



A descriptive study from the perspective of employees working in the Ecommerce sector in Ireland into their use of the social networking site LinkedIn and its privacy concerns both online and in the workplace.

Master of Arts in Human Resource Management

National College of Ireland

Elaine Byrne

Submitted to the National College of Ireland, August 2021

Submission of Dissertation Declaration Form

National College of Ireland Research Students Declaration Form

Name: Elaine Byrne

Student Number: x19242336

Degree for which thesis is submitted: Master of Arts in Human Resource Management

Title of Thesis: A descriptive study from the perspective of employees working in the Ecommerce sector in Ireland into their use of the social networking site LinkedIn and its privacy concerns both online and in the workplace.

Date: 18/08/2021

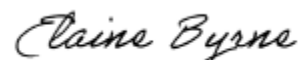
Material submitted for award

- A. I declare that this work submitted has been composed by myself.

- B. I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged.

- C. I agree to my thesis being deposited in the NCI Library online open access repository NORMA.

- D. I declare that no material contained in the thesis has been used in any other submission for an academic award.



(Signature of Research Student)

Abstract

The way in which technology has evolved in the past thirty years is staggering, and with it has brought new advancements in social networking sites online. The rapid growth of these sites, particularly LinkedIn, has had many advantages such as providing access to a wider network of potential employers, however the speed at which these sites are evolving is also causing problems. There are a multitude of dangers associated with sharing information online, most of which users are not made aware of when using the sites. This descriptive study aims to examine the behaviour of LinkedIn users online, particularly those working in the Ecommerce industry to find if they have an increased knowledge of how data is collected and used online from their daily interactions with data breaches.

Drawing on theoretical concepts found in current literature, the researcher used a survey as the quantitative research method chosen to collect the data. The survey was sent to employees working for the online retailer Wayfair located in Galway, Ireland and a total of 100 responses were collected. This data was then inputted into Statistical Package for the Social Sciences (SPSS) where a test was ran to validate the data. The results were then analyzed against the current literature surrounding the topic. The study was limited to employees working for one online retailer based in Ireland. To ensure there was no issue with the survey, a pilot test was conducted with ten participants prior to being sent to all Galway/Irish based employees.

The results of this study found that while employees working in the Ecommerce sector felt they had more awareness about their security online, the majority of respondents still do not know how their data is being used online and continue to share a lot of personal information online. Further research should focus more on why users are not more vigilant on protecting their data, and why privacy policies are not easier to read and understand.

TABLE OF CONTENTS	4
ABSTRACT	3
Chapter 1 : INTRODUCTION	6
1.1 Introduction	6
1.2 Background to Research	6
1.3 Purpose of the Research	7
Chapter 2 : LITERATURE REVIEW	9
2.1 Introduction	9
2.2 Privacy Online	9
2.3 GDPR	12
2.4 Cookies	13
2.5 Privacy Policy	14
2.6 Ecommerce Setting	14
2.7 Trust on LinkedIn	15
2.8 Privacy Concerns for Employees Online	16
2.9 Workplace Surveillance	18
2.10 Conclusion	19
Chapter 3: METHODOLOGY	20
3.1 Introduction	20
3.2 Research Question and Objectives	20
3.3 Research Philosophy	21
3.3.1 Positivism	21
3.3.2 Interpretivism	22
3.3.3 Pragmatism	22
3.3.4 Realism	22
3.4 Research Design	23
3.5 Data Collection Method	24
3.6 Data Analysis	25
3.7 Research Participants and Participants' Demographics	26
3.8 Sample Size	26
3.9 Pilot Test	27
3.10 Ethical Considerations	28
3.11 Limitations and Limiting Bias	28

Chapter 4 : FINDINGS AND ANALYSIS	30
4.1 Introduction	30
4.2 Reliability Test	30
4.3 Findings	31
Chapter 5 : DISCUSSION	44
5.1 Introduction	44
5.2 Ecommerce Setting	44
5.3 Privacy Online	45
5.4 Workplace Surveillance	46
5.5 Implications of the Research	47
5.6 Limitations of the Research	48
5.7 Future Research	50
5.8 Recommendations	52
5.9 Personal Learning Reflection	53
Chapter 6 : CONCLUSION	54
6.1 Introduction	54
REFERENCES	56
APPENDICES	69
Appendix A: Consent form	69
Appendix B: Online Questionnaire	70
Appendix C: Questionnaire Results	74

Chapter 1: Introduction

1.1 Introduction

Social media is a phenomenon that has become embedded into our daily lives both personally and professionally in the last twenty years. In 2020, there were over 3.6 billion social media accounts active worldwide with this figure projected to reach 4.1 billion by 2025 (Statistica, 2020). In comparison to traditional media outlets, social media is always on, 24/7 and can be accessed at any time, in any part of the world. Its use has quickly spread across all organisations and in all industries through its easily accessible and user-friendly technology which can quickly reach a wide audience (Bernoff and Schadler, 2010). People are the most valuable tool in any workplace, and because of this there is a huge focus for Human Resources on the recruitment of the right talent for the role (Taylor, 2014). With this in mind, it is no surprise that the social media phenomenon has made its way into the workplace through the online professional networking site LinkedIn. 81% of medium-sized organisations in Ireland advised in the year 2019 that they used LinkedIn in the workplace for recruiting new employees (Statista, 2021). The purpose of LinkedIn is to find and connect with professionals you know and trust in the business world (Cox, Li, and Wang, 2018). Through LinkedIn, employees can showcase their various skills and experience in order to advertise themselves to potential employers. In today's world, the days of looking through newspapers or searching job boards are long gone, and this process has almost completely moved online. The outbreak of the COVID19 pandemic has also led to a huge increase in the use of LinkedIn with a threefold increase in profits at the Irish branch of LinkedIn (RTE, 2021). The use of LinkedIn for recruiting purposes cannot be paralleled with any other method of traditional job searching as it is more versatile, easier to access and both individuals and businesses can advertise themselves and showcase their skills to a widespread audience based anywhere in the world.

1.2 Background to the Study

In this new digitalised society, people are more willing to share their personal data and information in order to enjoy the convenience of these online accounts (Jozani, *et al.* 2020). Individuals have a need to self-disclose, especially to solicit social interactions and

relationships and this need is constantly being fulfilled through social media posts. Such an increase in personal data being shared online however can lead to many security concerns and an increased risk of privacy violations. Privacy can be defined as a situation based, multidimensional and complex concept that changes and evolves with technology (Acquisti, Brandimarte and Loewenstein, 2015).

There is also the concern for how protected the employees are from their employer, when using LinkedIn in the workplace. LinkedIn is seen as a common workplace tool rather than a Social Networking Site (SNS), especially for those working in Human Resources or recruiting positions. This is where the lines can become blurred between LinkedIn as a professional tool for recruiting new employees, and the function of LinkedIn for the employee as a means of them personally using the site to showcase their skills and search for new employment. Workplace surveillance is a topical subject and one which is only heightened when moved to an online setting. The advancements in technology have also enhanced the ability to monitor employees through tracking software which oversee websites accessed by employees and cameras which in turn, monitor when employees are at or away from their desk. While the social media giant LinkedIn is a professional site, it too can lead to employer surveillance through the employee's actions online. Tensions can arise when competitive information is liked or favoured by an employee, which can be seen by colleagues, competitors, and management (Quinton and Wilson, 2016). There are countless studies available on the advantages of LinkedIn (Bohmova, 2016) (Constantinou, Melanthiou and Pavlou, 2015) (Eddy, 2012) and on the privacy concerns it raises (Chang, Lin, and Liu, 2015) (Koohang, 2017) however, little has been done to find the employee's mindset in relation to the privacy concerns of the social media giant LinkedIn.

1.3 Purpose of the Research

Since its creation in 2002, LinkedIn has undoubtedly had a considerable influence on recruitment in the Ecommerce sector in Ireland. With the Ecommerce setting, privacy is a major concern and there is little to no research available on the thoughts of employees in this sector, and how they use LinkedIn. In the current climate with all transactions having moved online due to the

COVID19 pandemic, the transfer of personal data to an organisation is not given a second thought when consumers are carrying out transactions. A study by PayPal in 2020 printed in the Irish Times (O'Brien, 2021) found that 79% of Irish consumers switched to shopping online during the COVID19 pandemic, and 33% of those advised they would continue to shop online after the pandemic. However the question could be asked are the employees themselves as concerned with protecting their own privacy online, as they are with protecting the privacy of their customers. The objective of this research paper is to investigate the employee's perspective on the use of LinkedIn in the workplace, and the privacy concerns it raises. Through a quantitative questionnaire, the study aims to investigate exactly how much data employees share with the online world and the trust they have in LinkedIn, and how aware they are of how their personal data is being used. The study will focus on a large Ecommerce company based in Galway, Ireland. Considering the current literature available on the topic which will be discussed in the following chapter, the Literature Review, there are three main areas this study will focus on.

1. Online Privacy and General Data Protection Regulation (GDPR) - How much data do employees share on LinkedIn and are they aware of how their data is being used?
2. Workplace Surveillance - Do employers have the right to monitor their employees personal LinkedIn account? Does this lead to a change in treatment of the employee?
3. Are privacy concerns heightened within the Ecommerce setting?

Chapter 2: Literature Review

2.1 Introduction

The concept of privacy can be found in literature as far back as Aristotle's works on politics and in the 1600s through the works of John Locke on privacy and public property. Westin (1967) coined the term privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated". Cappel, Shah and Verhulsdonck (2020) expanded on this definition stating that privacy included the right for individuals to be left alone and for everyone to have the right to control their own information. Altman (1978) suggested that privacy incorporates social and interpersonal aspects and varies depending on the individual's life experience. Many scholars have agreed that privacy is necessary to develop individuals to support society, foster different relationships and intimacy and to create a sense of autonomy (Allen 1988; Acquisti, Brandimarte and Loewenstein 2015; Sanders 2019; Mohamed 2010; Krämer and Schäwel 2020). Today, privacy concerns are heightened given the world of technology and social media, especially for employees in the workplace. O'Brien & Torres (2012) stated that an individual's privacy has been violated once they lose control of their personal data on SNS. This chapter will explore the key concepts of privacy online including GDPR, cookies, privacy policies, privacy concerns for employees online and employee surveillance.

2.2 Privacy Online

Privacy is a two-dimensional construct that deals with both control over information, and information use (Fox and Royne, 2018). Control over information becomes less possible in an online setting as this relinquishes the degree of control an individual has over one's information and can result in privacy compromising behaviour (Martin 2020). Information use or disclosure is described by Dhir. et al. (2021) as the critical point where privacy can become compromised. In both dimensions of privacy, any disclosure of information is considered privacy compromising behaviour and results in the user relinquishing control over their own privacy (Gabisch and Milne, 2014). Quan-Haase and Young (2013) stated that privacy concern online is an ethical issue as these online corporations rely on the collection and storage of users'

information for their databases. Adhikari and Panda (2018) defined user information privacy concerns as the ability of the individual to control how much of their personal information is collected and used by organisations online. With SNS such as LinkedIn, users willingly share vast amounts of personal identifiable features (Mohamed, 2010) such as profile picture, home addresses, previous places of work and education details. This open disclosure of personal information online can lead to an increased exposure to privacy risks for social media users online (Squicciarini, Xu and Zhang, 2011).

One major contributor to the literature on privacy in the new technological society is Shoshana Zuboff, who has spent years researching the topic and developing new ideas surrounding this. The most famous of her works, *The Age of Surveillance Capitalism* (2019) discusses how multinational corporations such as Facebook and Google persuaded us to give up our privacy in exchange for convenience. Zuboff (1988) stated before the emergence of technology and the internet as it is today, that all objects, events and exchanges would be translated to data and this in turn would be used for control and surveillance of individuals. Zuboff (2019) defines Surveillance Capitalism as the economic system which utilises personal data for profitable gain. Orange (2019) expanded on this definition stating that these large organisations use the personal data that individuals input into their systems to better understand the consumers behavioural features. Breckenridge (2020) details Zuboffs take on the way in which consumers have willingly given up their personal data to Google, Facebook, Amazon and other such organisations, either due to the fact that they view the convenience of the site as more important than protecting their data, or they fail to understand the purposefully complex and confusing language used in the privacy policy. Zuboff's work has been criticised for her attitude towards capitalism. Kapczynski (2020) stated that due to this fixation with capitalism, larger and arguably more important problems are left out of works, such as private power and how digital technology has affected labour in this information age.

The difference between a consumer's stated privacy preference and the amount of data they actually disclose has also been referred to as a privacy paradox (Martin 2020). While consumers value their privacy, they weigh up the risks of disclosing this information with the perceived benefits and continue to engage with these SNS. Kokolakis (2017) stated that the continued

proof of this privacy paradox and consumers' willingness to share their data, has led to the increase of firms collecting and using personal information. With a view to gain better understanding of the privacy paradox, Dinev and Hart (2006) created the privacy calculus theory which described this privacy calculus in which consumers weigh up the benefits of using SNS, against the risks such as a privacy breach with the results determined by the outcome of this trade off. Mahmoodi *et al.* (2018) expanded on this calculus theory stating that in this theory there was no paradox and the rewards came from self-disclosure however were still considered valid enough to take the privacy risk.

Fox and Royne (2018) discuss the lack of knowledge consumers have on how information such as their name, age and date of birth is used on the various social networking platforms which is concerning as these sites not only capture this data for their own use, but also to sell to other third parties. Kim and Kim (2011) explored the extent to which individuals believe they can control their privacy online by studying the relationship between consumer trust and the use of a third-party privacy seal. Tucker (2014) took a similar approach to investigate this relationship consumers have with privacy online through a study of Facebook's privacy policy. This study investigated how consumers' perception of their own personal privacy affected the likelihood of them sharing information and protecting their own data on SNS. Bornschein, Maier and Schmidt (2020) found that if consumers are aware of how their data is being used, or if they receive the policy warning on site, they may perceive a greater risk from that site. Zarouali *et al.* (2017) found however, that the use of cookies for personalised advertisements was successful as people were more likely to purchase from the targeted advertisement, compared to the non-targeted advertisement.

The Protection Motivation Theory (PMT) was first discussed by Rogers (1975) and states that an individual's motivation to protect themselves from risks comes from three components; response efficiency, perceived severity and perceived vulnerability. This theory was widely criticised for failing to give an explanation as to why individuals did not adapt protective behaviour and as such was improved and revised by Maddux and Rogers (1983) to include rewards, response cost related to risky behaviour and self-efficiency. The theory is used mostly in both health and information systems research to study behaviour and intention however a study by Adhikari and

Panda, (2018) applied this to the online privacy world and found users who are particularly concerned with how their online data is being used will adopt privacy protective behaviour's such as virus protection. This is also supported Oyserman and Schwarz (2020) who discussed the coping mechanisms people use when dealing with perceived threats and the motivations they use to avoid the threat in the future. Ahmad and Mohamed (2012) stated that motivation for self-protection is increased when an individual feels threatened by a risky event. This is supported by Adunlin *et al.* (2021) who discussed the effects the COVID 19 pandemic had on perceived risks online.

The ease of use of technology in the workplace is an essential tool, however it also opens a large privacy risk to all those who use it though data breaches (Cradduck and Gregory, 2016). A data breach can be defined as the loss or unauthorized access to data or information held by an entity (Cowan, Cradduck and Stevens, 2021). This can be carried out by a hacker, opportunistic employee (Fowler, 2019) or through human error. The organisation Security by Death (2019) found that 71% of data breaches that year were due to the result of human error. This can cause harm to the organisation through public embarrassment, fines or compensation orders (Cradduck et. al., 2021). Data subjects' now have a right to know if there has been a data breach as companies are obligated to report this to the data subject within 72 hours of being notified to ensure compliance with the General Data Protection Regulation (GDPR) (Chorpash 2020).

