services or benefits and most followed the privacy calculus while coming to this decision (Kobsa , 2007) and viewed their data as having value and could be traded for benefit as outlined by the privacy calculus model (Xu et al 2001). This positions them as active participants within the emerging data sharing economy and strengthens the theory that as long as there the risk doesn't seem great, millennials willingly share their data.

However, while on the surface, data trading appeared second nature to most millennials, there was a sense of resignation observed beneath the surface, when trading financial information. From this, it was understood that not all millennials willingly participate in data exchanges for benefits, some do out of resignation and cynicism as observed within previous research on the

subject (Giulia et al., 2018; Ward, Bridges and Chitty, 2005). This shows that millennials still care, to a certain extent about their data privacy online.

Recommendations

This research provided an insight into the attitudes and awareness of millennial consumers on the internet with regard to privacy and data protection in Ireland. It is clear from this research that despite government attempts to increase awareness levels, millennial consumers have low levels of awareness of what happens to their data online and their rights about data protection. The Government and The Data Protection Commission must create specific awareness programs to target millennials by way of interactive sessions, posters and videos. Companies should conduct more research and tailor their consent forms based on their users ages. Risky behavior amongst millennials should be discouraged by authorities, by demonstrating the implications of such risk. More generational specific research should be undertaken on awareness and attitudes of privacy and data protection, with emphasis on millennials, who are one of the largest segments of consumers on the internet. Research should not merely be based on how many people know but rather on what people know, when it comes to data privacy and protection.

CHAPTER 6

CONCLUSION AND LIMITATIONS

6.1 Conclusion

Millennials are one of the biggest segments on the internet. As digital natives, millennials are habituated to doing all their activities on the internet. Since they are the largest participants on the internet, it is important to know where they stand with regard to privacy and data protection online. The objective of the study was to understand the attitudes and awareness levels of millennial in Ireland about privacy and data protection on the internet. 7 semi- structure interviews were held. The researcher asked questions regarding their privacy concerns, risky behaviors, awareness levels amongst others.

The study found that with most millennials had prima facie awareness of privacy and data protection. Despite being digital natives, they didn't seem fully aware of the technology behind how data is collected by companies. They also showed ignorance of their rights under GDPR This ignorance stemmed from being put off by these issues due to complexity of the issues, legal and technical jargon. They strongly believed that it was the duty of the government and companies to bring awareness of these issues.

They were concerned about their privacy online, with most concern centered around their financial information. However, they still indulged in risky behaviors online like not reading consent forms and auto saving information online. Most millennials were willing to trade data for benefits but were wary of transactions involving money. Most of these finding had already been studied in previous literature. The findings also indicated that risky behaviors of millennials online were linked to trust on websites. They seemed willing enough to participate in the emerging data sharing economy but under the surface there was a feeling of resignation towards this system.

6.2 Limitations

This segment provides the other validated areas in which research could be expanded. This study focused only on millennials in Dublin and limerick, and therefore this sample wouldn't adequately represent millennials of Ireland. The sample size, due to time constraints was

limited to 7 participants, which would be a drawback to obtain more accurate and varied perspectives. The researcher has taken all measure to ensure no personal bias or expectation should affect the study. However, in the formation of the interview questions, there might be a level of bias due to need for potential answers to fulfill research questions. This research followed the mono qualitative path due to time constrains but would have benefited from mixed method approach to research.

CITATIONS

Aboim, S. & Vasconcelos, P., 2013. A critical reappraisal of Mannheim's classical approach. *European Journal of Social Theory,* 17(2), p. 165 183.

Allport, G. W. (1937). *Personality: A psychological interpretation.* New York, NY: Holt Rinehart & Winston.

Altman, I., 1975. *The Environment and Social Behaviour.* Brooks/Cole, Monterey, CA.

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative Research*, 1(3), pp.385-405.

Austin, L., 2003. *Privacy and the question of technology*. Law and Philosophy 22, 119–166.
Baker, T.L. (1994) *Doing Social research (2nd Edn.)*, New York: McGraw-Hill Inc.

Awad and Krishnan (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, 30(1), p.13.

Baker, T. L. (1994*). Doing Social Research* (2nd ed.). New York: McGraw-Hill Inc.

Baker, S, E and Edwards, R. (2012) '*How many qualitative interviews is enough'.* Discussion Paper. NCRM.

Barnes, S., B. (2006) A Privacy Paradox: Social Networking in the United States [Electronic Version]. *First Monday,* 11 (9). http://www.firstmonday.org/ISSUES/issue11_9/barnes/ (Acessed on 23/06/2018).

Beiske, B. (2007). *Research Methods: Uses and limitations of questionnaires, interviews and case studies,* Munich: GRIN Verlag.

Bharadwaj, A., El Sawy, O., Pavlou, P. and Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly*, 37(2), pp.471-482.

Black A, (2010) Gen Y. Gen Y: who they are and how they learn. *Educ Horiz.*;88(2):92–1

Bolton, R., Parasuraman, A., Hoefnagels, A., Migchels, N., Kabadayi, S., Gruber, T., Loureiro, Y., and Solnet, D., (2013) "Understanding Generation Y and their use of social media: a review and research agenda", *Journal of Service Management*, 24 (3), pp245-267

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology ,* 3 , 77–101. doi:10.1191/1478088706qp063oa.

Britten   N.   Qualitative   interviews   in   healthcare. *In* Pope C, Mays N (eds) *Qualitative research in health care.* 2nd ed. pp 11-19. London: BMJ Books, 1999.

Burgoon, J.K., Parrott, R., LePoire, B.A., Kelley, D.L., Walther, J.B., Perry, D.,1989. Maintaining and restoring privacy through communication in different types of relationship. *Journal of Social and Personal Relationships* 6, 131–158.

Bryman, A. (2012*). Social research methods* (5th ed.). Oxford: Oxford University Press. Collins, H. (2010) "*Creative Research: The Theory and Practice of Research for the Creative Industries"* AVA Publications

Carmichael, S. (2014). Do Millennials Believe in Data Security?. *Harvard Business Review*. [online]   Available   at: https://hbr.org/2014/02/do-millennials-believe-in-data-security#comment-section [Accessed 25 Jun. 2018].

Central Statistics Office, 2017. *CSO statistical release.* [Online]   Available at: https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2017/ [Accessed 18 JUNE 2018].

Collins, H. (2010). Creative research. Lausanne, Switzerland: AVA Pub. SA.

Collins Dictionary 2012, HarperCollins, London, viewed 15 June 2018, <http://www.collinsdictionary.com/>.

Cooley, T. M., 1879. *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract..* 2 ed. Chicago:: Callaghan.