2.3 GDPR

The discussion of balance between freedom of expression and an individual's right to privacy is not a new topic, but one discussed as far back as 1890 through the Harvard Law Review article by Brandeis and Warren (1980), where they criticised the press for overstepping in peoples' personal lives to create news headlines. This tension between personal privacy and freedom of information is openly visible through GDPR (Sanders 2019). The GDPR is an amendment of the 1995 Data Protection directive which came into effect on the 25th May 2018. GDPR expanded on the original directive as it allows more control for employees over their own personal data and is considered as a right to respect personal life and freedom of speech for individuals living in the EU (van Ooijen and Vrabec, 2019). The act states that data controllers must have a

disclaimer on their site to inform consumers about privacy risks when collecting data, however many individuals may not understand them. The GDPR works as a supervisory authority over organisations located within the EU and aims to keep up with changes to data and how it is being used. This legislation brings in much needed protection online for data subjects, and stricter requirements for organisations when collecting or storing an individual's data. Penalties such as fines can be imposed on individuals or organisations for a breach of collection, storage or processing an individual's personal data (van Ooijen and Vrabec, 2019). The GDPR has been criticised by Buocz et. al. (2019) for its different levels of discretion for each member jurisdiction and as such different levels of protection. This was challenged by Teixeira et al. (2019) who stated that as the GDPR is a regulation it automatically applies as a law to each union member, and as such everyone located within the union's personal data is protected. So how exactly does this legislation protect users in an online setting? Data protection laws attach specific rules and regulations to the act of collecting, processing and storing personal information online, thus making it increasingly difficult for online firms such as LinkedIn to retain an individual's data without their consent. Individuals have the right at any point to object or restrict the collecting or storing of their personal data. While users were found to disclose the least information on LinkedIn in comparison to other Social Networking Sites (SNS), there still is a concern for the data that is being shared, and how this data is being used (Krämer and Schäwel, 2020).

2.4 Cookies

A new tool called cookies were introduced in 1994 on social media networks and various websites in order to personalise ads and track the websites that each computer visited (Heyman and Pierson, 2011). Cookies gain such information as browsing behaviour, advertisements clicked on and time spent on a particular page (Rawlings, 2020). The introduction of GDPR brought with it two specifications for websites collecting data via cookies. Websites must now provide a visible notice to advise they are collecting data and they must give the consumers the option to consent or not (GDPR 2020). Wiederhold (2018) argued that privacy has not been taken away, but rather has changed due to the introduction of cookies and it is up to us to draw the line between intrusion on privacy and convenience. Many scholars (Rovatsos and Such,

2016; Das *et al.* 2018; Grannis, 2015) have argued however, that these policies are simply not readable and as such, customers are no further educated regarding their privacy after reading.

2.5 Privacy Policy

“The good news about privacy is that eighty-four percent of us are concerned about privacy. The bad news is that we do not know what we mean” (Branscomb 1994). Organisations use privacy policies to detail how an individual’s data is being collected and used. Consumers are becoming increasingly concerned with how their data is being used online and as such the privacy policy aims to overcome the consumers' concerns and detail why the data is being collected. This acts to establish an agreement between consumer and organisation or informed consent to the processing of their data (Rovatsos and Such, 2016). Privacy policies are the only source of information available to consumers on how their data is being used (Grannis, 2015). Beldad, de Jong and Steehouder (2011) found that consumers use several different tests to determine if they trust the site or not, such as the organisation’s reputation, privacy policy and third-party seal of approval. Fox and Royne (2018) discussed the social media privacy policies stating they are generally written in extremely technical language, making it difficult for consumers to understand what the policy actually means. The readability of privacy policies has made it increasingly difficult for consumers to understand exactly how their data is being used. This complex language can serve to protect the organisation and allows them to freely capture the data without consumer knowledge and influences the balance of power between organisation and consumer (Das *et. al.* 2018). Fox and Royne (2018) concluded that while consumers' trust in a particular organisation is based off their privacy policy is largely unproven, it is expected that more awareness around privacy policies does lead to more trust in the brand (Clayton, Dae-Hee and Hettche, 2015).

2.6 Ecommerce setting

E-commerce can be defined as a monetary transaction for a product or service over the internet (Krishnamoorthy and Vigram, 2020). It enables organisations to reach a much wider audience and increase profitability however also opens new avenues of privacy risks for its consumers

(Jozani et al. 2020). The collection of data is particularly important within the Ecommerce setting for organisations as they require this data to understand their consumer's needs. Consumers have traditionally been defined as buyers of goods or services, however as this process moves online, they can now also be defined as end users of an application or service online (Adhikari and Panda, 2018). Granms (2015) discussed the importance of a privacy policy within the Ecommerce sector in order to create a relationship with their consumer and build trust. Trust is a crucial factor for online businesses as it enables them to create a relationship with their consumers (Aminilari Hassanian-Esfahani and Miremadi 2013). When an online transaction is made, personal details are also transmitted along with that buyers' habits, and the same can be said for individuals who are merely surfing rather than buying (Seetharaman et. al. 2017). Cappel et.al. (2020) expanded on this, stating that once data is exchanged with an online provider, there is a risk of identity theft, distortion, corruption or profiling. Oyserman and Schwarz (2020) discuss the importance of motivating and integrating employees into the organisational strategy in order to effectively implement the process within the organisation. Organisations are encouraged to train and educate employees on the strategy including the use of cookies to capture the data of online shoppers so that their shopping preferences can be targeted to improve overall sales.

Employees within this sector are aware of the use of cookies for targeted marketing and the increased risks around privacy online, and as such this study aims to investigate if they themselves are cautious when inputting their data online given their increased knowledge.

2.7 Trust on LinkedIn

Trust in technology can be defined as the willingness of users to depend on the system's functions as they believe the technology will protect their concerns (Chang, Liu and Shen, 2017). Online trust can be beneficial, as it enables users to believe that the SNS can protect their information and integrity from potential misuse or breach (Li and Zhou, 2014). This increases the likelihood of online providers placing more emphasis on security, as users who do not trust the network will have limited interactions with the site. Consumers have every right to be cautious, as a study by Pearce (2017) found that LinkedIn teamed up with a software company Data Swift to create a feature called Engagement Insights which captures an individual's

personal preferences and delivers marketing based upon this information. This technology analyses five aspects of a user's activity online which are topic analysis, text analysis, links shared, demographics and engagement such as likes and comments. Pearce (2017) stated that while GDPR was introduced to protect the individual's safety, it does not go far enough and the burden of ensuring privacy was on the consumer. Temraoui (2017) supported this through the study of LinkedIn, Facebook and Twitters privacy policies. It found that LinkedIn's policy by comparison with the other two was written in difficult terminology, with no paragraphs or subheadings and could benefit from added colour or picture charts to make it more legible. Chang, Liu and Shen (2017) supported this need for a clearer privacy policy as they stated that users on LinkedIn in comparison to Facebook, placed more emphasis on the trust in the SNS. LinkedIn is used primarily for work purposes and career progression and as such, users expect the information they disclose online to be confidential among groups with similar professional interests. As LinkedIn connections are based on individuals with similar professional interests rather than family and friends as with Facebook, their privacy concerns are heightened and should LinkedIn fail to respect this, it will result in a decline in the number of users on the site.

2.8 Privacy concerns for Employees Online

The age of social media brings with it a desire for people to share personal content and connect with others online. Dowding (1987) stated that social media fulfils the basic human desire by creating relationships and is important for the individual's self-development. Unfortunately, once this personal information is shared, it is available for all to see, including employers. Brown and Dent (2017) discuss the three factors of the employer employee relationship that are most relevant here. The first is the tension between an employee's role as an individual within the workplace and their role as an individual outside the workplace. While employees can change their privacy settings from public to private to restrict who sees the content they share, many employers will request to friend their employees to monitor their online persona (Ford and Ludlum, 2016). This raises concerns for the employee as they may fear it will affect their position in the workplace should they refuse to accept the request. The second tension discussed by Brown and Dent (2017) is the extent to which the employee's use of social media could impact the employer. This could be through a negative review online on the organisation's

products or services or the disclosure of a trade secret, which would financially impact the company. While an employee has the right to complain if being treated unfairly by an employer, this should not lead to the reputation of the employer becoming damaged or a financial loss on the organisation. The third tension is the access of an employer to an employee's social media post (Brown and Dent, 2017). Employers can monitor the employees posts to investigate a report of online bullying of a colleague or if they feel the reputation of the organisation is at risk. DeMaria, Magee and Sullivan (2016) investigated the case of the organisation Triple Pay in which employees publicly complained on Facebook for an error with tax payments and were subsequently let go for disloyalty. While employees can post freely to their personal SNS, should this negatively impact the organisation employers can use this against their employees.

Employer screening can be defined as the background verification of a potential candidate by an employer which can include traditional methods such as a Curriculum Vitae (CV) check and reading referral letters, or the modern method of checking the internet and the various SNS (Cooley and Parks-Yancy, 2018). Landers and Schmidt (2015) found almost every organisation now uses social media to screen potential candidates. Through the increased use of social medias', recruiters have a multitude of platforms to view what kind of person the potential candidate is. In today's digitalised society, many first impressions of an individual are formed based on some form of digital mediation (Utz, 2010). It also gives the interviewer additional information which may be inappropriate to ask in an assessment situation such as information on age, race or marital status, which could lead to potential discrimination (Donegan, Rothschild and Thomas, 2014). Ford and Ludlum (2016) raise the question of how much privacy employees really have online. Employers can monitor any public posts an employee may share, which is an intrusion on the employee/employer relationship outside the workplace. Casiglia (2021) stated that employers can use the argument that access to an employee's social media is necessary to protect their reputation and trade secrets and to ensure their employees are complying with state regulations to prevent legal action. Thomas *et al.*, (2014) expanded on this stating that social media reveals the undisclosed, or hidden truths potential candidates may fail to mention on their application. CIPD (2013) supported this stating that individuals display their true selves online and do not list misleading information, as a CV may. This is argued by Hall *et al.*, (2014) who stated that individuals present the best versions of themselves online, or the version of

themselves they aspire to be. The data displayed on a SNS may not be entirely accurate, and as such employers could perceive a bias based on something they saw online, which may be incorrect. Employees can also alter different profiles to suit the audience and as such will display different aspects on each platform (Jeske and Shultz, 2016). Employees may display more aspects of their personality and interests on their Facebook profile, whereas this might be significantly filtered for a LinkedIn page where employers are likely to screen. Jeske and Shultz (2016) argue that users may feel pressure to filter their profiles to suit potential employers screening and are conforming to less autonomy online. As a result, the screening process may be becoming less reliable as the online profile information may be incorrect, or very limited.

2.9 Workplace surveillance

There is no doubt that LinkedIn is an extremely beneficial tool in the workplace and has improved the recruitment process for both the employer and employee. It allows for a wide scope of talented employees to search for specific, desirable jobs and can all be done online, which saves on costs. With the increased use of LinkedIn in the workplace it has improved employment relationships as it allows for connections to be built with customers and clients and can enhance interaction, learning and development in the workplace (Aramo-Immonen, Jussila and Kärkkäinen, 2014). The employment relationship is based on the psychological contract which exists between the employee and employer and is built on trust (Chang *et al.*, 2017). It can be defined as the individual's opinion in relation to the working environment and the complicated relationship between employer and employee and the way in which this relationship affects the loyalty, performance and incentive of the employee (Budhwar, Gillani and Kutaula, 2020). When moving this relationship to an online setting, this can create a more complex relationship (Black *et al.*, 2015). The use of LinkedIn at the workplace can blur the lines between personal and professional life. By accepting professional colleagues and management to an individual's profile, this allows for a greater insight to be shared with the organisation on one's personal beliefs (Brown and Dent, 2017). Quinton and Wilson (2016) discuss how employees have raised privacy concerns when using LinkedIn, and these concerns only become heightened when LinkedIn is introduced into the workplace. Tensions can arise when competitive information is liked or favoured by an employee, which can be seen by colleagues, competitors, and

management (Quinton and Wilson, 2016). Employer surveillance on LinkedIn has risen and is a major concern for employees. With the increased use of LinkedIn for recruitment, employers can also observe the candidate's attitude, language appropriateness and their behaviour in a professional setting through LinkedIn interactions (Hideyuki Yokoyama, 2016). This allows for the organisation to make a judgement on the employee prior to hiring or change a judgement they held of a current employee based on their online habits. An employee's LinkedIn post, while on their personal page can be received by customers and clients of the organisation through their connections. While this may be posted from the personal account, should a customer or stakeholder of the business disagree with the beliefs, this could financially impact the organisation (Brown and Dent, 2017). This is challenged by Black, Stone and Johnson, (2015) who state that once the information posted is not during work hours or about the workplace, employees should have freedom of speech.

2.10 Conclusion

While privacy has been investigated and discussed in depth, little has been researched into those working in the Ecommerce setting, to investigate if they are more cautious when inputting their data online. From reviewing the current literature around online privacy, it is clear to see that employees are exposed to serious security risks given the amount of information they share on social networks and are often unaware of why this data is collected or how it is being used. While the introduction of the GDPR brought new regulations such as the requirement to display their privacy policy and allow consumers the option to accept or deny the use of cookies, many sites have made these policies difficult to read and understand. The current literature shows that many consumers neither read nor understand the policy, however little research has been done on those working in the Ecommerce sector who themselves have a greater understanding of the use of cookies on how they protect their privacy online. It is also clear from the current literature that the introduction of social media has brought with it many concerns for employees in the workplace. This study aims to understand to what extent employees are comfortable sharing their personal social networks with their employer and how comfortable they are with social media screening.

Chapter 3: Methodology

3.1 Introduction

In the previous chapter the researcher explored the theoretical and practical basis of models of privacy identified the need for an investigation into the privacy concerns of those working in the Ecommerce setting both of their own personal privacy, and privacy in the workplace. While the field of privacy is well known, there are significant gaps of knowledge at the point of applying this to employees within the Ecommerce setting who have greater knowledge of how data is used, and little is understood of how this applies to their personal social networking platforms. This chapter describes the chosen research design and the methodology employed by the researcher to achieve this study. Details of the sampling procedure are outlined, as well as the data collection and data analysis techniques used. This chapter also discusses the ethical considerations, bias as well as limitations of the study.

3.2 Research Question and Objectives

The purpose of this research is to investigate how much data employees share with the online world, how they view the perceived risks with using social networking sites online and the use of cookies, and to investigate if an employee's online persona can affect their current role in an organisation. The researcher chose to focus on employees in an online setting, to investigate if they are more private with the data they share, given their increased knowledge in how data is collected and used online.

Overall research objective: To understand how much privacy employees do have online and, in the workplace, and are employees more aware of how their data is used when working in the Ecommerce sector.

Research Objective 1: Are employees working in the Ecommerce sector more aware of how their data is collected and used online?

Research objective 2: Do employers have the right to monitor their employees personal LinkedIn account? Does this lead to a change in treatment of the employee?

Research objective 3: Are employees aware of how their data is being utilised?

Research objective 4 : How much data do employees share on LinkedIn and are they aware of how their data is being used?

Research objective 5: Do employees feel the benefits outweigh the perceived risks when sharing their data online?

Finding answers to these research objectives will allow the researcher to explore the various responses provided and find if employees working in the online sector are more careful when sharing their data online. This research aims to study the topic in depth to understand both the positive and negative aspects of sharing data and how this shared data can affect one's professional life.

3.3 Research Philosophy

Lewis, Saunders, and Thornhill (2009) described the term “research philosophy” as an arrangement of expectations, beliefs or assumptions surrounding the evolution of knowledge. For the purpose of this methodology, the research “Onion” theory of Lewis et. al. (2009) will be considered as this provides a practical understanding for presenting all the available research methods while using the chosen approach, methodology, strategy, research methods along with the analysis and collection of data. The outer layer of this onion details Positivism, Interpretivism, Pragmatism and Realism, the four research philosophies that a research study can be constructed from.

3.3.1 Positivism

This study will be based on the Positivist philosophy, which generally takes on a deductive approach. Positivism states that the only way to find the truth is through science (Ryan 2018). Positivists treat their results as facts, rather than experimental results and examine the truth by investigating current literature and hypothesis and following this process, select a fitting research strategy and develop a new hypothesis from the results (Demuth and Terkildsen, 2015).

3.3.2 Interpretivism

Positivism is contrasted by Interpretivism which employs the humanistic element as researchers interpret the results of the study (Dudovskiy, 2018). It argues that human beings and social interactions cannot be studied in the same way as physical interactions and as a result believes social science research should be different from natural science research. (Reger, 2013)

3.3.3 Pragmatism

Pragmatism views concepts as only important when they support action (Powell, 2020). It views the research questions as the most important part of the study and aims to create viable solutions that inform future practice (Lewis et. al., 2009).

3.3.4 Realism

Realism relies on the idea that a universal reality exists regardless of a prior knowledge or particular state of mind (Lewis et. al., 2009). It is divided into critical realism and direct realism. Critical realism states that we have two ways of interpreting the world, through events we experience and through our mental state when we process the event (Montoya-Vargas, Parra and Said-Hung, 2021). Direct realism believes that everything that is seen is true. Direct realism denies that justification for external world events depends on justification for such mind related events (Huemer, 2018).

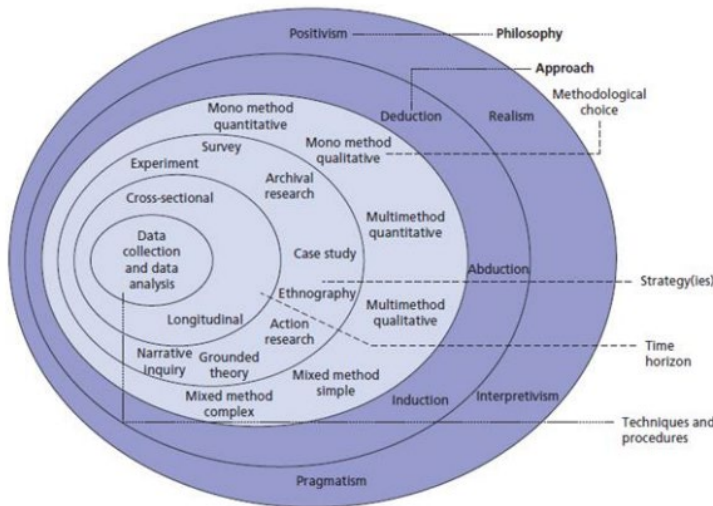


Figure 1: The Research Onion
Lewis et al. (2009)

From reviewing previous research in this field in the literature review, researchers typically used either qualitative, for example Black et. al., (2015) or quantitative, like Bohmova (2016), Chang

et. al. (2017) and Aramo-Immonen et. al., (2014), methods. The Quantitative research method will be used for this paper as this comes from the belief that human experience and variables in human behaviour can be objectively studied (Vindrola-Padros et. al., 2020).

3.4 Research Design

This section provides an outline of the research design adopted for the present study as a means of addressing the research question of the privacy online of employees within the Ecommerce setting. For this study, the researcher had chosen a quantitative approach to gather the data required for this study. Aliaga and Gunderson (2002) state that quantitative research is “explaining phenomena by collecting numerical data that are analysed using mathematically based methods (in particular statistics)”. The quantitative research approach focuses on statistical data, the emphasis of which is more centred on numerical information, as opposed to verbal accounts as with qualitative research. Gray (2017) described qualitative research as a way of answering questions or explaining an idea of interest, culture or social process through the perspective of the participant by collecting and analysing descriptive data. Interviews were considered for this research however the researcher was mindful of the time constraint as this study was carried out over one academic year, making quantitative research more practical as qualitative research generally requires the researcher to be submerged in the participants culture to collect several different types of information (Creswell and Poth, 2018).

From reviewing the literature, it became apparent that a lot of information has been collected regarding the privacy of employees online, what is not apparent however is how secure people are online working in the Ecommerce sector. For this reason, a quantitative approach had been chosen as by selecting a larger research group of 100 participants, the researcher could gain a broader understanding of their privacy concerns. Research by the University of Lancaster (2016) found that quantitative methods of research have many advantages such as a larger sample size, which allows for more generalised results. Consequently, a qualitative research approach would not have been suitable in this case, as due to the topic which is privacy and security online the researcher felt that qualitative primary data collection methods such as an interview would not allow anonymity for the participants which may deter them from partaking. Previous researchers

investigating the topic of online privacy such as Bohmova (2016), Chang et. al (2017) and Aramo-Immonen et. al., (2014) also used surveys to collect their data. Therefore, the researcher found quantitative research with a survey as the most suitable method of collecting data. Quinlan et. al. (2015) listed roughly twenty different research types to choose from, this was challenged by Lewis et. al., (2009) who cut this down to just seven; survey, ethnography, grounded theory, case study, experiment and action research. These can be shown in the middle layer of Saunders research onion, and for this study the survey research method will be used. The tool Google Forms was enlisted to create and send the survey to those working in the company. A pilot study was tested first on 10% of the sample size to ensure content, language, format and length were all appropriate (Vindrola-Padros, et al., 2020).

3.5 Data Collection Method

The researcher chose a cross-sectional web-based survey as the preferred form of data collection for this study. Creswell (2009) stated that survey research is beneficial as it allows the researcher to gather numerical data which describes the attitudes, trends and opinion of a population. Cross-sectional studies are beneficial when there are time constraints or limited resources available. (Collis and Hussey, 2009) While there have been some issues raised with survey research such as a low response rate and the possibility of false information provided (Gillespie, Lovekamp, and Soboroff, 2017) however Levin (2021) stated their importance in research as they provide researchers with a large amount of data in a short space of time and are low cost. Given the time constraint to complete this research due to the August 2021 deadline and the topic of the research which was privacy online and the use of social networks, a web-based survey was found to be most practical for the researcher. Bell and Bryman (2011) added that web-based surveys provide quicker response rates, are easier to administer and use and leave fewer questions unanswered. Given the topic of online trust, a web-based questionnaire was deemed more suitable as the data subjects would have little interaction with the researcher and felt more honest answers would be provided. Online privacy is a sensitive topic and as such an anonymous questionnaire provides a platform for a range of anonymous responses and allows the researcher to gather the relevant information.

The platform Google Forms was used with a structured questionnaire using closed questions with the exception of four questions. A consent form appeared on the first page of the study which can be seen in Appendix A, required respondents to read and acknowledge this before proceeding to the survey. The first question was based on the amount of data shared online which required respondents to tick the box, the second required respondents to select from 4 different cohorts to determine the amount of connections they had on LinkedIn, the third requested employees to rate on a scale of 1-10 how comfortable they were with sharing data online and the fourth requested respondents to select how important it was for them to control who sees their online profile from extremely comfortable to extremely uncomfortable. Appendix B includes all the questions asked for the purpose of this research. Imai, Rosenfeld, and Shapiro (2016) found that studies that contain predetermined questions and answers are beneficial as the precise data will be presented as there are only a limited number of answers. The researcher chose predetermined questions as it cuts out bias from the researcher and is the most convenient way to collect enough quantitative data to rely on the results as a fair sample of the general population. It also cuts out on bias from the researcher.

3.6 Data Analysis

Data analysis is an integral part of the research and can be defined as the way in which we understand the data before presenting it for interpretation. (Rashidi, 2014) There are two different types of data which can be gathered during research such as this. These are primary data, the method we will be using in this research piece which is gathered from first hand sources such as surveys or experiments, and the second is secondary which is obtained from second hand sources such as other researchers interviews, census or government records (Bryman, 2012). Lewis et al. (2009) discuss the two ways of collecting data in this field. Mono which is gathering and analysing data in one way and the second is Multiple, a method that utilising multiple models to collect and analyse the data. For this study, we will be using the Mono Quantitative method to analyse the data with graphs and statistics using numerical data.

The data was analysed using the tool SPSS. The data was downloaded on the 27th July 2021 using Google Forms, which downloaded the data through Excel, allowing for the data to be easily transferred through to SPSS. Luff and Sturgis (2020) stated that this was one of the major

advantages of using web-based survey software, as it removed the large task of transferring data. The researcher then uploaded the file to SPSS, where the data was then validated using Cronbach's Alpha.

3.7 Research Participants and Participants' Demographics

The researcher carried out a survey with 100 participants all working in the same large Ecommerce sector in Galway, Ireland. The researcher chose the large Ecommerce company Wayfair based in Galway, Ireland as the researcher felt that by surveying a number of employees working for the one company this would ensure consistency throughout the knowledge of the employees from the training they had received. Their age ranged from twenty-one to sixty which was also important as this would supply insight from employees of all ages, who would all have different experiences when it comes to protecting their data online. The researcher used the anonymous platform Google Forms to allow participants to feel at ease in answering these questions which are of a sensitive nature. If there is an anonymous platform, the participant may feel more inclined to answer honestly and truthfully.

3.8 Sample Size

In its broadest terms, the aim of this study is to understand how all of those working in the Ecommerce sector in Ireland view their privacy online, and what concerns they have in relation to its use in the workplace. However, given the number of employees working in this sector in Ireland and with the number of employees working from home during the COVID 19 pandemic, contacting each employee would be a monumental undertaking. Instead, this study will focus on 100 employees working in the same large, Ecommerce business located in Galway, Ireland. Cohen, Mannion and Morrison (2007) identify the following as important criteria when choosing the sampling strategy for the research to be conducted:

- the sample size.
- representativeness and parameters of the sample.
- access to the sample.
- the sampling strategy to be used.

3.9 Pilot Test

Pilot tests are essential to ensure questions are phrased correctly so that participants can easily understand their meaning and answer accordingly and to ensure the answers provided supply enough of the required data. (Luff and Sturgis, 2020) A pilot survey was carried out with 10 participants from the same target audience and was sent via email. Reio (2007) stated that a minimum of 10 responses were needed for a pilot test, however Lewis *et. al* (2012) argued that the pilot size was dependent on the size of the study.

The pilot test was not only necessary to ensure the data was working and recording the responses correctly, but also to ensure enough data was being collected to support the hypothesis. Based off the pilot study, changes were made to the study to include more questions to ensure enough data was being collected, and enough information would be gathered. The pilot study was created using the site SurveyMonkey as O'Brien & Torres, (2012) stated that its automatic data function reduced human error in computing. The researcher then decided to change this platform to Google Forms however as SurveyMonkey only allowed for 10 questions to be used for the free trial and Google Forms allowed for more questions to be asked. Although the sample size was relatively small, with 100 participants the author believes that the information gathered, whilst the researcher is not claiming to be representative of employees as a whole, instead it is representative of how the participating users protect their privacy online and how they utilise social networks in their everyday professional lives.

3.10 Ethical Considerations

Ethics can be defined as the moral principles which dictate a person's group, conduct or organisation (Quinlan *et. al.*, 2015). Ethical considerations need to be taken into consideration when sending out a survey relating to workplace practices within an organisation. As the participants in this survey would be disclosing information about the conduct of the organisation they currently are employed with, their confidentiality and anonymity must be considered. In order to avoid any ethical issues, the researcher first submitted an ethics review form which was approved by the ethics board prior to carrying out any research. The participants remained anonymous throughout the survey and were not required to input personal details at any time.

The researcher included a cover letter at the start of the survey detailing the aims of research and how each participant's data would be used. The researcher also advised all participants the opportunity to view the results of the study should they wish to see this. Each participant was required to acknowledge this by clicking to “accept” that they had read and understood the aims of the research prior to accessing the survey. Results from the data were always also safely stored and password protected. The data will be destroyed once it is no longer required for the purpose of this research.

3.11 Limitations and Limiting Bias

Moosa (2019) defined the occurrence of bias in research as when fundamental error is introduced to research by selecting or encouraging one outcome or answer over various other alternatives. To ensure that the results would not be contaminated, and bias was not a factor, all questions were composed in a neutral fashion. As the sample size was on a small scale as well as the time constraints of this research, the findings of this study are not representative of the experience of all employees working in the Ecommerce sector, but only represent the responses of the participants in this study working for one company. Should the researcher have had more time, a wider sample audience could have been surveyed with responses from not only Wayfair, but other Ecommerce companies. The scope of the study is also limited in terms of geographical data as all employees work in Galway in the West of Ireland. A sample of employees from all over Ireland would provide the researcher with more countrywide data and further extend this across the globe, rather than data from one section of the country. This would ensure representative reliability.

One of the limitations of this study was cost. As mentioned previously, the researcher had intended to use SurveyMonkey to create and send the survey, however once created the researcher found this would not be possible as it only allowed for ten questions for free. This was then changed to Google forms.

Another limitation the researcher experienced was the lack of variables used in this study in order to analyse the data through SPSS. It would have been beneficial for the researcher to use a number of variables such as gender or age in order to compare the results and analyse this in

SPSS. These variables could have been cross examined to find differences between them and could have provided an insight into if gender or age played a role in how secure these employees are when it comes to their privacy online. Instead this study was a descriptive investigation into how much these employees knew about online security.

Chapter 4: Findings and Analysis

4.1 Introduction

This chapter outlines the main findings that emerged from data analysis of the surveys carried out with 100 employees, on their experiences of privacy online and in the workplace. This study is a descriptive exploratory analysis into the behaviors of employees working in the Ecommerce sector and how secure they are with their personal data online. From analysing the data from this questionnaire, the researcher is able to answer and discuss the research objectives as well as the overall research question.

4.2 Reliability Test

In order to validate the data, the researcher first needed to validate the data. The scales were adapted from the studies of Chang, *et. al* (2015), Greene (2013) and the work of Jones (2020) and as such had previously been validated. As they were adapted for this study however it was essential to retest the validity of the sales. To test the reliability of the study, Cronbach’s Alpha reliability test was ran through SPSS on the different groups of questions. Olvera *et. al.*, (2020) found that values should ideally be above 0.7 to report validity, however when there are a smaller number of items in the scale being tested these figures tend to be lower. Question 4 was a multiple choice question and as such each choice was broken into an individual question for reporting purposes. The questions were then grouped according to approach to LinkedIn, Workplace Surveillance and Online Privacy. The results of the Cronbach’s Alpha tests listed below.

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.364	.476	16

Table 1 : Reliability test LinkedIn approach

Output

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.490	.377	4

Table 2: Workplace surveillance

Output

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.530	.513	6

Table 3: Online Privacy Output

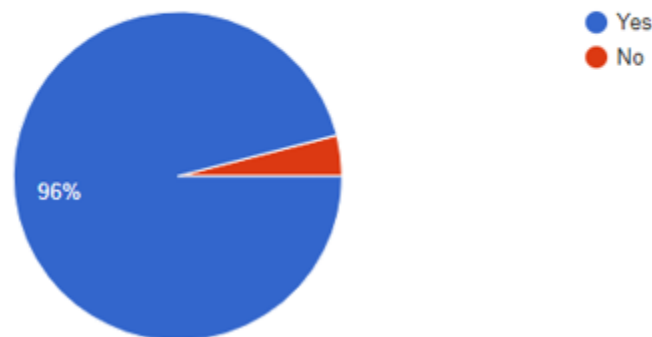
4.3 Findings

The survey was created and sent out on the 6th of July 2021, and was left open for 3 weeks to ensure a high participation rate which was achieved. The questions were all listed as required questions, therefore the survey could not be completed prior to answering all questions. Prior to participating in the survey, each individual was required to read and accept the terms listed in the consent form. The first 7 questions are concerned with LinkedIn, and how much data users share on the platform. Questions 8-11 are concerned with data and cookies online, and how much data users are willing to share. Question 12 is concerned with the respondents job, and questions if they have an increased awareness of privacy online from working in the eCommerce sector. Questions 13-15 focus on workplace surveillance and the final 3 questions aim to discover exactly how secure the respondents feel when sharing data online.

Question 1:

Do you have a LinkedIn account?