Constitution of Ireland (1937) Available at:http://www.taoiseach.gov.ie/eng/Historical_Information/The_Constitution/February_2015_-_Constitution_of_Ireland_.pdf (Accessed 28 jume 2018).

Corbin, J. and Strauss, A. (1990). Grounded Theory Research: Procedures, Canons and Evaluative Criteria. *Zeitschrift für Soziologie*, [online] 19(6), pp.418-419. Available at: http://zfs-online.org/index.php/zfs/article/viewFile/2741/2278 [Accessed 3 Jun. 2018].

Council of Europe (1950) 'European Convention on Human Rights'. Available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed: 23 June 2018).

Cranor, L. F., Reagle, J. & Ackerman, M., 1990. *"Beyond Concern : Understanding Net Users Attitudes about Online Privacy,* s.l.: AT&T Labs Technical Reports.

Creswell, J. and Miller, D. (2000). Determining Validity in Qualitative Inquiry. *Theory Into Practice*, [online] 39(3), pp.124-130. Available at: https://people.ucsc.edu/~ktellez/Creswell_validity2000.pdf [Accessed 14 Jul. 2018].

Creswell, J. W. (2009) *Research design: qualitative, quantitative and mixed methods approaches*. 3rd Ed. London: Sage Publications.

Culnan, M. (1993) '"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use'. *MIS Quarterly*, Volume 17(3): 341-363.

Data Protection Acts 1988 and 2003. Available at: https://www.dataprotection.ie/docs/DATAPROTECTION-ACT-1988-REVISED-Updated-to-14-October-2014/1469.htm (Accessed 28July 2018).

Data Protection Commissioner (2013) 'Public awareness surveys'. Available at: https://www.dataprotection.ie/docs/Public-Awareness-Surveys/1287.htm (Accessed: 25 July 2018).

Dataprotection.ie. (2018). *A guide to your rights - Plain English Version - Data Protection Commission - Ireland*. [online] Available at: https://www.dataprotection.ie/docs/A-guide-to-your-rights-Plain-English-Version/r/858.htm [Accessed 24 Apr. 2018].

Dataprotection.ie. (2018a). *Legislative Frameworks Overview - Data Protection Commission - Ireland*. [online] Available at: https://www.dataprotection.ie/docs/legislation/k/1728.htm [Accessed 29 Jun. 2018].

Dataprotection.ie. (2018b). *Legislative Frameworks Overview - Data Protection Commission - Ireland*. [online] Available at: https://www.dataprotection.ie/docs/legislation/k/1728.htm [Accessed 29 Jun. 2018].

Dataprotection.ie. (2018c). *Training and Public Awareness - Data Protection Commission - Ireland*. [online] Available at: https://www.dataprotection.ie/docs/Training-and-Public-Awareness/b/805.htm [Accessed 29 Aug. 2018].

Davies, S. G., 1997. Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity,. In: . P. E. Agre & M. Rotenberg, eds. *Technology and Privacy: The New Landscape.* Cambridge,MA: MIT Press, pp. pp. 143-165.
.
Davinson, N., and E. Sillence. 2010. "It Won't Happen to Me: Promoting Secure Behaviour among Internet Users." *Computers in Human Behavior* 26 (6): 1739–1747.

Debasish, S.S. and Muralidhar, M., (2013). Print Advertising: Consumer Behaviour. *SCMS Journal of Indian Management,* 10(1), pp. 78-88

DMA (2018). *DATA PRIVACY: WHAT THE CONSUMER REALLY THINKS*. [online] Dma.org.uk. Available at: https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy---what-the-consumer-really-thinks-final_5a857c4fdf799.pdf [Accessed 29 Jul. 2018].

Dommeyer, C, & Cross, B .(2003).What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. , *Journal Of Interactive Marketing (John Wiley & Sons)*, 17, 2, pp. 34-51, Business Source Complete, EBSCO*host*, viewed 20 July 2018.

DeCew, J., 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, Ithaca.

DeCew, J. W., 2016. Privacy and Its Importance with Advancing Technology. *42 Ohio Northern University Law Review,* Issue 42, pp. 471-492.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2012) Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. European Journal of Information Systems, 22, 61-80.

Dwyer, C., Hiltz, S.R. & Passerini, K. (2007) 'Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace', Paper presented at the *Proceedings of the Thirteenth Americas Conference on Information Systems*. Colorado, August 09 – 12.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers.

Easterby-Smith, M., Thorpe, R. and Jackson, P. R. (2008) *Management Research*. 3rd ed. London: Sage Publications.

Eggers, W. and Campbell, R. (2006). *States of transition*. [Reston, Va.]: Deloitte.

Eggers, W., Hamill, R. and Ali, A. (2018). *Data as the new currency*. [online] Deloitte Insights. Available at: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html [Accessed 29 Jun. 2018].

E.M. Caudill, P.E. Murphy (2000), Consumer online privacy: Legal and ethical issues *Journal of Public Policy & Marketing*, 19(1) pp. 7-19

Equifax, 1996. *Equifax/Harris Consumer Privacy Survey,* s.l.: Equifax/Harris.

E. R. Foxman and P. Kilcoyne, "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issue," Journal of Public & Marketing, Vol. 12, No. 1, 1993, pp. 106-119.

European Communities (Electronic Communications Networks and Services (Privacy and Electronic Communications) Regulations 2011, SI 336 of 2011.

European   Commision,   n.d.   *What   is   personal   data?*.   [Online] Available   at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [Accessed 13 june 2018].

European Commission (2009) 'EU Charter of Fundamental Rights'. Available at: http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (Accessed: 27 july 2018).

European Commission (2016) 'Reform of EU data protection rules' Available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm (Accessed: 14 July 2018).

Feldman, A., 2000. Protecting Your Financial Privacy. *Money,* 29(6), pp. 161-164.

Feilzer, M. Y. (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research*, 4(1), pp.6-16.

Fereday, J. and Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal   of   Qualitative   Methods*,   [online]   5(1),   pp.80-92.   Available   at: http://journals.sagepub.com/doi/pdf/10.1177/160940690600500107 [Accessed 7 Jul. 2018].

Fischer, E., and Arnold, S. J., (2006) *Sex, gender identity, gender role attitudes, and*

consumer behavior. Psychology and Marketing **11**(2): 163-182.

FLEMING, J. and ADKINS, A. (2016). *Data Security: Not a Big Concern for Millennials*. [online] Gallup.com. Available at: https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx [Accessed 28 Jul. 2018].

Flick, U. (2011). *Introducing research methodology: A beginner's guide to doing a research project.* London: Sage.