100 responses

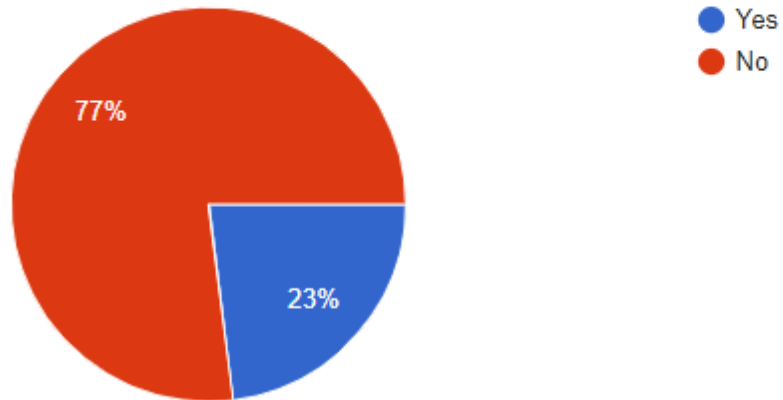


The first question of the study found that of the 100 participants, 96% had a LinkedIn account. LinkedIn stated in the most recent Pressroom in August 2021, that they have over 774 million users in over 200 countries (LinkedIn, 2021). This survey mirrors that, as in this workplace with employees of varying ages over 95% of employees questioned have a LinkedIn account.

Question 2:

Have you read the LinkedIn privacy policy?

100 responses

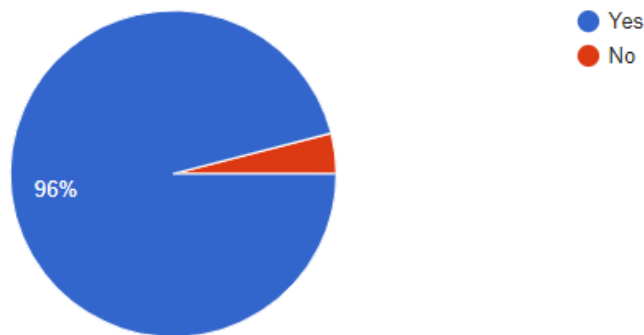


Of these 96% that do have an account, only 23% have read LinkedIn’s privacy policy. This question was asked to determine whether or not employees who deal with online privacy in their everyday work are concerned about their own privacy when using the internet. Interestingly, 77% of respondents have not read the policy.

Question 3:

Do you refrain from posting certain things to your LinkedIn in case it would impact you professionally?

100 responses



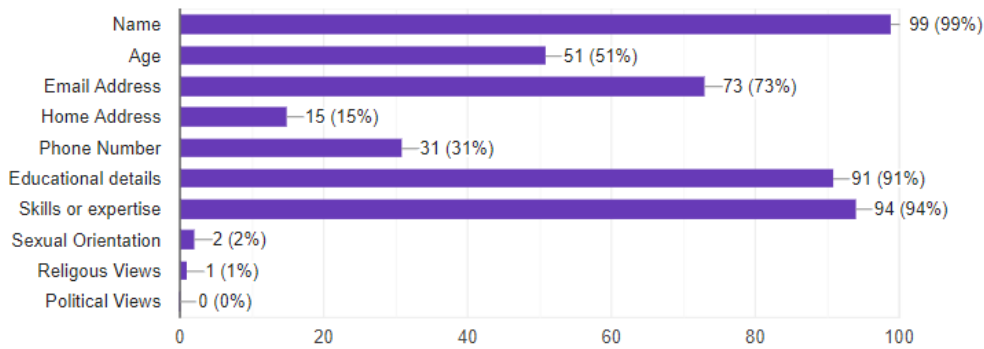
96% of people stated that they would refrain from posting certain information to their LinkedIn account as they felt it would impact them professionally. The motivation behind joining LinkedIn is varied for different people however Agrawal et. al. (2016) found that over 90% of employees join the SNS to not necessarily find a new job, but to hear about the available opportunities.

Question 4:

How much personal information do you share on LinkedIn? Tick all that apply



100 responses

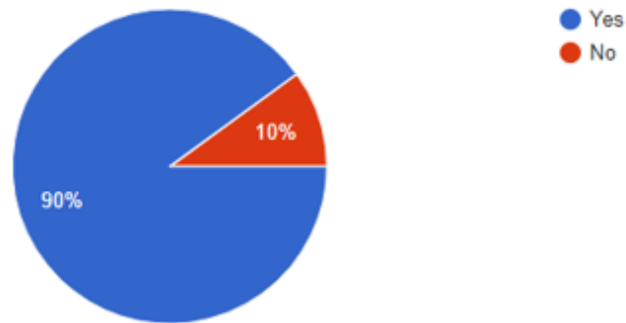


This question aimed to understand exactly how much data employees are sharing on their LinkedIn page. What is interesting to note is the amount of data the participants are sharing. Over 90% of the participants disclosed their name, educational details and skills, while 73% also shared their email address. While the findings show that respondents were slow to share personal details such as sexual orientation, religious view and personal views, users still share a vast amount of data such as 51% disclosing age and 31% displaying their personal phone number. Displaying this amount of data can lead to data breaches which these users are familiar with from their current profession, the research shows that users are still willing to take the risk.

Question 5:

Do you think the information you share on LinkedIn has an impact on recruiters reaching out to you?

100 responses

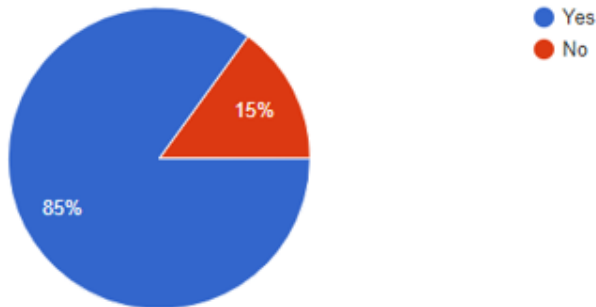


An understandable 90% of users found that information disclosed on LinkedIn would affect potential recruitment opportunities. Perkins (2015) carried out an interesting study in the US surrounding this topic which found that one third of employers would not consider interviewing a potential employee if they did not have any kind of online presence. While it is important for professionals to have a LinkedIn account, opinions or comments they post can be seen by recruiters and as such users are very much aware of what they post online. This is in line with previous studies in this field such as Jeske and Shultz (2016) who stated that employees are aware that recruiters are screening their profiles and as such are careful to filter what they post online.

Question 6:

Do you agree with recruiters screening potential employees LinkedIn profile prior to reaching out to them?

100 responses

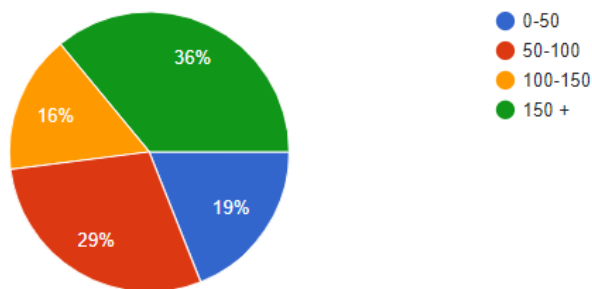


An interesting find in this study was the vast majority of users do agree with online screening of their LinkedIn profile. Levashina and Roulin (2019) found that individuals display their best self on LinkedIn with extensive lists of skills and accomplishments, primarily for recruiters to view. This is in line with question 5 as the survey found that employees will filter their profiles to what they would like a recruiter to see, and they do agree with recruiters screening their profile prior to reaching out to them. LinkedIn is viewed as a second survey and as such, individuals have no issue with this platform being viewed if the reason is for potential employment.

Question 7:

Approximately how many connections do you have on your LinkedIn profile?

100 responses

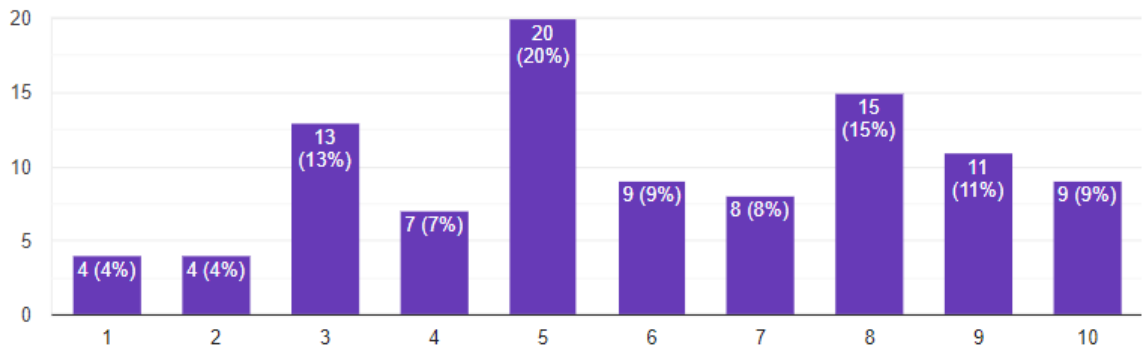


The number of connections on a LinkedIn profile was relatively evenly split, however the highest percentage went to those with 150 connections or more. This is quite a significant a significant number of people to share personal data with, especially as the results show that users are afraid of how their data is used. The results of this study can be compared to that of Banerji and Reimer (2019) who found that well connected professionals on LinkedIn does not always equate to more success. The study found that who employees were connected to was more important than the number of connections they had. Almost 50% of participants had less than 100 connections, however these users are still quite active online sharing high amounts of personal data as seen in question four.

Question 8:

How comfortable (on a scale of 1-10) do you feel with LinkedIn storing your data and the use of cookies?

100 responses

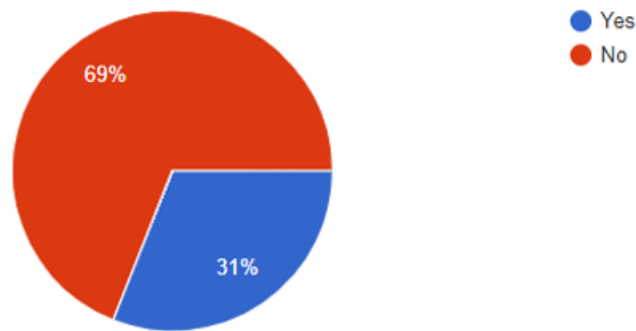


With 1 being comfortable, and 10 being uncomfortable, this question yielded varying results from the respondents. Of the 96 users that have a LinkedIn account, only 4% were extremely comfortable with LinkedIn using and storing their data, and 20% felt they were undecided on the matter. What is interesting is that while 40% of people were more uncomfortable than comfortable with the LinkedIn using their data, still only 23% of people have read the privacy policy to understand how their data is used. Kroll and Stieglitz (2021) found similar results in their study on users perception on the collection and storage of data online. They found that users have mixed feelings about the use of their data online as for the majority they are unsure how this is used, however control for them was the most important factor.

Question 9:

Has your employer ever requested to connect with you via LinkedIn?

100 responses

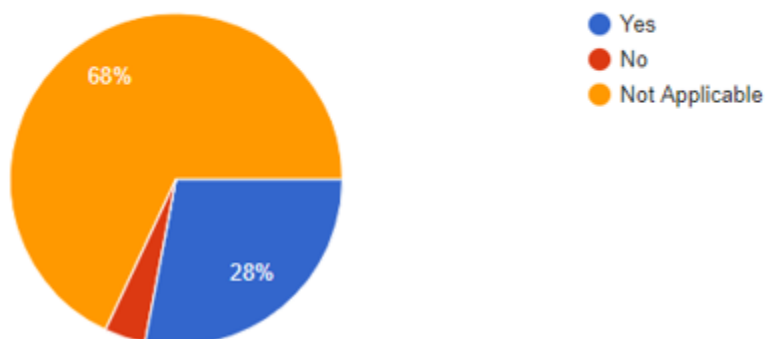


This question has an interesting find, with only 31% of users experiencing an employer requesting to connect with them online. While employers likely have viewed the LinkedIn profile or another personal SNS, this study found a relatively low number of employers had requested to connect with their employees. Flinchum, Kruse and Norris (2018) found that employers have the upper hand when it comes to the power online and this is clear from the results of this survey. Employers know they are crossing a line by requesting to connect online however 31% have done so regardless.

Question 10:

If yes, have you accepted them to connect with you?

100 responses

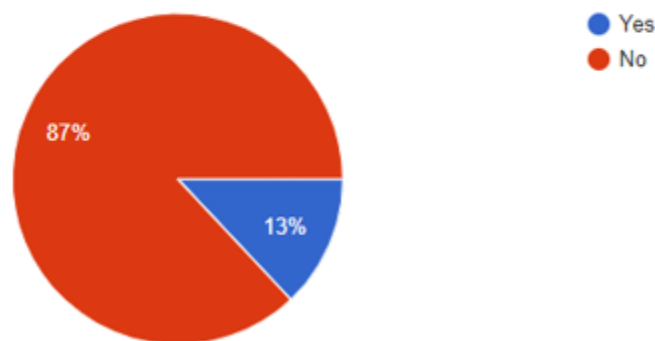


While only 31% of employees have had this request, 28% of respondent's accepted the request from their employer. The majority of respondents, did accept their employers request to connect online. Brown and Dent (2017) concluded from their study that while employees may not be entirely comfortable with this connection, they do not want to risk the repercussions of not accepting this request from their employer. This highlights a lack of protection for employees from their employer when it comes to security online. Further research could be done on why exactly such a high number of employees accepted their employers request.

Question 11:

Do you read privacy policies for other sites prior to accepting cookies?

100 responses

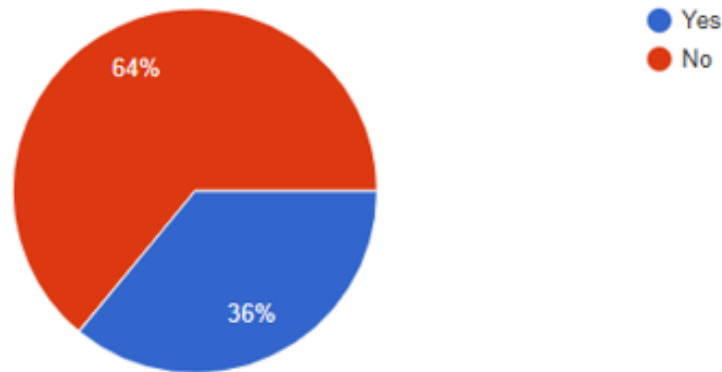


What is interesting to note, is while only 23% have read the LinkedIn privacy policy, only 13% of respondent's have read privacy policies for other sites. Such and Rovatsos (2016) found that people may be more likely to read privacy policies concerning social media sites, rather than the privacy policies of regular websites. This is due to the fact that the information shared is more public, and easily accessible to a wide audience. It also coincides with the work of Bornschein, Schmidt and Maier (2020) as previously mentioned that unless a privacy warning is given on site, or users are made aware of how their data is being used individuals are happy to ignore the risks for the perceived benefits.

Question 12:

Do you understand how your data is used when captured online?

100 responses

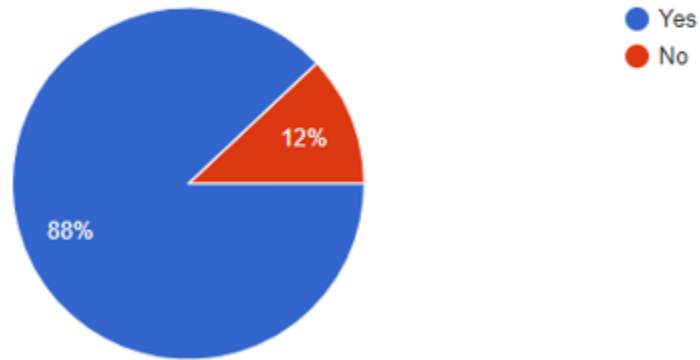


64% of people stated that they don't know how their data was being used online. Fox and Royme (2018) raised concerns around this topic as 64% is quite a high percentage of users to be unaware of how their data is not only being collected and stored, but oftentimes sold to other third party sites for targeted advertisements. This response is not surprising, given how little of the respondents have read the LinkedIn and other privacy policies. This study supports the studies of Breckenridge (2020) and Kapczynski (2020) as discussed in the Literature Review, that the complex language of privacy policies means that even with the GDPR making these policies a requirement for users to accept, users are still failing to read these due to the complex wording in which they are written.

Question 13:

Do you believe recruiters view your personal social media sites?

100 responses

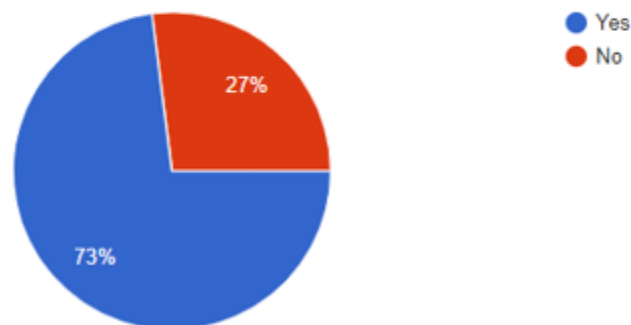


Jeske and Shultz (2016) found that while the screening of LinkedIn was expected, looking up personal social networking sites is unethical. 88% of those surveyed felt that employers were not only screening their LinkedIn profile, but also their other personal social networking sites. This coincides with the work of Kokolakis (2017) as previously discussed in the literature review. While employees are not completely comfortable with their employers requesting to connect with them online 85% of participants confirmed they agree with recruiters screening their networking profiles.

Question 14:

Have you used the added security features to restrict what people can see on your profile?

100 responses

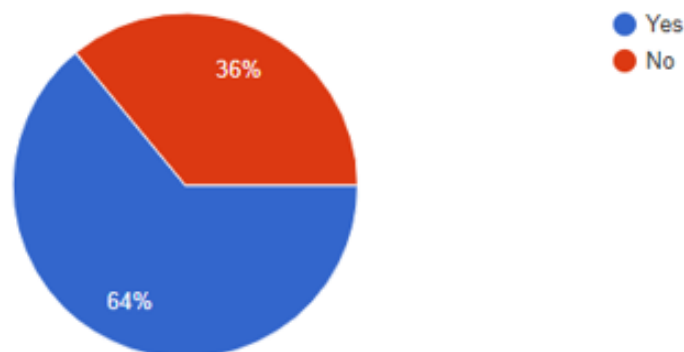


73% of users reported using the additional security features when it comes to restricting how much personal information people can access. In contrary to other similar studies of this nature such as Cradduck and Gregory (2016) and Kokolakis (2017), quite a high number of respondents reported using additional security features. This is likely due to the increased awareness these employees have of online data from working in Ecommerce, as reported in question 15. This is supported by work of Adhikari and Panda (2018) as previously mentioned, who found that those who were particularly concerned with the overexposure of their data online did employ the use of the additional security features.

Question 15:

Do you feel as though you have a greater understanding of how your personal data is used online from working in the ecommerce sector?

100 responses

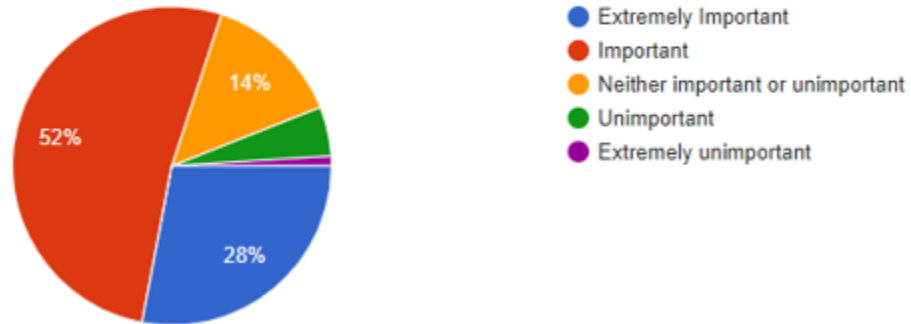


64% of people reported that they felt they had a greater understanding of how their data was used online from working in the eCommerce sector. This was an interesting result as this area had not been investigated before, and from this result it is clear more research can be done into why these employees feel they have an increased awareness. It is clear from the responses to other questions that while these employees within the Ecommerce sector do feel more informed, they are perhaps quite open with the amount of data they share and the number of connections they have online.

Question 16:

How important is it to you to control who views your profile online?

100 responses

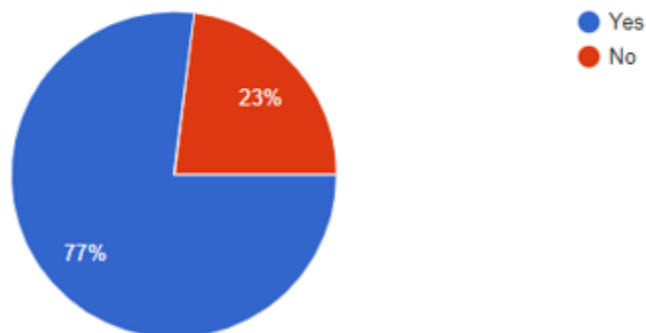


52% of people felt it was important to control who views their profile online, while only 1% of those asked found this to be extremely unimportant and 5% found it was unimportant. Control online is a determining factor when it comes to online privacy. O'Brien & Torres (2012) found that once an individual has lost control of their data online, or if they feel they are losing control they will no longer trust that site. Over 75% of respondents do find it important to control who they connect with, and 73% have used the security features who restrict who can see their profile. This does show that some efforts are being made to protect their data.

Question 17:

Do you worry about your privacy and data when using the internet?

100 responses



77% reported that they worried about how their privacy and data was being collected and used online. Despite this fear of how their data is being used, it has not stopped users from joining the networking site, or from sharing a vast amount of personal information online. It is also concerning that while the participants felt that they had a greater awareness of how their data is used online from working in an online business themselves, still only 36% of the participants understand how their data is used. Since the introduction of the GDPR in 2018, this has brought stricter rules for organizations when collecting data online and has made it easier for consumers to protect their data as displaying the privacy policy is now mandatory. While steps such as this have been taken to protect data online, the study shows the majority of people are not well informed on the matter, and as such fail to read privacy policies and accept the risk they are taking. 64% of people reported in Question 12 that they did not know how their data was used, yet over 75% of people stated they are worried about their data online. The responses from this study show that while employees are worried about their online privacy, an effort is not made to inform themselves on data protection online.

Chapter 5: Discussion

5.1 Introduction

The aim of this research was to understand how much privacy employees have both online and in the workplace, and are employees working in the Ecommerce sector more aware of how their data is stored. The research also aimed to investigate how much knowledge Irish consumers have regarding sharing their data online, and how many risks they are willing to take in order to open and maintain SNS such as LinkedIn. A questionnaire was used as the research collection method which received a total of 100 responses. The main themes that emerged from the findings of the study will be discussed in this chapter and commonalities and contradictions will be drawn in relation to the literature reviewed in chapter two.

5.2 Ecommerce setting

The first sub objective the researcher wanted to investigate unlike the previous works in this field was to understand if the line of work of all those who were surveyed – i.e. if these employees working in Wayfair who deal with online transactions on a daily basis had an increased awareness into how their data was used and placed more emphasis on their online security because of this. As mentioned in the literature review, there is a gap of knowledge surrounding the various careers online and whether they are at an advantage when it comes to protecting their data online from the different data breaches and online transactions they have dealt with.

64% of respondents felt that they have a greater understanding of how their personal data is used online from working in the Ecommerce sector. What is interesting to note is that while a large percentage of these employees feel more educated when it comes to data online, over 75% of those surveyed reported feeling worried about their privacy and data online when using the internet, and the majority of respondents also admitted to sharing a large amount of personal information to their networking profile. Benson, Saridakis and Tennakoon (2015) carried out a similar study which yielded very similar results. This study found that a large amount of personal information disclosure was associated with a lack of knowledge in how the data was being used, which is how the employees in this survey too responded. The main theme that emerged from

this section of the study was that employees working in this sector did feel they had greater knowledge of how data is processed online, however it does not restrict them from posting personal information, or ease their concerns on the risks of data breaches and identity theft online.

5.3 Privacy Online

The second sub objective to investigate was how secure respondents felt with sharing data online. The understanding that was gained from the surveys was that the participants' articulation of online security was wide ranging. One of the most worrying finds of this study was similar to the results of Chang *et.al.*, (2017), the research found that while many users were worried about how their data was being used online, and many did not understand how this was being used, a high percentage of users still shared a substantial amount of personal data on the networking site. There was a definite agreement from all participants that there is a security risk when sharing personal data online. This contrasts with the findings of Pitkänen and Tuunainen (2012) who found that users in Finland had trust in the online platforms to protect their data, the Irish participants in this survey did not. This study supports previous work such as Qin and Tan (2012) and Kokolakis (2017) in their theory of the privacy paradox. While respondents displayed unease at the collection and use of data, they were still willing to self-disclose in order to continue to use the network. Some users did admit to using the additional security features to restrict who can see the information on their profile, however these people are still putting themselves at risk. The highest portion of respondents reported having over 150 connections on their LinkedIn account, while the second highest portion of respondents reported to have between 50 and 100 connections. This is a worrying number of people to share such high amounts of personal data with. These findings are supported by Budak, Rajh and Škrinjarić, (2019) who discussed this worrying trend of users being aware of the risks, however posting this personal information anyway without any pressure on them to do so.

As Gabisch and Milne (2014) discussed, once you agree to share your data online you are accepting the risks associated with data breaches. With that said, there seems to be a lack of knowledge among the participants with exactly how their data is used, yet the participants still fail to read companies privacy policies to educate themselves on how the data is being used, and

how best to protect themselves. Less than 25% of those surveyed have read the LinkedIn privacy policy, and only 13% stated they had read the policy of other sites prior to using them. Zuboff (2019) suggested one of the main reasons for such a small number of people reading the policies was since they were intentionally written in complex and confusing language so that people would not understand how the data was being used. The main theme that emerged from the research in relation to privacy online was that while respondents are aware of the risks associated with sharing data online, they are willing to take the risk in order to have an online presence. It does appear however that the respondents do try to take additional care when it comes to their data by using the security features and restricting who and what can be seen on their profiles by the public.

5.4 Workplace surveillance

The third sub objective to investigate was the issue of workplace surveillance, particularly in an online setting. From reviewing the literature, it is clear how popular the social media giant LinkedIn has become, particularly in the professional world and as such it came as no surprise that 96% of participants had an account. In contrast to the findings of Ford and Ludlum (2016) a relatively small percentage (just under one third) of the respondents reported that an employer had requested to connect with them via LinkedIn. Of those that had an employer request to connect however, most respondents accepted this request. Brown and Dent (2017) stated the reason for this high percentage of employees accepting their employers is fear that they would be treated differently or unfavourably in the workplace had they not accepted the request. Employers may feel employees have something to hide or are not totally committed to the workplace.

This findings in this research supports the findings of Cooley and Parks-Yancy (2018) in the awareness employees have of employers not only viewing their LinkedIn profile, but personal sites also. Almost 90% of respondents felt that personal sites were being checked along with the expected screening of their LinkedIn profile. 96% of respondents also admitted to restricting what they post on their LinkedIn account in case it would impact them professionally. Utz (2010) noted that the more recruiters can see prior to meeting a potential employee, the more biased they will be in an interview setting from what they have seen online. It is clear this is a source of

worry among the employees who engaged in this survey, as almost 75% admitted to using the additional security features to restrict what information can be viewed on their online profile.

Contrary to the findings of Hall et al., (2014) that employees present the best version of themselves online and as such would not be opposed to employers viewing their networking sites, only 6% of the respondents of this survey felt it was not important to control who viewed their online profile. The main theme that emerged from the workplace surveillance section of this study is that employees are concerned with how much their employer can see about them online, but also fear if they don't allow access to their employer it may cause a change in treatment. The amount of freedom an employee has on their own personal networking site is becoming more and more restricted through the various social platforms online.

5.5 Implications of the Research

This research has a number of implications for several domains. Firstly the current research on privacy online is expanded to professions, with this study focusing on those working in the Ecommerce sector. The results from this research shows that users online are worried about their data, and don't trust online retailers when it comes to protecting their data. A worrying find from this study is that while all the employees surveyed for this research work for an online retailer, they too do not trust how their data is processed online. From this it is clear there is an issue with how open retailers are with data, and their willingness to sell the data to third parties.

This dissertation research has implications to different stakeholders such as online retailers themselves. This study which has been supported by a range of literature surrounding this topic shows that retailers leave a lot to be desired when it comes to users' trust in their site. Many consumers do not understand how their data is being used and as such it would be beneficial to explain more about this to the consumer in lay terms rather than the complex privacy policy. This is supported in the study by Fox and Royne (2018) who found that users failed to read the privacy policy not because they weren't concerned about their data, but because it was too difficult to follow. As previously discussed in the literature review, Li and Zhou (2014) mentioned that online trust would be an extremely important factor for organisations as users would be more willing to use the site if they felt their online integrity was being protected.

Organisations must have a greater awareness for these policies. Although creating new, understandable privacy policies would come with significant costs to the organisation they are necessary in order to regain users trust. This would then boost capital for the organisation as more users would be willing to join, and current users feel more comfortable in using the sites and would be willing to spend more. Organisations could also reduce cost through high turnover rates, retraining employees and reduced productivity from employee participation on SNS. (Lu and Pan, 2019) Employee participation on sites such as LinkedIn can be seen as a negative factor from an employer's perspective should something negative or unprofessional be posted online, however organisations must understand that these professional SNS play an important role in the individual employees professional progression.

These findings also hold importance for current employees. There is a need for employees themselves to take charge of their privacy online and educate themselves on how to be more secure, and how to protect their data. While privacy policies can be complex, they do explain in depth how exactly the data is taken and processed and users do have to option to decline this.

5.6 Limitations of the Research

This study aims to add to the field of literature surrounding online privacy and employee surveillance, however, must be viewed with some limitations experienced when carrying out this work.

The first limitation to be considered is the sample size of 100 people which would be considered a small-scale quantitative study. Should there not have been the time constraint of this work due in August, the project could have been left open for longer to ensure a much higher response rate and gain a greater insight into the research. This study also focuses on one company, Wayfair whose employees are situated in Galway, Ireland one of 9 office locations across 3 countries. The study does not give an insight into a range of different online companies as some may have received greater training and have had more exposure to protecting their data online than others. Other factors to consider include looking at Wayfair itself as a type of retail company. Wayfair is

an online furniture company and may have exposure to threats than perhaps a retailer working with clothing or other services.

Timescales played a limiting factor in this research. The study would also have benefited from a mix-methods approach to gain a more in-depth understanding into the kind of exposure the employees had to online data through their role in Wayfair. This would allow for a greater understanding of how much additional knowledge they had, and how exactly they felt about the topic. This study also has no control group. The researcher had to take into account what could be done in the timescale given. The researcher prioritized a descriptive study over a comparative one, as they felt they could completely focus on this and complete it in the timeframe given, rather than rush the study and yield unsuccessful results. Should the researcher have had more time, an interesting take on this study would be to create a comparison group of employees who do not work in the Ecommerce sector, and compare the results of this.

The survey was built around insights found in the literature review and was adapted to suit this study. The researcher would have benefited from an already validated scale to ensure all data interpreted was valid. This would also have expanded the range of tests that could have been carried out in the data in SPSS, as from the scale the researcher would have had a number of variables such as age or gender. The primarily yes/no survey responses meant the various methods to interpret the data was limited.

As with the sensitive nature of privacy online, there may have been bias from those who felt more strongly about the topic and as such filled out the survey as those who were perhaps not as passionate on the topic. This may have led to a bias in the results and as such should be viewed as a possible limitation in the study. Saunders *et al* (2012) stated as with all research reliant on human response there is a limitation as people tend to give socially pleasing feedback to paint themselves in the best possible light.