Frand, J .(2006) . "The Information Mindset: Changes in Students and Implications for Higher Education ." *EDUCAUSE Review* 41 (March/April): 14–16

Friedman, B., Khan, P. & Howe, D. (2000) 'Trust Online'. *Communications of the ACM*, Volume 43(12): 34-40.

Gallup, I. (2015). *Millennials Most Trusting on Safety of Personal Information*. [online] Gallup.com. Available at: https://news.gallup.com/poll/183074/millennials-trusting-safety-personal-information.aspx [Accessed 25 Aug. 2018].

Gates, C. and Matthews, P. (2014). Data Is the New Currency. *Proceedings of the 2014 workshop on New Security Paradigms Workshop - NSPW '14*

Glesne, C., & Peshkin, P. (1992). *Becoming qualitative researches: An introduction.* New York, NY: Longman.

Gill, P., Stewart, K., Treasure, E. and Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, [online] 204(6), pp.291-295. Available at: https://s3.amazonaws.com/academia.edu.documents/42377023/Methods_of_data_collection_in_qualitativ20160208-31828 yh1vmq.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1534523501&Signature=q2XWOBUY5dwhs19yfJzUP9K3xJk%3D&response-content-disposition=inline%3B%20filename%3DMethods_of_data_collection_in_qualitativ.pdf [Accessed 5 Jun. 2018].

Giese, J. and . Cote, J. (2002). Defining Consumer Satisfaction. *Academy of Marketing Science Review*, [online] 2000(1). Available at: https://www.researchgate.net/profile/Joan_Giese/publication/235357014_Defining_Consumer_Satisfaction/links/5419a5790cf203f155ae0afb/Defining-Consumer-Satisfaction.pdf [Accessed 26 Jun. 2018].

Giulia, R., Newlands, E., Anselm, G., Andreotti, A., Eichhorn, T., Etter, M., Hoffmann, C., Jürss, S. and Lutz2, C. (2018). *Millennials and the Sharing Economy: European Perspectives*.

Goddard, W. & Melville, S. (2004). *Research Methodology: An Introduction*, (2nd ed.) Oxford: Blackwell Publishing.

Goodwin, C., 1991. Privacy: Recognition of a consumer right.. *Journal of Public Policy & Marketing,* 10(1), pp. 149-166.

Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing,* 10 (Spring), 149-66.

Goldkuhl, G. (2012). *Pragmatism vs interpretivism in qualitative information systems research*. [online] Available at: http://www.diva-portal.org/smash/get/diva2:515141/FULLTEXT01.pdf [Accessed 10 Jun. 2018].

Graziano, A. M. and Raulin, M. L. (2009) *Research methods: a process of inquiry*. 7th Edition. London: Pearson Education Inc.

Grehan, D. and Yamamoto, O. (2017). Relationship Between Millennials and Brand Loyalty: Mediating Brand Loyalty Factors. *Journal of Business Theory and Practice*, 5(3), p.223

Hazari, S. and Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, 9(4), pp.31-51.

H. Jeff Smith, T. D. H. X., December 2011. INFORMATION PRIVACY RESEARCH: AN INTERDISCIPLINARY REVIEW. *MIS Quarterly,* 35(4), pp. pp. 989-1015.

Howe , . N. & Strauss, . W., 2007. the next 20 years: how customer and workforce attitudes will evolve".. *Harvard Business Review,,* 85(8), p. pp. 41-52..

Hoepfl, M. C. (1997). Choosing qualitative research: A primer for technology education researchers. *Journal of Technology Education*, 9(1), 47-63. Retrieved February 25, 2018, from http://scholar.lib.vt.edu/ejournals/JTE/v9n1/pdf/hoepfl.pdf.

Hogg, M., & Vaughan, G. (2005). *Social Psychology (4th edition)*. London: Prentice-Hall.

Hsu, M.-H., and Chiu, C.-M., (2004) *Predicting electronic service continuance with a decomposed theory of planned behaviour*. Behaviour and Information Technology, 23, 359-373.

Huberman, M. and Miles, M. (2012). *Cram101 textbook outlines to accompany Qualitative data analysis*. [U.S.]: Content Technologies Inc., pp.59-64.

Itu.int. (2018). *ICT Facts and Figures 2017*. [online] Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx [Accessed 11 Jun. 2018].

Kaifi, B., Nafei, W., Khanfar, N. and Kaifi, M. (2012). A Multi-Generational Workforce: Managing and Understanding Millennials. *International Journal of Business and Management*, [online] 7(24). Available at: https://www.researchgate.net/publication/270955270_A_Multi-Generational_Workforce_Managing_and_Understanding_Millennials [Accessed 14 Jun. 2018].

Kantar TNS UK (2018). *GDPR Awareness Index | TNS UK*. [online] Tnsglobal.co.uk. Available at: https://www.tnsglobal.co.uk/GDPR [Accessed 18 Jun. 2018].

Kaplan, A. and Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, [online] 53(1), pp.59-68. Available at:

http://michaelhaenlein.com/Publications/Kaplan,%20Andreas%20-%20Users%20of%20the%20world,%20unite.pdf.

Katz, D. (1960). The functional approach to the study of attitudes. *Public Opinion Quarterly, 24,* 163-204

Kelley, P.G. et al., 2009. A "nutrition label" for privacy. Proceedings of the 5th Symposium on Usable Privacy and Security SOUPS 09, 1990, p.1. Available at: http://portal.acm.org/citation.cfm?doid=1572532.1572538

Kennedy vs Ireland [1987] IR 587

Kidder, L., Judd, C. and Smith, E. (1991). *Research methods in social relations*. Fort Worth, Tex.: Harcourt Brace Jovanovich College Publishers.

Kobsa , A., 2007. Privacy-enhanced personalization. *Communications of the ACM,,* 50(8), pp. 24-33.

Kothari, C. R. (2004). *Research methodology: methods and techniques*. New Delhi: New Age International.

LAROSE, R. and RIFON, N. (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs*, [online] 41(1), pp.127-149. Available at: https://pdfs.semanticscholar.org/9ce4/7bd1035080922713abf654e75adfd514547d.pdf.

Landsdowne Market Research, (2008). *"Public Awareness Survey 2008".* [online] Dataprotection.ie. Available at: https://www.dataprotection.ie/documents/press/Survey08.pdf [Accessed 28 Jul. 2018].

Lee, Y., & Kozar, K. (2005). Investigating factors affecting the anti-spyware system adoption. *Communications of the ACM, 48*(8), 72–77.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolff, S. (2003) *A Brief History of the Internet.* Internet Society.