Cost was another limiting factor in this survey. The study was initially conducted via the platform SurveyMonkey however as this would only allow ten questions for the free trial, the researcher chose to switch to Google Forms.

COVID 19 also played a role in limiting this study. As the researcher was not able to physically meet the employees of this study and explain more about it, the researcher felt that this limited them in terms of the responses they received in the survey. As such the researcher chose quantitative research instead of qualitative such as an interview, which may have provided a more in depth and descriptive feedback into the thoughts and perceptions of these employees. The survey was open for 3 weeks and received 100 responses out of a workplace of over 400. The researcher felt that had they been able to speak with employees and explain more about the study, they would have been able to gain a higher response rate.

The study could be repeated ensuring a larger sample size, a mixed method research model, a range of different companies and a broader time horizon. While the study did have various limitations, the researcher was happy with the overall results and the insights which were gained.

5.7 Future research

The results of this survey have highlighted several areas for future research. As mentioned previously this was quite a small-scale study due to the time constraint, however a larger and more in-depth study into the topic with a variety of different online retailers from different geographic locations would yield more generalised results on this topic. Another interesting aspect of this study would be to investigate if there is a difference between variables such as age or gender when it comes to online privacy.

This study found that while users were worried about their data, and though they feel they have a greater knowledge of how their data is used online, the vast majority of respondents still fail to read the company's privacy policy to understand and accept the company's intention to use or sell their data. With the privacy policy now being a necessary component to accept prior to visiting the site an interesting study would be to understand if more people are now reading this since its introduction, or simply accepting the terms to continue to the site. An interesting area of future study that has been highlighted from this research would be to take a closer look at privacy policies themselves. Budak et.al. (2019) carried out an interesting study surrounding this topic, however it found that it was too early to see the true effect of laws introduced by the

GDPR requiring privacy policies. Now, over 3 years after the introduction of GDPR laws into Ireland would be an important time to continue this study into privacy policies to see if they have impacted how secure people are online, or if people are simply accepting all policies to continue to use the site.

This dissertation focused on how much privacy employees have online and in the workplace and are employees more aware of how their data is used when working in the Ecommerce sector. Future studies could consider the limitations of this study, the factors that constrained this research and develop new methods based on the data findings from this study and recommendations offered.

5.8 Recommendations

It is clear from the findings of this research that online privacy is a cause for concern for internet users. Users need to be aware of the risks associated with the amount of data willingly shared online, such as identity theft and data breaches. The increased use of LinkedIn by recruiters also means that more of what is shared by users online can be easily accessed by their current or potential employers. This led the researcher to question not only if users themselves are doing enough to protect their data, but also if the social networking sites and online retailers are doing enough to protect their users, or are willingly trying to deceive its users by using elongated privacy policies filled with wordy corporate jargon. This researcher recommends that social networking sites need to evaluate how they currently display their privacy policy, and how they educate their users on data processing. This researcher also recommends the rules of the GDPR be extended to not only ensure sites display their privacy policy, but also to change the policies to short and easy to read pop ups that users can understand.

The findings suggest that while users feel they have somewhat of a greater knowledge around their data online, they still don't feel secure with the use of cookies and don't understand how their data is used. Based off these findings, the researcher recommends more work should be put into privacy policies to make them more understandable. The researcher also recommends that employees who are working in Ecommerce should receive greater training from their organisations on how to protect their data online. This would not only provide them with an

increased awareness so on how to protect their own data online but can also protect the data of their customers.

These online companies need to be more transparent with their customers not only through the privacy policy, but also through the screening of social networking sites. This has become common practice for recruitment and while the results of this study show that users are aware it is being done, many users still fail to protect how much data they share online. Another recommendation would be to make the employee aware if an employer views not only the LinkedIn profile of a potential employee, but also their personal networking. Should this be disclosed, this will reduce friction caused within the workplace by online workplace surveillance.

This researcher recommends that should future work be carried out surrounding this topic, the budget would need to be considered. Many sites such as SurveyMonkey and Laerd Statistics for help with SPSS require paid fees or monthly subscriptions, which was not possible for the researcher. The cost factor would need to be considered particularly when expanding the study to include a wider audience. If future research intended to carry out qualitative research to gain a deeper insight into the employees perspective, a recording device would be needed. This researcher had no such equipment available, and as such had little choice but to use a quantitative research method in the form of the survey.

5.9 Personal Learning Reflection

Throughout this dissertation experience, I have had to overcome many challenges and have learned a number of new skills during the process. I found the experience challenging at times, however extremely rewarding to see the final project come together.

This experience has definitely improved my organisational skill and time management skills. While at the beginning it appeared to be a monumental task in a relatively short space of time I struggled to find where to start, once I broke the work into the different headings and created weekly tasks it became a lot clearer on what needed to be done. I experienced first-hand the importance of keeping a notepad in order to stay organized. This was crucial to success as by

finding similarities and differences between the different research papers, and breaking this down into the different topics to suit my Literature Review I was able to keep on top of the work and ensure the literature was organised. Going forward I will continue to utilize this as I find when undertaking a large task such as this, a notepad works for me remain organised throughout. I also learned to remain flexible throughout the process. While I reviewed a vast amount of literature prior to writing this piece, not all papers could be included or were too outdated for the research. It was also important to remain flexible when the work was not going to plan. I experienced the disappointment of utilising a validation type, Cronbach's Alpha that yielded results below the expected 0.7 to validate the data. This is a learning outcome I will be carrying with me throughout my career as a HR professional, issues such as this will always arise however it is important to accept that issues such as this can happen however they can also be overcome. This issue with the data validation below 0.7 was a limitation in this study, however it does not mean the data cannot be used. To be successful, it was important to always remain mindful of what works and what doesn't, and constantly question why. It was also important for me to stay motivated to find out the answers and to continue with the research even in times such as this when it was not going to plan. I also am more cautious myself when using the internet and now read privacy policies before accepting cookies, or if I do not have the time I only allow functional cookies.

While issues such as this did arise, I am extremely proud with how I overcame each problem that came my way, and how this research piece has evolved. Undertaking this dissertation was an excellent learning opportunity and first-hand learning it has given me will be extremely important as I continue my career in Human Resources.

Chapter 6 : Conclusion

6.1 Conclusion

This research set out to study the area of online privacy from the perspective of employees, particularly those working in the Ecommerce sector. From reviewing the literature it is clear there are a number of concerns users have when it comes to protecting their data online. The rapid advancements in technology in the past number of years has had many advantages for social networking sites such as LinkedIn, however has brought many risks to users who are unaware how their data is being captured and processed online. The research also sought to investigate how employees felt about workplace surveillance not only in the physical workplace, but online also given the rise of LinkedIns' use in the professional setting.

As those working in the Ecommerce sector deal with privacy and data breaches on a daily basis, the aim of the study was to see if they had an increased knowledge into how their data was being used and from this, were more secure online. As mentioned in the methodology section, a web-based survey was the instrument of choice to gather the data for this research as the researcher felt this would gain insight from a wider audience given the time constraints. (Lovekamp et. al., 2017) This proved successful as the 100 responses received yielded a range of insights into how much data users were disclosing online, and also what measures they were using to protect their data. The theoretical framework for this research focused on how much data users were sharing on LinkedIn and were they aware of how this data was being used, and how users felt about their online social media presence being monitored by their employer.

As the existing research around this topic focused primarily on data breaches and privacy online, little has been done to investigate if different professions have more awareness surrounding the topic, and if this changes their behaviour online. The researcher chose the large Ecommerce company Wayfair based in Galway, Ireland as by choosing one company to survey this would

not only ensure consistency throughout the knowledge of the employees from the training they had received, but also provided responses from a varying age group ranging from 21-60 who would all have different experiences when it comes to online security. A pilot study was conducted on ten participants to ensure the survey was understandable and the data was being collected and recorded (Saunders et al., 2012). To ensure reliability the researcher conducted the Cronbach's Alpha test in which not all results were above 0.7, however this is due to the scale being modified to suit this study.

The findings of this study has significant impact not only for online businesses, but also for users of these online platforms. The results of this study shows a correlation between employees working in the Ecommerce sector having a greater awareness of how their data is used online, however they still continue to share a lot of personal information online. The results also show that while the employees work for an Ecommerce company, it does not ease their concerns about how their data is processed and used online. Online social platforms and retailers need to be more transparent when it comes to how they are using and processing data. Privacy policies should be easier to read and understand, so that more users can make informed decisions when accepting or declining the policies. Barth, et. al. (2019) discussed the worrying lack of knowledge users have when it comes to disclosing their data online, and the results of that are mirrored in this survey. Users need to be more informed in order to protect themselves online. Sindermann et al. (2021) stated that a lack of knowledge in how online data is used leads to data breaches and identity theft as users share too much information online.

This study did face some limitations such as the time restraint which meant that this study only surveyed one company, rather than a range of different Ecommerce organisations. It must be stated that the findings of this study represent employees in one Ecommerce organisation in Ireland, rather than all employees working for Ecommerce organisations. Regardless of the limitations, this study provides a valuable insight from the perspective of employees into their knowledge and feelings towards protecting their data online. The findings suggest that employees feel not only are their LinkedIn profiles being screened, but this process has now moved to screening personal networking sites also. Jeske, Lippke and Shultz (2019) found that the more common this practice becomes, the more people will alter their online persona. Based

on the data that has been examined and analysed the researcher suggests more should be done to educate people on protecting their data online. The researcher also finds that further training should be provided to those in the Ecommerce sector so that they can not only deal with security threats at work but can also protect themselves when it comes to sharing their data online.

Reference List

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015) 'Privacy and human behaviour in the age of information', *Science*, 347(6221), pp. 509–514. Available at: <http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=edsjsr&AN=edsjsr.24745782&site=eds-live&scope=site> (Accessed: 31 March 2021).

Adhikari, K. and Panda, R. K. (2018) 'Users' Information Privacy Concerns and Privacy Protection Behaviours in Social Networks', *Journal of Global Marketing*, 31(2), pp. 96–110. doi: 10.1080/08911762.2017.1412552.

Adunlin, G. *et al.* (2021) 'Using the protection motivation theory to examine the effects of fear arousal on the practice of social distancing during the COVID-19 outbreak in rural areas', *Journal of Human Behaviour in the Social Environment*, 31(1–4), pp. 168–172. doi: 10.1080/10911359.2020.1783419.

Agrawal, A., Fruehauf, S., Hester, L., Ignatova, M. Lee Cruz, E., and Schnidman, A. (2016), 2016 Global Talent Trends – Data on How Candidates Want to Be Recruited, LinkedIn, available at: <http://business.linkedin.com/content/dam/me/business/en-us/talent-solutions/resources/pdfs/2016-global-talent-trends-v4.pdf> (accessed 1 August 2021).

Allen, A.L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. New Jersey: Rowman & Littlefield.

Altman, I., (1978). *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. *Contemporary Sociology*, 7(5), p.638.

Aminilari, M., Hassanian-Esfahani, R. and Miremadi, A. (2013). A new trust model for B2C e-commerce based on 3D user interfaces, in: 7th International Conference on eCommerce in Developing Countries: With Focus on e-Security (ECDCC), 2013. IEEE, pp. 1–12.

Aramo-Immonen, H., Jussila, J. J. and Kärkkäinen, H. (2014) 'Social media utilization in business-to-business relationships of technology industry firms', *Computers in Human Behavior*, 30, pp. 606–613. doi: 10.1016/j.chb.2013.07.047.

Banerji, D. and Reimer, T. (2019) 'Startup founders and their LinkedIn connections: Are well-connected entrepreneurs more successful?', *Computers in Human Behavior*, 90, pp. 46–52. doi: 10.1016/j.chb.2018.08.033.

- Barth, S. et al. (2019) 'Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources', *Telematics & Informatics*, 41, pp. 55–69. doi: 10.1016/j.tele.2019.03.
- Beldad, A., de Jong, M. and Steehouder, M. (2011) 'A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet', *Information Society*, 27(4), pp. 220–232. doi: 10.1080/01972243.2011.583802.
- Benson, V., Saridakis, G. and Tennakoon, H. (2015) 'Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?', *Information Technology & People*, 28(3), pp. 426–441. doi: 10.1108/ITP-10-2014-0232.
- Bernoff, J. and Schadler, T., (2010). *Empowered*. Boston, Mass.: *Harvard Business Review*.
- Black, S.L., Johnson, A.F. and Stone, D.L. (2015), "Use of social networking websites on applicants' privacy", *Employee Responsibilities and Rights Journal*, Vol. 27 No. 2, pp. 115-159.
- Bohmova, L. (2016) 'The Use of Social Media in the Recruitment Process', *FAIMA Business & Management Journal*, 4(2), pp. 20–30. Available at: <http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=116220277&site=ehost-live> (Accessed: 19 January 2021).
- Bornschein, R., Maier, E and Schmidt, L. (2020) 'The effect of consumers' perceived power and risk in digital information privacy: The example of cookie notices', *Journal of Public Policy & Marketing*, 39(2), pp. 135–154. doi: 10.1177/0743915620902143.
- Brandeis, L. D. and Warren, S.D. (1890) *The Right to Privacy*, 4 *Harvard Law Review*. pp. 193,195.
- Branscomb, A. (1994). *Who Owns Information?: From Privacy To Public Access*. New York, Basic Books.
- Breckenridge, K. (2020) 'Capitalism without Surveillance?', *Development & Change*, 51(3), pp. 921–935. doi: 10.1111/dech.12588.
- Brown, M. and Dent, C. (2017) 'Privacy Concerns over Employer Access to Employee Social Media', *Monash University Law Review*, 43(3), pp. 796–827. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=a9h&AN=129760268&site=ehost-live> (Accessed: 25 May 2021).
- Bryman, A. (2012). *Social Research Methods*. 5th ed. Oxford, UK: Oxford University Press.
- Budak, J, Rajh, E. and Škrinjarić, B. (2019) 'Perceived quality of privacy protection regulations and online privacy concern', *Economic Research-Ekonomska Istrazivanja*, 32(1), pp. 982–1000. doi: 10.1080/1331677X.2019.1585272.

Budhwar, P. S., Gillani, A. and Kutaula, S. (2020) 'An analysis of employment relationships in Asia using psychological contract theory: A review and research agenda', *Human Resource Management Review*, 30(4). doi: 10.1016/j.hrmr.2019.100707.

Buocz, T. *et al.* (2019) 'Bitcoin and the GDPR: Allocating responsibility in distributed networks', *Computer Law & Security Review*, 35(2), pp. 182–198. doi: 10.1016/j.clsr.2018.12.003.

Cappel, J. J., Shah, V. and Verhulsdonck, G. (2020) 'Perceptions of Online Privacy', *Journal of Business & Educational Leadership*, 10(1), pp. 122–133. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=148175915&site=ehost-live> (Accessed: 1 August 2021).

Casiglia, S. (2021), 'Covert Video Surveillance in the Workplace Does Not Violate Article 8 ECHR in the López Ribalda Case', *Journal of Internet Law*, vol. 24, no. 7, pp. 3–11, viewed 27 May 2021, <<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=149860679&site=ehost-live>>.

Chang, S. E., Lin, S. and Liu, A. Y. (2015) 'Exploring privacy and trust for employee monitoring', *Industrial Management & Data Systems*, 115(1), pp. 88–106. doi: 10.1108/IMDS-07-2014-0197.

Chang, S. E., Liu, A. Y. and Shen, W. C. (2017) 'User trust in social networking services: A comparison of Facebook and LinkedIn', *Computers in Human Behavior*, 69, pp. 207–217. doi: 10.1016/j.chb.2016.12.013.

Chorpash, J. (2020) 'Do You Accept These Cookies? How the General Data Protection Regulation Keeps Consumer Information Safe', *Northwestern Journal of International Law & Business*, 40(2), pp. 227–249. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=142291750&site=ehost-live> (Accessed: 19 May 2021).