Levine, S. (2011). Students still struggling with Internet privacy. Retrieved august 4, 2018, from *USA TODAY*: http://college.usatoday.com/2011/08/31/students-still-struggling-with-internet-privacy/

Levin, A. & Abril, P.S. (2009) 'Two Notions of Privacy'. *Vanderbilt Journal of Entertainment & Technology Law*, Volume (11): 1001-1051.

Lyons, S. & Schweitzer, L., 2012. *Managing the new workforce: International perspectives on the Millennial generation..* Cheltenham: Edward Elgar Publishing, Inc

MAXQDA - The Art of Data Analysis. (2018). *What is MAXQDA? - MAXQDA - The Art of Data Analysis*. [online] Available at: https://www.maxqda.com/what-is-maxqda [Accessed 29 Jun. 2018].

Malhotra, N., 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), pp.336-355

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

Margulis, S. T. 2003."On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues*(59:2), pp. 411-429.

Mann P.H. (1985) *Methods of Social Investigation.* Basil Blackwell, Oxford.

Mays N, Pope C. *Quality in qualitative health research.* In: Pope CP, Mays N, eds. Qualitative research in health care, 2nd edn. London: BMJ Books, 2000: 89–101.

McAfee, A., and Brynjolfsson, E. 2012. "Big Data: The Management Revolution." *Harvard Business Review* 90:60– 68.

McDonald, P. & Thompson , P., 2015. Social Media(tion) and the Reshaping of Public/Private Boundaries in Employment Relations. *International Journal Of Management Review*

McGee v Attorney General [1974] IR 284.

Meister, J. and Willyerd, K. (2010). SPOTLIGHT ON LEADERSHIP: THE NEXT GENERATION Mentoring Millennials. *Harvard Business Review*, [online] pp.1-4. Available at: https://www.harvardbusiness.org/sites/default/files/HBR_Mentoring_Millennials.pdf [Accessed 10 Jun. 2018].

Metzger, M.J., (2004) 'Privacy, Trust and Disclosure: Exploring Barriers to Electronic Commerce', *Journal of Computer-Mediated Communications*, Volume 9(4).

Michell, J. (2005). The Meaning of the Quantitative Imperative. *Theory & Psychology*, 15(2), pp.257-263.

Milne, George R., and Mary J. Culnan. 2004. Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing,* 18 (3): 15–29

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. Journal of Consumer Affairs, 43(3), 449-473.

Milne, G. R., A. J. Rohm. 2000. Consumer privacy and name removal across direct marketing channels: Exploring opt in and opt-out alternatives. *J. Public Policy Marketing* 19(2) 238-249.

 Mintel (2014). *Sixty percent of Millennials willing to share personal info with brands*. [online] Mintel. Available at: http://www.mintel.com/press-centre/social-and-lifestyle/millennials-share-personal-info [Accessed 29 Jul. 2018].

MIP. (2015). How Millennials get news.. Retrieved December 10, 2016, from *American Press Institute:* https://www.americanpressinstitute.org/publications/reports/survey-research/digital-lives-of-millennial

Mitchell, A. (2016). GDPR: Evolutionary or revolutionary? *Journal of Direct, Data and Digital Marketing Practice*, 17(4), pp.217-221.

Mittal, Vikas, Pankaj Kumar, and Michael Tsiros. 1999. "Attribute-Level Performance, Satisfaction, and Behavioral Intentions over Time: A Consumption-System Approach." *Journal of Marketing 63* (April): 88-101.

Miyazaki, A. D., A. Fernandez. 2000. Internet privacy and security: An examination of online retailer disclosures. */. Public Policy Marketing* 19(1) 54-61.

Monsuwe, T.P., Dellaert, B.G.C and De Ruyter, K., (2004) *What drives consumers to shop online*? A literature review. International Journal of Service Industry Management, 15, 102-121.

Moore, M. (2012). Interactive media usage among millennial consumers. *Journal of Consumer Marketing*, [online] 29(6), pp.436-444. Available at: https://www.researchgate.net/profile/Marguerite_Moore/publication/241946613_Interactive_media_usage_among_millennial_consumers/links/02e7e53371717aaae9000000/Interactive-media-usage-among-millennial-consumers.pdf [Accessed 10 Aug. 2018].

Moqbel, M., Bartelt, V., Al-Suqri, M. and Al-Maskari, A. (2017). Does privacy matter to millennials? The case for personal cloud. *Journal of Information Privacy and Security*, 13(1), pp.17-33.

Morgan D L. (1998) *The focus group guide book.* London: Sage Publications

M.Vaismoradi, J. Jones, H. Turunen, and S. Snelgrove, (2016)"Themedevelopment in qualitative content analysis and thematic analysis," *Journal of Nursing Education and Practice,* vol. 6, no. 5, article p100,.

Myerscough, S., Lowe, B. & Alpert, F., 2006. Willingness to provide personal information online: The role of perceived privacy risk, privacy statements and brand strength. *Journal of Website Promotion,* Volume 2, pp. 115-140.

National Cyber Security Alliance. 2012. NCSA / McAfee Online Safety Survey. Accessed October 12, 2013. http://staysafe online.org/stay-safe-online/resources/.

National Cyber Security Alliance. 2013. *Preparing Millennials to Lead in Cyberspace.* Accessed April 21, 2014. http://staysafeonline.org/ncsam/resources/

Newman, I. (1998). *Qualitative-quantitative research methodology: Exploring the interactive continuum.* Carbondale: Southern Illinois University Press.

Nimon, S. (2007). Generation Y and higher education: The *other* Y2K. *Journal of Institutional Research, 13 (1), 21-41.*

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

Nowak, Glen J. and Joseph Phelps (1995), "Direct Marketing and the Use of Individual-Level Consumer Information: Determining When 'Privacy' Matters," *Journal of Direct Marketing, 9* (Summer), 46-60.

Obal M. (2015) Generational Differences in Online Trust Development: Millennials V. Baby Boomers. In: Robinson, Jr. L. (eds) Marketing Dynamism & Sustainability: Things Change, Things Stay the Same…. Developments in Marketing Science: Proceedings of the Academy of Marketing Science. Springer, Cham

O'Brien, D. & Torres, A.M., (2012) 'Social Networking and Online Privacy: Facebook Users' Perceptions', *Irish Journal of Management*, Volume 31(2): 63-97.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of *Economic Psychology,* 25(2), 243–262

Palfrey, J., and U. Gasser. 2008. *Born Digital: Understanding the First Generation of Digital Natives*. New York: Basic Books.

Park, M., Jang, H., Lee, S. and Brayley, R. (2010) Tourism and the N Generation in a Dynamically Changing Society: The Case of South Korea. In: Benckendorff, P., Moscardo, G. and Pendergast, D., Eds., *Tourism and Generation Y*, CAB International, Cambridge, 85-97.