CIPD (2013) Pre-employment checks: an employer's guide. Available at: <http://www.cipd.co.uk/hr-resources/guides/pre-employment-checks.aspx> (accessed 27 May 2021).

Clark, L. A., and Roberts, S. J. (2010). Employer's use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics*, 95(4), 507–525.

Clayton, M. J., Dae-Hee, K. and Hettche, M. (2015) 'The Privacy Paradox and Calculus Among Millennials: An Empirical Study of Privacy Attitude-Behavior Congruence', *AMA Marketing & Public Policy Academic Conference Proceedings*, 25, pp. 84–86. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=119960827&site=ehost-live> (Accessed: 11 August 2021).

Collis, J. and Hussey, R. (2009) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, 3rd Edition. Houndsmills, Basingstoke: Palgrave Macmillan.

Constantinou, E., Melanthiou, Y. and Pavlou, F. (2015) 'The Use of Social Network Sites as an E-Recruitment Tool', *Journal of Transnational Management*, 20(1), pp. 31–49. Available at: <http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoah&AN=34929251&site=ehost-live> (Accessed: 21 January 2021).

Cooley, D. and Parks-Yancy, R. (2018) 'Who gets the job? First-generation college students' perceptions of employer screening methods', *Journal of Education for Business*, 93(1), pp. 1–10. doi: 10.1080/08832323.2017.1409691.

Cowan, M., Craddock, L., and Stevens, S. (2021) 'Data sharing, international property practices and the GDPR: communicating with your consumers', *Property Management*, 39(1), pp. 22–33. doi: 10.1108/PM-05-2020-0033.

Cox, A., Li, X., and Wang, Z. (2018) 'How do social network sites support product users' knowledge construction? A study of LinkedIn', *Online Information Review*, 42(3), pp. 304–323. Available at: <http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoah&AN=45465175&site=ehost-live> (Accessed: 21 January 2021).

Craddock, L. and Gregory, M. (2016), "Racing to the future: security in the gigabit race?", in Kommers, P., Issa, T., McKay, E. and Isaias, P. (Eds), *Proceedings of the International Conferences on Internet Technologies and Society 2016 (ITS 2016), Educational Technologies 2016 (ICEduTech 2016) and Sustainability, Technology and Education 2016 (STE 2016)*, IADIS Press, pp. 263-266.

Creswell, J.W. (2009) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. London: Sage Publications Inc.

Das, G. *et al.* (2018) 'Privacy Policies for Apps Targeted Toward Youth: Descriptive Analysis of Readability', *JMIR mHealth and uHealth*, 6(1), p. e3. doi: 10.2196/mhealth.7626.

DeMaria, A., Magee, S. and Sullivan, K., (2016). Employees Have Right to Be Disloyal and Use Vulgarity in Social Media Posts About Their Employer. *Management Report for Nonunion Organizations*, 39(1), pp.1-8.

Demuth, C. and Terkildsen, T. (2015) 'The future of qualitative research in psychology—A discussion with Svend Brinkmann, Günter Mey, Luca Tateo, and Anete Strand', *Integrative Psychological & Behavioral Science*, 49(2), pp. 135–161. doi: 10.1007/s12124-015-9297-3.

Dhir, A. *et al.* (2021) 'The dark side of social media: Stalking, online self-disclosure and problematic sleep', *International Journal of Consumer Studies*. doi: 10.1111/ijcs.12659.

Donegan C., Rothschild P.C. and Thomas SL. (2014) Social networking, management responsibilities, and employee rights: the evolving role of social networking in employment

decisions. *Employee Responsibilities and Rights Journal*. Available at: <http://link.springer.com/article/10.1007/s10672-014-9250-5> (accessed 27 May 2021).

Dowding, K. (1987) 'Freedom of Speech (Book)', *Political Studies*, 35(3), p. 530. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=a9h&AN=14145831&site=ehost-live> (Accessed: 25 May 2021).

Dudovskiy, J. (2018). Research Philosophy. [online] research-methodology.net. Available at: <https://research-methodology.net/research-philosophy/> [Accessed 15 Jun. 2021].

Eddy, N. (2012) 'Facebook, LinkedIn Changing Employee-Recruitment Methods: Report', *eWeek*, p. 3. Available at: <http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=91662290&site=ehost-live> (Accessed: 21 January 2021).

Flinchum, J. R., Kruse, L. M., and Norris, D. R. (2018) 'Social Media as a Public Sphere? Politics on Social Media', *Sociological Quarterly*, 59(1), pp. 62–84. doi: 10.1080/00380253.2017.1383143.

Ford, D. G. and Ludlum, M. (2016) 'Employee Privacy outside the Workplace', *Southern Law Journal*, 26(2), pp. 321–344. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=a9h&AN=120614616&site=ehost-live> (Accessed: 25 May 2021).

Fowler, E. (2019), "AMP contractor gets community service for data theft, financial review", March 21, 2019, available at: <https://www.afr.com/companies/financial-services/amp-contractor-gets-community-service-for-data-theft-20190321-p516a1> (Accessed 19 May 2021).

Fox, A. K. and Royne, M. B. (2018) 'Private Information in a Social World: Assessing Consumers' Fear and Understanding of Social Media Privacy', *Journal of Marketing Theory & Practice*, 26(1/2), pp. 72–89. doi: 10.1080/10696679.2017.1389242.

Gabisch, J. A. and Milne, G. R., (2014) "The Impact of Compensation on Information Ownership and Privacy Control." *Journal of Consumer Marketing* 31 (1): 13–26.
GDPR (2020). *Cookies, the GDPR, and the ePrivacy Directive - GDPR.eu*. [online] Available at: <https://gdpr.eu/cookies/> [Accessed 3 June 2021].

Gillespie, M. D., Lovekamp, W. E. and Soboroff, S. D. (2017) 'Engaging Students in Survey Research Projects across Research Methods and Statistics Courses', *Teaching Sociology*, 45(1), pp. 65–72. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eric&AN=EJ1124274&site=ehost-live> (Accessed: 30 June 2021).

Grannis, A. (2015) 'You Didn't Even Notice! Elements of Effective Online Privacy Policies', *Fordham Urban Law Journal*, 42(5), pp. 1109–1170. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=a9h&AN=120822604&site=>

Gray, J.R. (2017). Qualitative research methods. In J.R. Gray, S.K. Grove, & S. Sutherland (Eds.), *Burns and Grove's the practice of nursing research: Analysis, synthesis, and generation of evidence* (8th ed., pp. 251-283). St. Louis, MO: Elsevier.

Greene, P. (2013) *Online Trust : An Investigation into the Privacy Attitudes and Awareness of Social Network Users in Ireland*. Masters thesis, Dublin, National College of Ireland.

Heyman, R. and Pierson, J. (2011) 'Social media and cookies challenges for online privacy', *Info*, 13(6), pp. 30–42. Available at:

<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoh&AN=25853947&site=eohost-live> (Accessed: 19 May 2021).

Hideyuki Yokoyama, M (2016), 'How Social Network Sites (SNS) Have Changed the Employer-Employee Relationship and What Are the Next Challenges for Human Resource (Hr)?', *REGE Revista de Gestão*, vol. 23, no. 1, pp. 74–85, (Accessed 22 January 2021), <<http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=115496186&site=eohost-live>>.

Huemer, M. (2018) 'The virtues of direct realism', in Smythies, J. and French, R. (eds) *Direct versus indirect realism: A neurophilosophical debate on consciousness*. San Diego, CA: Elsevier Academic Press, pp. 95–112. doi: 10.1016/B978-0-12-812141-2.00007-6.

Imai, K., Rosenfeld, B. and Shapiro, J. N. (2016) 'An Empirical Validation Study of Popular Survey Methodologies for Sensitive Questions', *American Journal of Political Science* (John Wiley & Sons, Inc.), 60(3), pp. 783–802. doi: 10.1111/ajps.12205.

Jeske, D., Lippke, S. and Shultz, K. S. (2019) 'Predicting Self-Disclosure in Recruitment in the Context of Social Media Screening', *Employee Responsibilities & Rights Journal*, 31(2), pp. 99–112. doi: 10.1007/s10672-019-09329-8.

Jeske, D. and Shultz, K. S. (2016) 'Using social media content for screening in recruitment and selection: Pros and cons', *Work, Employment and Society*, 30(3), pp. 535–546. doi: 10.1177/0950017015613746.

Jones, B. (2020) *Understanding ecommerce consumer privacy from the behavioral marketers' viewpoint*, *Dissertation Abstracts International: Section B: The Sciences and Engineering*.

ProQuest Information & Learning. Available at:

<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=psych&AN=2020-04050-201&site=eohost-live> (Accessed: 4 June 2021).

Jozani, M. *et al.* (2020) 'Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective', *Computers in Human Behavior*, 107. doi: 10.1016/j.chb.2020.106260.

Kapczynski A., (2020) 'The Law of Informational Capitalism', *Yale Law Journal*, 129(5), pp. 1460–1515. Available at:

<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=142547988&site=ehost-live> (Accessed: 28 May 2021).

Kaul, R. (2019) 'A Contemporary Analysis of Online Privacy & Data Protection in the context of Parallel Privacy Policies', *Scholedge International Journal of Management & Development*, 6(5), pp. 67–70. Available at:
<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=138064047&site=ehost-live> (Accessed: 1 August 2021).

Kim, K. and Kim, J. (2011) 'Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust', *Journal of Interactive Marketing*, 25(3), pp. 145–158. doi:
10.1016/j.intmar.2010.09.003.

Kokolakis, S. (2017). "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64: 122–134.

Koohang, A. (2017) 'Social media sites privacy concerns: Empirical validation of an instrument', *Online Journal of Applied Knowledge Management*, 5(1), pp. 14–26. doi:
10.36965/ojakm.2017.5(1)14-26.

Krämer, N. C. and Schäwel, J. (2020) 'Mastering the challenge of balancing self-disclosure and privacy in social media', *Current Opinion in Psychology*, 31, pp. 67–71. doi:
10.1016/j.copsyc.2019.08.003.

Kroc, E., Olvera Astivia, O. L., and Zumbo, B. D. (2020) 'The Role of Item Distributions on Reliability Estimation: The Case of Cronbach's Coefficient Alpha', *Educational and Psychological Measurement*, 80(5), pp. 825–846. Available at:
<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eric&AN=EJ1263670&site=ehost-live> (Accessed: 5 August 2021).

Kroll, T. and Stieglitz, S. (2021) 'Digital nudging and privacy: improving decisions about self-disclosure in social networks', *Behaviour & Information Technology*, 40(1), pp. 1–19. Available at:
<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoah&AN=55222198&site=ehost-live> (Accessed: 11 August 2021)

Krishnamoorthy, D. and Vigram, R. P. (2020) 'A study on website quality and its impact on customer satisfaction with reference to ecommerce companies', *Journal of Contemporary Issues in Business & Government*, 26(2), pp. 888–895. doi: 10.47750/cibg.2020.26.02.126.

Landers, R. N., and Schmidt, G. B. (2015). *Social media in employee selection and recruitment theory, practice, and current challenges*. Geneva, Switzerland: Springer.

Levashina, J. and Roulin, N. (2019) 'LinkedIn as a new selection method: Psychometric properties and assessment approach', *Personnel Psychology*, 72(2), pp. 187–211. doi:
10.1111/peps.12296.

- Levin, A. V. (2021) ‘What’s in a “Welcome Survey”?’ Designing a Course Welcome Survey as Introduction to Research Methods in Communication’, *Communication Teacher*, 35(2), pp. 98–103. Available at:
<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eric&AN=EJ1288955&site=ehost-live> (Accessed: 11 August 2021).
- Lewis, P., Saunders, M. and Thornhill, A. (2009) *Research Methods for Business Students*, Fifth ed., Harlow: *Financial Times*, Prentice Hall.
- Lu, Y. and Pan, T. (2019) ‘The Effect of Employee Participation in Enterprise Social Media on Their Job Performance’, *IEEE Access*, 7(1), pp. 137528–137542. Available at:
<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoah&AN=51108849&site=ehost-live> (Accessed: 11 August 2021).
- Li, H. and Zhou, T. (2014) ‘Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern’, *Computers in Human Behavior*, 37, pp. 283–289. doi: 10.1016/j.chb.2014.05.008.
- Maddux, J. E., and Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. doi:10.1016/0022-1031(83)90023-9.
- Mahmoodi, J. *et al.* (2018) ‘Internet users’ valuation of enhanced data protection on social media: Which aspects of privacy are worth the most?’, *Frontiers in Psychology*, 9. doi: 10.3389/fpsyg.2018.01516.
- Martin, K. (2020) ‘Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms’, *Business Ethics Quarterly*, 30(1), pp. 65–96. doi: 10.1017/beq.2019.24.
- Mohamed, A.A. (2010) 'Online Privacy Concerns Among Social Networks' Users'. *Cross-Cultural Communication*, Volume 6(4): 74-89.
- Montoya-Vargas, J., Parra, J. D. and Said-Hung, E. (2021) ‘(Re)introducing Critical Realism as a Paradigm to Inform Qualitative Content Analysis in “Causal” Educational Research’, *International Journal of Qualitative Studies in Education (QSE)*, 34(2), pp. 168–182. Available at:
<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eric&AN=EJ1287731&site=ehost-live> (Accessed: 16 June 2021).
- Moosa, I. A. (2019) ‘The fragility of results and bias in empirical research: an exploratory exposition’, *Journal of Economic Methodology*, 26(4), pp. 347–360. doi: 10.1080/1350178X.2018.1556798.
- O’Brien, C., (2021). *Covid-19 pushes more people to buy goods, services online*. [online] The Irish Times. Available at: <<https://www.irishtimes.com/business/retail-and-services/covid-19-pushes-more-people-to-buy-goods-services-online-1.4387224>> [Accessed 1 April 2021].

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

Orange, M. (2019) 'How Free Is Too Free?', *Virginia Quarterly Review*, 95(2), pp. 156–159.

Available at:

<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=a9h&AN=136923879&site=ehost-live> (Accessed: 27 May 2021).

Oyserman, D. and Schwarz, N. (2020) 'Identity-based motivation and the logic of conversations obfuscate loss of online privacy and what policy-makers can do about it', *Journal of Consumer Psychology*, 30(4), pp. 759–766. doi: 10.1002/jcpy.1189.

Pearce, S. (2017) 'Analytics and privacy', *NZ Business + Management*, 31(5), p. M18. Available at:

<https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=123210567&site=ehost-live> (Accessed: 21 May 2021).

Perkins, O. (2015), "More than half of employers now use social media to screen job candidates, poll says; even friend requests", available at:

http://www.cleveland.com/business/2015/05/more_than_half_of_employers_no_1.html (accessed 15 August 2021).

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.

Powell, T. C. (2020) 'Can quantitative research solve social problems? Pragmatism and the ethics of social research', *Journal of Business Ethics*, 167(1), pp. 41–48. doi: 10.1007/s10551-019-04196-7.

Quan-Haase, A. and Young, A. L., (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, 16(4), 479– 500. doi:10.1080/1369118X.2013.777757

Quinton, S. and Wilson, D. (2016) 'Tensions and ties in social media networks: Towards a model of understanding business relationship development and business performance enhancement through the use of LinkedIn', *Industrial Marketing Management*, 54, pp. 15–24. doi: 10.1016/j.indmarman.2015.12.001.

Rashidi, M. Z. (2014) 'Praxis and Proficiency in Mixed Methods Research: A Framework for Conceptualizing and Testing Integration of Qualitative and Quantitative Data and Analysis', *Journal of Independent Studies & Research: Management & Social Sciences & Economics*, 12(2), pp. 129–132. Available

at: <http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=117676319&site=ehost-live> (Accessed: 24 January 2021).

Rawlings, E. D. (2020) 'Do you know what's in those cookies? An analysis of the readability of social media cookie policies', *Proceedings of the Association for Information Science and Technology*, 57(1). Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoh&AN=54463149&site=ehost-live> (Accessed: 19 May 2021).