Patton, M. Q. (2002). *Qualitative evaluation and research methods* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA L. REV*. 1701 (2010);

Peifer, K. (2014). Personal privacy rights in the 21st century: logic and challenges. *Journal of Intellectual Property Law & Practice*, 9(3), pp.231-238.

Polit. D.F., Beck C.T. & Hungler. B.P. (2001) Essentials of Nursing Research: Methods, Appraisal and Utilization. 5th Edition, Lippincott. Williams &Wilkins, Philadelphia.

Phelps, J., Nowak, G. & Ferrell, E., 2000. Privacy concers and consumer willingness to provide personal informatiom. *Journal of Public Policy & Marketing,* 19(1), pp. 27-41.

Phoenix Strategic Perspectives Incorporated. (2013). *Survey of Canadians on privacy-related issues.*

Pitkänen, O. & Tuunainen, V.K. (2012) 'Disclosing Personal Data Socially - an Empirical Study on Facebook User's Privacy Awareness'. *Journal of Information Privacy & Security*, Volume 8(1): 3-29

Prensky, M . (2005) . *"Listen to the Natives* ." Educational Leadership 63 (4): 8–13.

Punch, K. (2006). *Review: Keith F. Punch (2005). Introduction to Social Research— Quantitative & Qualitative Approaches*.

Rainie, L., S. Kiesler, R. Kang, and M. Madden. 2013. *Anonymity, privacy, and security.*.http://www.pewinternet.org/2013/09/05/anonymity-privacy   -and-security-online/. (Accessed May 27, 2018)

Ranney, M., Meisel, Z., Choo, E., Garro, A., Sasson, C. and Morrow Guthrie, K. (2015). Interview-based Qualitative Research in Emergency Care Part II: Data Collection, Analysis and Results Reporting. *Academic Emergency Medicine*, 22(9), pp.1103-1112

Reed, A. (2013). *Study by the Center for the Digital Future shows that 'Millenials' care less about online privacy.* [online] Annenberg.usc.edu. Available at: https://annenberg.usc.edu/news/centers/study-center-digital-future-shows-millenials-care-less-about-online-privacy [Accessed 28 Jul. 2018].

Report from the EU H2020 Research Project Ps2Share: Participation, Privacy, and Power in the Sharing Economy. [online] pp.31-34. Available at: https://www.bi.edu/globalassets/forskning/nordic-centre-for-internet-and-society/focus-group-working-paper-final-version-for-web.pdf [Accessed 25 Jul. 2018].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union*, Vol. L119 (4 May 2016), pp. 1-88

Rice, P. L., & Ezzy, D. (1999). *Qualitative Research Methods: A Health Focus*. South Melbourne (Australia): Oxford University Pre

Richards, J., 1997. Legal Potholes on the Information Superhighway. *Journal of Public Policy and Marketing,* 15(2), pp. 319-326.

Ridley-Siegert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice*, 17(1), pp.30-35.

Rob Hamill and Abed Ali, 2013. Data as the new currency. *Deloitte Review,* Issue 13, pp. 19-31.

Robson, C. (2011) *Real world research: a resource for users of social research methods in applied settings*. 3rd Edition. Oxford: Wiley.

Rosenblum, D., 2007. 'What Anyone can Know: The Privacy Risks of Social Networking Sites',. *IEEE Security and Privacy,* Volume 5, p. pp. 40–49..

Ruane, L, Wallace, E. (2013) 'Generation Y females online: insights from brand narratives. Qualitative Market Research': *An International Journal*, 16(3): pp. 315-335.

Rygielski, C., Wang, J. and Yen, D. (2002). Data mining techniques for customer relationship management. *Technology in Society*, [online] 24(4), pp.483-502. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.474.2713&rep=rep1&type=pdf.

Salazar, M. and Woodward, B. (2017). WITH GREAT DATA, COMES GREAT RESPONSIBILITY: UNIVERSITY STUDENTS' PERCEPTIONS ON DATA PRIVACY. *Issues in Information Systems*, [online] 18,(1), pp.191-201. Available at: http://www.iacis.org/iis/2017/1_iis_2017_191-201.pdf [Accessed 20 Jun. 2018].

Sampler, J. L., 1998. Redefining industry structure for the information age. *Strategic Management Journal ,* Volume 19(4), pp. 343- 355.

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students, (6th ed.) London: Pearson

Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research methods for business students*.6th ed. England: Pearson Education Limited.

Silverman D.(2000) *Doing qualitative research.* London: Sage Publications

Smith, Amy K., Ruth N. Bolton, and Janet Wagner. 1999. "A Model of Customer Satisfaction with Service Encounters Involving Failure and Recovery." *Journal of Marketing Research* 36 (August): 356-372.

Smith, T. and Nicholas, T. (2015). Understanding the Millennial Generation. *Journal of Business Diversity*, [online] 15(1), pp.39-47. Available at: https://www.researchgate.net/profile/Tommy_Nichols/publication/324922926_Understanding_the_Millennial_Generation/links/5aeb549c0f7e9b01d3e052e8/Understanding-the-Millennial-Generation.pdf?origin=publication_detail [Accessed 15 Jun. 2018].

Solomon, M. Bamossy, G. Askegaard, S. and Hogg, M (2013). *Consumer Behaviour: A European Prespective*. 5th ed. Essex: Prentice-Hall

Spreng, Richard A., Scott B. MacKenzie, and Richard W. Olshavsky. 1996. "A Reexamination of the Determinants of Consumer Satisfaction." *Journal of Marketing* 60 (July): 15-32.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory proceduresand techniques*. Newbury Park, CA: Sage Publications, Inc.

Swire, P. P. and Ahmad, K. (2012) *Foundations of Information Privacy and Data Protections*, Portsmouth, NH: International Association of Privacy Professionals.

Tablante, M. (2013). How college students can maintain online privacy. Retrieved December 12, 2017, from *USA TODAY:* https://www.usatoday.com/story/tech/personal/2013/04/23/college-students-online-privacy-tips/2107313/ .

Tansey, O. (2007). Process Tracing and Elite Interviewing: A Case for Non-probability Sampling. *PS: Political Science & Politics*, [online] 40(04), pp.765-772. Available at: http://observatory-elites.org/wp-content/uploads/2012/06/tansey.pdf [Accessed 29 May 2018].

Taylor, A. (2012). The Information Search Behaviour of the Millennial Generation. *Ubiquitous Learning: An International Journal*, 4(3), pp.85-98.

Team, M. (2018). *Sixty percent of Millennials willing to share personal info with brands*. [online] Mintel. Available at: http://www.mintel.com/press-centre/social-and-lifestyle/millennials-share-personal-info [Accessed 25 Jun. 2018].

Timm, D. M., & Duven, C. J. (2008). Privacy and Social Networking Sites. *New Directions for Student Services 124*, 89-102. Retrieved from http://ryanpstone.com/yahoo_site_admin/assets/doc s/socialnetwork1.250104344.pdf

Tuckett, A. G. (2005). Applying thematic analysis theory to practice: A researcher's experience. *Contemporary Nurse, 19*(1-2), 75-87.

Ward, K., Legard, R. and Keegan, J. (2003). IN DEPTH INTERVIEWS. In: J. RITCHIE and J. LEWIS, ed., *QUALITATIVE RESEARCH PRACTICE A Guide for Social Science Students and Researchers*, 1st ed. [online] SAGE Publications Ltd, pp.138-140. Available at: https://mthoyibi.files.wordpress.com/2011/10/qualitative-research-practice_a-guide-for-social-science-students-and-researchers_jane-ritchie-and-jane-lewis-eds_20031.pdf [Accessed 17 Aug. 2018].

Ward, S., Bridges, K. and Chitty, B. (2005). Do Incentives Matter? An Examination of On-line Privacy Concerns and Willingness to Provide Personal and Financial Information. *Journal of Marketing Communications*, 11(1), pp.21-40.

Warren, S., Brandeis, L.D., (1890) . The right to privacy. *Harvard Law Review*, 5. Available online at ⟨http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html⟩ (accessed on 20 June 2018).

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

Wiles, R., Crow, G., & Pain, H. (2011). Innovation in qualitative research methods: a narrative review. *Qualitative Research, 11*(5), pp.587-604.

Williams , K. C. & Page , R. A., 2011. Marketing to the Generations. *Journal of Behavioral Studies in Business.*

Winter, G. (2000). A comparative discussion of the notion of validity in qualitative and quantitative research. *The Qualitative Report*, *4*(3&4). Retrieved June 5, 201 8, from http://www.nova.edu/ssss/QR/QR4-3/winter.html

Wood, L. M. (2004). Dimensions of brand purchasing behavior: Consumers in the 18-24 age group. *Journal of Consumer Behavior,* 4(1), 9-24.

Xu, H., Dinev, T., Smith, J. & Hart, P. (2011) 'Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances'. *Journal of the Association for Information Systems*, Volume 12(12): 798-824.

Van Teijlingen, E. and Hundley, V. (2002). The importance of pilot studies. *Nursing Standard*, 16(40), pp.33-36.

Vollmer, N. (2018). *Recital 30 EU General Data Protection Regulation (EU-GDPR). Privacy/Privazy according to plan.*. [online] Privacy-regulation.eu. Available at: http://www.privacy-regulation.eu/en/recital-30-GDPR.htm [Accessed 29 Jul. 2018].

Yang, B., and Lester, D., (2004) Attitudes toward buying online. *Cyber Psychology and Behavior,* 7, 85–91.

YOUN, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, 43(3), pp.389-418.

Zimmer, X.J., Arsal, R.E., Al-Marzouq, M. & Grover, V. (2010) 'Investigating Online Information Disclosure: Effects of Information Relevance, Trust and Risk'. *Information and Management*, Volume 47(2): 115-123.

Appendix

Appendix 1

Interview Consent Form:

This form was provided to the participants on the face to face interview.

Through this form I understand the elements involved to take part in the research.

I have voluntarily taken part in this research and have been briefed about its purpose and objectives.

I understand that my identity will be anonymized and no identifiers that related to me shall be present in the research

I understand and agree that my interviews will be recorded for research purposes only and will be deleted after the study is completed.

I can refuse to answer certain questions if I find it unsuitable.

I hereby consent to participate in this study

Appendix 2

Interview Questions

What do you know about privacy on the internet?

DO you know your personal data is collected on the internet and how it is collected?

Are you worried or concerned about your data privacy online?

Are you afraid of someone stealing your financial information on the internet?

Do you fully understand how to protect your data on the internet?

Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc?

What are your views on a company holding your personal data?

Are you aware of how your data can be used to a company's advantage?

Are you aware of the legal avenues open to you, to protect your data?

What do you know about the GDPR and the Data protection Act, 2018?

What do you prefer – permitting access to your data, if it makes a transaction easier or not permitting access, despite the ease involved?

Where does your awareness of data protection and privacy on the internet stem from?

Are you partial about which websites you disclose your data to ?

Who do you think should bring about awareness of data privacy and protection?

Do you personally take steps to educate yourself on these matters?

How do you suggest is the most effective way to create awareness of data protection and privacy?

Appendix 3

INTERVIEW 1:

Age :26

Occupation: working for a company as data administrator

Education: Masters

What do you know about privacy on the internet?

Privacy on the internet is an illusion. Private data is being publicly used by companies to create profiles of end users.

DO you know your personal data is collected on the internet and how it is collected?

Yes I am aware that my data is collected on the internet. I know that it is collected by pretty much all the services and applications I use. But too sure about how.

Are you worried or concerned about your data privacy online?

I am worried about my privacy online, the other day I was looking at my timeline on google maps and I was surprised to see the amount of data that was collected by google maps alone. Its almost creepy for them to know all the places I have been to and exactly how long I spent in all of these places.

Are you afraid of someone stealing your financial information on the internet?

Not always I am not worried about this, as that would entail hacking into my browser/system and stealing my card details, which is very difficult, also I keep monitoring my bank account to check for any suspicious activity.

Do you fully understand how to protect your data on the internet?

I am a software engineer, so I know exactly how to go anonymous on the internet, but it's very tedious to do that also all the information gathered on the internet also has its advantages.

Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc? do you indulge in risky behaviours online?

" I am cautious about what I reveal on the internet and i have set difficult passcodes for most of my online presence What are your views on a company holding your personal data?

Depends on the Company I am giving my data to, for example I know for a fact that google collects a lot of data on me, I wouldn't be comfortable with smaller

companies that I am unaware of to collect that amount of data.

Are you aware of how your data can be used to a company's advantage?

Kind of, not in detail though.

Are you aware of the legal avenues open to you, to protect your data?

NO

What do you know about the GDPR and the Data Protection Act, 2018?

I recently learned about GDPR and that all companies collecting data will not have
to mandatorily provide justification as to why they collect that data that they do
and should also be have provisions in place to delete a user's data if requested by a
user. I do know that the I have some rights, not in detail though

What do you prefer – permitting access to your data, if it makes a transaction easier or not
permitting access, despite the ease involved?

I recently learned about GDPR and that all companies collecting data will not have
to mandatorily provide justification as to why they collect that data that they do
and should also be have provisions in place to delete a user's data if requested by a
user..

Are you willing to compromised privacy for benefits?

Yes, it's inevitable anyway. I mean as long as I am not harmed. I don't like compromising
financial information but it's inevitable. initially I was uncomfortable with sharing my card
and home details with apps like my taxi but I later learnt my friends would get amazing deals,
so I gave in as it's an app everyone uses

Where does your awareness of data protection and privacy on the internet stem from?

I know about the GDPR due to seminars and policy changes at work

Are you partial about which websites you disclose your data to ?

Yes I am very partial, I would not be comfortable giving access to my private
information to an unknown service.

Who do you think should bring about awareness of data privacy and protection?

I don't think its right for end users to decide this, because they would just want to
use a service so no they just accept terms and agreements to use services, I feel
government bodies must keep such big organizations in check so they don't misuse
the data they collect.

Do you personally take steps to educate yourself on these matters?

I read article if I come across but not in depth and not voluntarily

How do you suggest is the most effective way to create awareness of data protection and privacy?

By bodies who create this regulation.

INTERVIEW 2

Age: 22

Occupation: childcare worker

Education: Bachelor's degree

(s)What do you know about privacy on the internet?

(p) Not much, just that we should be careful

(s)DO you know your personal data is collected on the internet and how it is collected ?

(p) Yes, I know data is collected not too sure how its collected or used

(s)Are you worried or concerned about your data privacy online?

(p)Often when I browse products on the internet, however random, I still end up receiving advertisements for them on social media/ random unrelated webpages and this makes me concerned about someone monitoring my behaviour online.

(s)Are you afraid of someone stealing your financial information on the internet?

(p) I am kind of cautious about my financial movement online and don't log in using wifi but use my personal network for financial transactions

S) Do you fully understand how to protect your data on the internet?

p) not really, it sounds complex

(s) Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc? do you have any risky behaviours?

(p) No. I do sometimes auto save passwords without checking secure sites

(s)What are your views on a company holding your personal data?

I'm ok as long as no risk. But not financial data.

(s)Are you aware of how your data can be used to a company's advantage?

(p) all I know about data being used is for mainly marketing purposes, like on instagram or facebook

s) Are you aware of the legal avenues open to you, to protect your data?

p) No

s) What do you know about the GDPR and the Data protection Act, 2018?

(p)Sure, I do know what GDPR is, it's that European regulation that is related to our privacyI had no clue that there were rights! Sure, I know someone cannot touch or miss use your data, but I didn't know these were like actual rights.

s) What do you prefer – permitting access to your data, if it makes a transaction easier or not permitting access, despite the ease involved?

p) Yes, as long as no risk to me. Not bank details but face book log in.

s) Are you willing to compromise privacy for benefits

p) yes, as long as no issue for me. due to financial constraints, I use subsidized versions of software online, in exchange for personal information

s)Where does your awareness of data protection and privacy on the internet stem from

p) work

s)Are you partial about which websites you disclose your data to ?

p) Well known websites like Facebook, Ryanair, Skyscanner etc, I trust and save my online details. If I use a website regularly, if its reputed I would trust and save details/ disclose or else no.

s)Who do you think should bring about awareness of data privacy and protection ?

(p)Governments bring these rules, so they must make sure we know

s)Do you personally take steps to educate yourself on these matters?

(p)ah it's a hot topic now isn't it, but I honestly wasn't bothered to figure what the fuss was about

s)How do you suggest is the most effective way to create awareness of data protection and privacy?

p) Creative way like adds, posters and videos so that its easily understandable.

Interview 3

Age :20

Education level :leaving cert

Occupation : student

What do you know about privacy on the internet?

Not too much, but I know privacy is kind of non-existent

DO you know your personal data is collected on the internet and how it is collected?

I often hear about how companies collect our data to sell it but I have no clue what happens to it

Are you worried or concerned about your data privacy online?

Yes, very .I often feel that someone might steal my information online, i am also concerned that even simple data about me, can be used for a malicious purpose against me.

Are you afraid of someone stealing your financial information on the internet?

Yes

Do you fully understand how to protect your data on the internet?

No

Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc? do you have any risky behaviours online?

No. I use a fair bit of online site to upload and edit my photographs and while I do this via a secure account, I've never thought of it until the site began to suggest names for my albums, based on my location. I often become scared about this behaviour online but I eventually get out of that zone and forget it"

What are your views on a company holding your personal data?

Dislike it, and makes me feel uncomfortable

Are you aware of how your data can be used to a company's advantage?

Very little

Are you aware of the legal avenues open to you, to protect your data?

Nope.

What do you know about the GDPR and the Data Protection Act, 2018?

I noticed most sites had begun to ask consent and though I didn't read it in detail, I saw something about GDPR".

What do you prefer – permitting access to your data, if it makes a transaction easier or not permitting access, despite the ease involved?

Yes, first one

Are you willing to compromise your information for benefits?

 I often sign up on random pages, for freebies"

Where does your awareness of data protection and privacy on the internet stem from?

Conspiracy theories

Are you partial about which websites you disclose your data to ?

Yes, only ones I trust

Who do you think should bring about awareness of data privacy and protection?

Government and companies

Do you personally take steps to educate yourself on these matters?

Nope

How do you suggest is the most effective way to create awareness of data protection and privacy?

The companies should have a smaller version of readable agreement to agree to along with long ones like a summary. Maybe some music videos as well.

Interview 4

Age : 25

Education: Masters

occupation: engineer

What do you know about privacy on the internet?

Privacy on the internet can be really difficult to accomplish. Most of the websites and apps we use, do track the users or collect user's information to sell it to advertisers.

DO you know your personal data is collected on the internet and how it is collected?

Yes, I do. Mostly cookies and take data on like getting access to location, contact list and file explorer

Are you worried or concerned about your data privacy online?

Yes, when the Facebook scandal came to light, my concern for what was happening with my data also increased. Sure I was concerned before, but it wasn't anything major until this incident

Are you afraid of someone stealing your financial information on the internet?

Yes, dont give my credit card details online unless it is absolutely necessary

Do you fully understand how to protect your data on the internet?

Mostly

Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc? Do you have risky behaviours?

Yes . I don't often change passcodes often and log in to no secure sites as well

What are your views on a company holding your personal data?

I'm ok along as I am not in danger. Also, I'm concerned if my data is safe

Are you aware of how your data can be used to a company's advantage?

By tracking my behaviour and what kind of things interests me and advertise me with those things. And the company will tailor make products for my likings.

Are you aware of the legal avenues open to you, to protect your data?

I know just that we can do something if we are harassed online

What do you know about the GDPR and the Data Protection Act, 2018?

GDPR is great news for the people of Europe as this is a first step to keep the data

of European safe..

What do you prefer – permitting access to your data, if it makes a transaction easier or not permitting access, despite the ease involved?

The former, for convenience. I would prefer the company telling me what data they hold when I log in into their account.

Are you willing to compromise your information for benefits ?

Most clubs often have this scheme where if you sign up on their webpage or like

their page on social media and like share you pics there with a tagged location, you get free drinks" most companies have this offer – they get you to create an online account and they offer you discount, I've done that loads of times for the crazy insider online sales"

 Where does your awareness of data protection and privacy on the internet stem from

work

Are you partial about which websites you disclose your data to ?

Yes like google

Who do you think should bring about awareness of data privacy and protection ?

Companies

Do you personally take steps to educate yourself on these matters?

Sometimes read blogs but not too often

How do you suggest is the most effective way to create awareness of data protection and privacy?

All companies have a portal where the user can see what information is beings shared online and editing that section of sharing information.

Interview 5

Age: 21

Ed: leaving cert

Occupation: Window Cleaning

What do you know about privacy on the internet?

There's more to it than we know!

DO you know your personal data is collected on the internet and how it is collected?

Yes, through monitored data online

Are you worried or concerned about your data privacy online?

Yes

Are you afraid of someone stealing your financial information on the internet?

Yes

Do you fully understand how to protect your data on the internet?

Not sure I fully understand

Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc? do you indulge in risky behaviour?

Sometime, but not frequently. Yes, I do some negligent behaviours like keeping my hotspot on without password. Also "I constantly check in on various applications, upload my location and review places- it's how my gang moves"

What are your views on a company holding your personal data?

Depends on whether they have my consent. Are you aware of how your data can be used to a company's advantage?

Not really!

Are you aware of the legal avenues open to you, to protect your data?

Not really!

What do you know about the GDPR and the Data protection Act, 2018?

I think it has something to do with the stuff we post online

What do you prefer – permitting access to your data, if it makes a transaction easier or not permitting access, despite the ease involved?

I'd prefer the latter but usually go with the former

Where does your awareness of data protection and privacy on the internet stem from

Thanks to the different stories on identity theft and cybercrime we hear on the

news.

Are you willing to compromise security for benefits?

Sometimes, not always, especially if my data is personal or financial. for example I absolutely hate saving credit cards but I don't want to buy things vis the guest user option as most companies process these orders slower than member and like millions use this site to shop and their information is intact right"

Are you partial about which websites you disclose your data to ?

Yes

Who do you think should bring about awareness of data privacy and protection?

Government and companies. I mean I can hardly understand the law words, so its government's job to inform us

Do you personally take steps to educate yourself on these matters?

I do try

How do you suggest is the most effective way to create awareness of data protection and privacy?

By using popular social media platforms to spread awareness.

Interview 6

Age:24

Education: Masters

Occupation student

What do you know about privacy on the internet?

Privacy is often compromised.

DO you know your personal data is collected on the internet and how it is collected ?

Yes, I guess cookies

Are you worried or concerned about your data privacy online?

Yes

Are you afraid of someone stealing your financial information on the internet?

Yes

Do you fully understand how to protect your data on the internet?

No

Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc? do you indulge in risky behaviours online?

No. I don't keep complex passcodes or secure my data via security questions

What are your views on a company holding your personal data?

I don't mind organisations holding my data as long as it is helpful for me

Are you aware of how your data can be used to a company's advantage?

For ads

Are you aware of the legal avenues open to you, to protect your data?

No

What do you know about the GDPR and the Data protection Act, 2018?

Speaks of some rights not sure what

What do you prefer – permitting access to your data, if it makes a transaction easier or not permitting access, despite the ease involved?

Permitting- I've saved loads of personal information on webpages due to the ease online of accessing it". Most companies have this offer – they get you to create an online account and they offer you discount

Are you willing to compromise privacy for benefits?

Yes, as long as my data is secure

Where does your awareness of data protection and privacy on the internet stem from?

I've come across a few articles on the net and heard a lecturer mention it. I'd probably say that my knowledge level is minimal, however I do attempt to educated myself, but it isn't an active choice

you partial about which websites you disclose your data to?

yes

Who do you think should bring about awareness of data privacy and protection?

Governing and regulatory bodies

Do you personally take steps to educate yourself on these matters?

Not much

How do you suggest is the most effective way to create awareness of data protection and privacy?

Advertisements, workshops and campaigns. (Similar to the ones from RSA)

Participant 7

Age: 24

Education: Masters

Occupation: works for Aws

What do you know about privacy on the internet?

There is no privacy on the internet. Everything is tracked.

DO you know your personal data is collected on the internet and how it is collected?

YES, through sign up pages . however, the deep end of the technology I don't know too much as I am into programming

Are you worried or concerned about your data privacy online?

yes

Are you afraid of someone stealing your financial information on the internet?

Yes

Do you fully understand how to protect your data on the internet?

To an extent as I am an engineer but not fully

Do you engage in security enhancing behaviours on the internet like changing passcodes often/ updating security information etc? Do you indulge in risky behviours online

Yes, well I try. Not always though. Sometimes especially with satnav and maps

What are your views on a company holding your personal data?

all of our information is already on the internet. Only thing to remember is what sort of personal data is with whom.

Are you aware of how your data can be used to a company's advantage?

Yes, but I don't understand tech behind it in detail

Are you aware of the legal avenues open to you, to protect your data?

Not in detail

What do you know about the GDPR and the Data Protection Act, 2018?

Kind of, I usually google if I'm in doubt, so I don't exactly know. I do know its for data protection in Europe.

What do you prefer – permitting access to your data, if it makes a transaction easier or not permitting access, despite the ease involved?

When transactions are concerned, there are some sites that have strict regulations

in place. Such as Netflix or Spotify. So, these companies would need your personal

data as a part of your activity. If not permitting access is something that the

individual is considering, then he/she has to minimize the digital activities. And

these days the digital activities are hard to minimize.

Are you willing to compromise privacy for benefit?

Yes, as long as I am not exposed to data theft

Where does your awareness of data protection and privacy on the internet stem from?

Work mostly

Are you partial about which websites you disclose your data to ?

Yes, only secure trusted ones

Who do you think should bring about awareness of data privacy and protection?

Governments, companies, colleges

Do you personally take steps to educate yourself on these matters?

Sometimes not voluntarily though

How do you suggest is the most effective way to create awareness of data protection and privacy?

Before providing any information, there has to be a message, clearly indicating how the data is going to be used and for how long. In colleges, it has to be made must for each student to know what's the internet like with your personal data. In working environments, there has to be the same level of practice, and also how the company is making use of your personal data.