Reger, A. (2013). The impact of the business networking site LinkedIn on private, large, multinational companies' recruitment process in Ireland. Postgraduate. National College of Ireland.

Reio, T. G., Jr. (2007) 'Survey Nonresponse Bias in Social Science Research', *New Horizons in Adult Education & Human Resource Development*, 21(1–2), pp. 48–51. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eric&AN=EJ983865&site=ehost-live> (Accessed: 1 July 2021).

RTE., (2021). *LinkedIn Ireland records three-fold increase in profits*. [online] RTE.ie. Available at: <<https://www.rte.ie/news/business/2020/1129/1181272-linkedin-ireland-records-three-fold-increase-in-profits/>> [Accessed 1 April 2021].

Ryan, G. (2018) 'Introduction to positivism, interpretivism and critical theory', *Nurse researcher*, 25(4), pp. 14–20. doi: 10.7748/nr.2018.e1466.

Sanders, A. K. (2019) 'The GDPR One Year Later: Protecting Privacy or Preventing Access to Information?', *Tulane Law Review*, 93(5), pp. 1229–1253. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=a9h&AN=137020794&site=ehost-live> (Accessed: 19 May 2021).

Security in Depth (2019), "2019 annual report – state of cyber security", available at: <https://img1.wsimg.com/blobby/go/35c0baf2-aefc-46ca-9c76-5431e30e646a/downloads/2019%20State%20of%20Cyber%20Security%20Report.pdf?ver=1586160732816> (accessed 19 May 2021).

Seetharaman, A. *et al.* (2017) 'A Study of the Moderate Growth of Online Retailing (Ecommerce) in the Uae', *Journal of Developing Areas*, 51(4), pp. 397–412. doi: 10.1353/jda.2017.0109.

Shi, D. *et al.* (2018) 'Examining chi-square test statistics under conditions of large model size and ordinal data', *Structural Equation Modeling*, 25(6), pp. 924–945. doi: 10.1080/10705511.2018.1449653.

Sindermann, C. *et al.* (2021) 'Online Privacy Literacy and Online Privacy Behavior – The Role of Crystallized Intelligence and Personality', *International Journal of Human-Computer Interaction*, pp. 1–12. doi: 10.1080/10447318.2021.1894799.

Squicciarini, A.C., Xu, H. & Zhang, X. (2011) 'CoPE: Enabling Collaborative Privacy Management in Online Social Networks'. *Journal of the American Society for Information Science & Technology*, Volume 62(3): 521-534.

Statista. (2021). *Linkedin Users In Ireland 2025* [online] Available at: <<https://www.statista.com/forecasts/1146446/linkedin-users-in-ireland>> [Accessed 24 January 2021].

Statista. (2021). *Number of global social network users 2017-2025* [online] <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/> > [Accessed 28 March 2021].

Sturgis, P. and Luff, R. (2020) 'The demise of the survey? A research note on trends in the use of survey data in the social sciences, 1939 to 2015', *International Journal of Social Research Methodology: Theory & Practice*. doi: 10.1080/13645579.2020.1844896.

Such, J. M. and Rovatsos, M. (2016) 'Privacy Policy Negotiation in Social Media', *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 11(1), pp. 1–29. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoh&AN=38544703&site=ehost-live> (Accessed: 19 May 2021).

Taylor, S. (2014). *Resourcing and Talent Management*. 6th ed. London: Chartered Institute of Personnel and Development.

Temraoui, R. (2017) 'Is your privacy in danger when using social networks? An analysis of the contractual terms and conditions using Multi-Attribute Decision making', *PM World Journal*, 6(11), pp. 1–8. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=bsu&AN=126250293&site=ehost-live> (Accessed: 21 May 2021).

Tucker, C. E. (2014) 'Social Networks, Personalized Advertising, and Privacy Controls', *Journal of Marketing Research (JMR)*, 51(5), pp. 546–562. doi: 10.1509/jmr.10.0355.

University of Lancaster (2016). *Qualitative and Quantitative Research*. [eBook] Lancaster: University of Lancaster. Available at: <https://www.lancaster.ac.uk/media/lancasteruniversity/content-assets/documents/learningskills/quantitativevqualitativeanswers.pdf> [Accessed 16 Jun. 2021].

Utz, S. (2010) Show me your friends and I will tell you what type of a person you are: How one's profile, number of friends, and type of friends influence impression formation on social network sites. *Journal of Computer-Mediated Communication* 15: 314–335.

van Ooijen, I. and Vrabec, H. U. (2019) 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective', *Journal of Consumer Policy*, 42(1), pp. 91–107. doi: 10.1007/s10603-018-9399-7.

Vindrola-Padros, C. *et al.* (2020) 'Carrying Out Rapid Qualitative Research During a Pandemic: Emerging Lessons From COVID-19', *Qualitative health research*, 30(14), pp. 2192–2204. doi: 10.1177/1049732320951526.

Westin, A.F. (1967) *Privacy and Freedom*. New York: Athenaeum.

Wiederhold, B. K. (2018) 'Has the internet killed privacy, or has our definition simply changed?', *Cyberpsychology, Behavior, and Social Networking*, 21(7), pp. 403–404. doi: 10.1089/cyber.2018.29117.bkw.

Zarouali, B. *et al.* (2017) ““Do you like cookies?” adolescents’ skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing’, *Computers in Human Behavior*, 69, pp. 157–165. doi: 10.1016/j.chb.2016.11.050.

Zuboff, S., (1988). *In the age of the smart machine*. Basic Books. Pp. 26-108

Zuboff, S.(2018) The Age of Surveillance Capitalism: The Fight for Human Future at the New Frontier of Power’, *Social Change*, 49(4), pp. 735–738. Available at: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=eoh&AN=51820538&site=ehost-live> (Accessed: 27 May 2021).

Appendices

Appendix A – Consent form with Questionnaire

Consent form

This questionnaire is part of research for a Masters in Human Resource Management at the National College of Ireland.

Consent form:
You are invited to participate in an online survey on the use of LinkedIn in the workplace. This quantitative survey is a part of a research project lead by Elaine Byrne. It should approximately take 5-7 minutes to complete.

Participation:
Your participation is voluntary and honorary. You can refuse to take part in the survey at any given point without any consequences/penalties. You can refuse to answer any any part of the questionnaire and may exit anytime during answering the questionnaire.

Risks and opportunities:
There are no risks involved in this survey as the data collected will be kept in secured devices and will be removed after analysis. The confidentiality of this survey is also ensured by the fact that there will be no collection of email addresses or any other personal details. On the beneficial aspect your opinion and insight will help the researcher gain a valuable market insight in the HR administration field.

Confidentiality:
The survey analysis or submissions will be sent and stored to a link at [form.google.com](https://forms.google.com) which does not collect your personal data such as: Your name, email address or other tracking information (i.e IP address). Your responses will be anonymous and your participation will be kept confidential. This research is conducted solely for scholarly purpose. No further use of the provided data will be used or stored for any future purposes whatsoever and is subject to the consent of the individual.

For any further queries regarding the survey, all questions are to be forwarded to the email address:
x19242336@student.ncirl.ie

By clicking to continue you confirm that

1. You have voluntarily agreed to take part in this research without any expected remuneration.
2. You have read the above information.
3. You are above 18 years.

If you do not wish to proceed you can decline the participation.

[Next](#)

Appendix B – Questionnaire

Questionnaire

Do you have a LinkedIn account? *

- Yes
 No

Have you read the LinkedIn privacy policy? *

- Yes
 No

Do you refrain from posting certain things to your LinkedIn in case it would impact you professionally? *

- Yes
 No

How much personal information do you share on LinkedIn? Tick all that apply *

- Name
 Age
 Email Address
 Home Address
 Phone Number
 Educational details
 Skills or expertise
 Sexual Orientation
 Religious Views
 Political Views

Do you think the information you share on LinkedIn has an impact on recruiters reaching out to you? *

- Yes
- No

Do you agree with recruiters screening potential employees LinkedIn profile prior to reaching out to them? *

- Yes
- No

Approximately how many connections do you have on your LinkedIn profile? *

- 0-50
- 50-100
- 100-150
- 150 +

How comfortable (on a scale of 1-10) do you feel with LinkedIn storing your data and the use of cookies? *

1 2 3 4 5 6 7 8 9 10

Comfortable Uncomfortable

Has your employer ever requested to connect with you via LinkedIn? *

- Yes
- No

If yes, have you accepted them to connect with you? *

- Yes
- No
- Not Applicable

Do you read privacy policies for other sites prior to accepting cookies? *

- Yes
- No

Do you understand how your data is used when captured online? *

- Yes
- No

Do you believe recruiters view your personal social media sites? *

- Yes
- No

Have you used the added security features to restrict what people can see on your profile? *

- Yes
- No

Do you feel as though you have a greater understanding of how your personal data is used online from working in the ecommerce sector? *

- Yes
- No

How important is it to you to control who views your profile online? *

- Extremely Important
- Important
- Neither important or unimportant
- Unimportant
- Extremely unimportant

Do you worry about your privacy and data when using the internet? *

- Yes
- No

[Back](#)

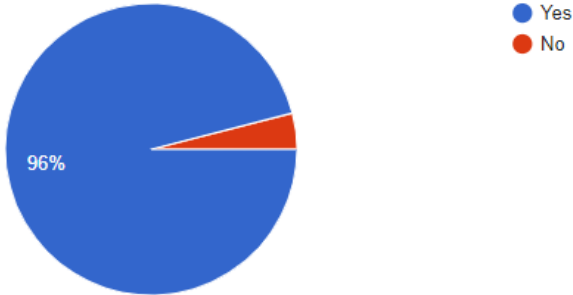
[Submit](#)

Appendix C – Overall Results

Questionnaire

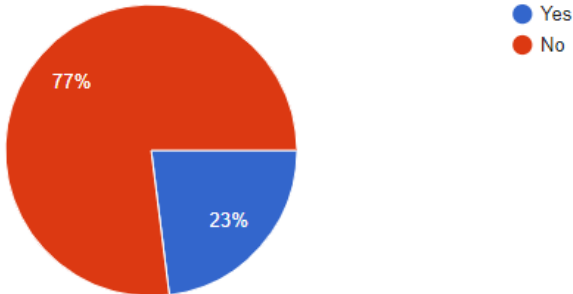
Do you have a LinkedIn account?

100 responses



Have you read the LinkedIn privacy policy?

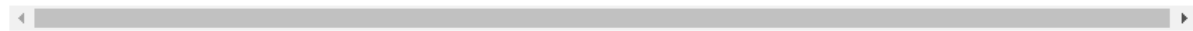
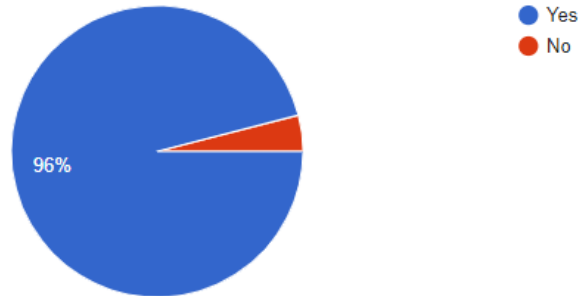
100 responses



Do you refrain from posting certain things to your LinkedIn in case it would impact you professionally?

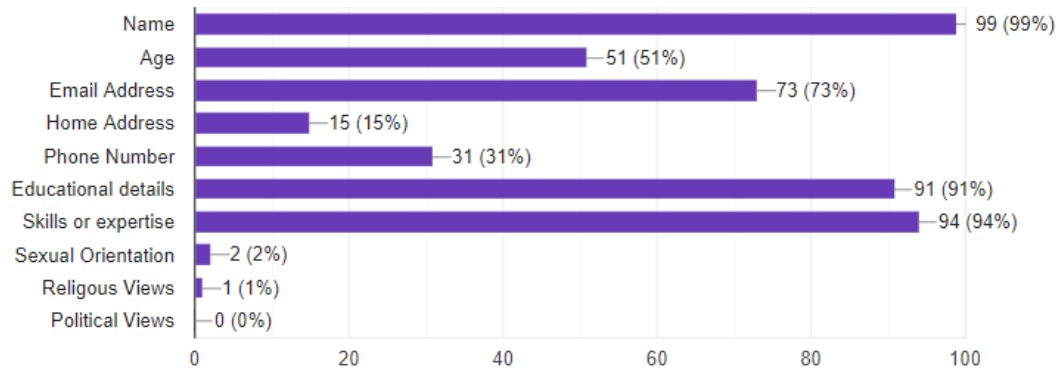


100 responses



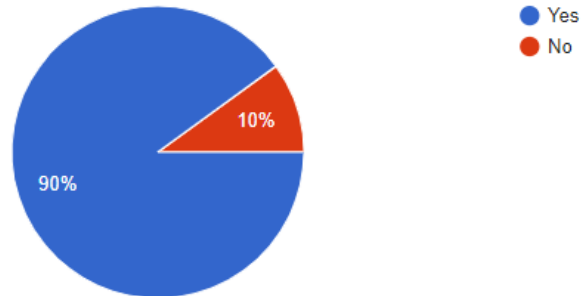
How much personal information do you share on LinkedIn? Tick all that apply

100 responses



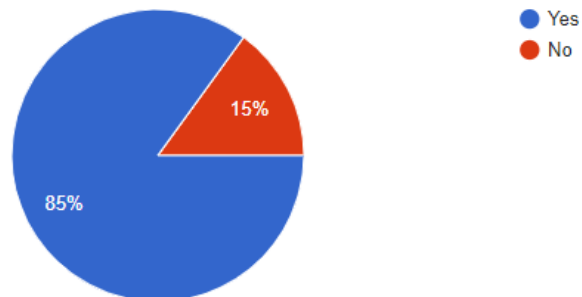
Do you think the information you share on LinkedIn has an impact on recruiters reaching out to you?

100 responses



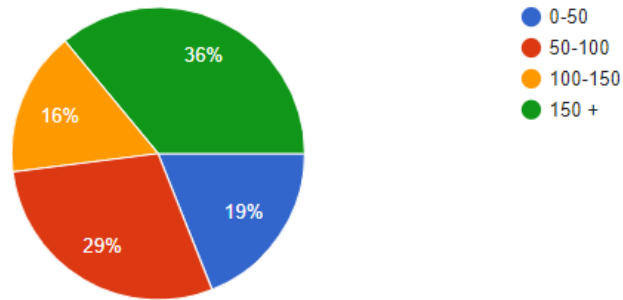
Do you agree with recruiters screening potential employees LinkedIn profile prior to reaching out to them?

100 responses



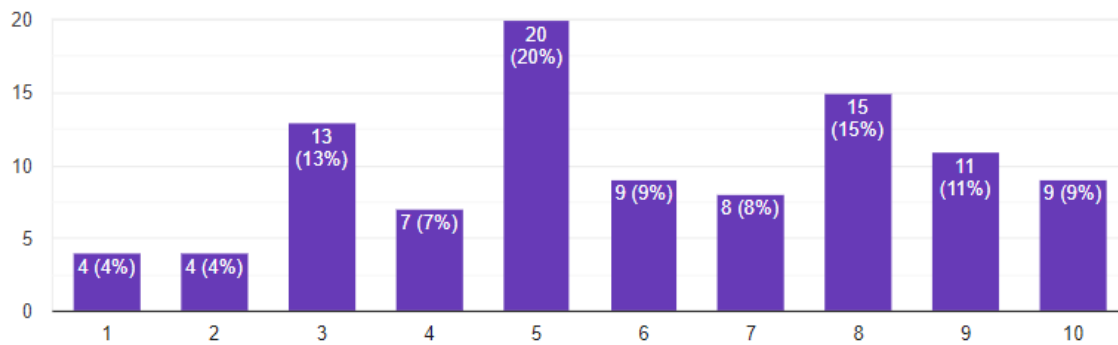
Approximately how many connections do you have on your LinkedIn profile?

100 responses



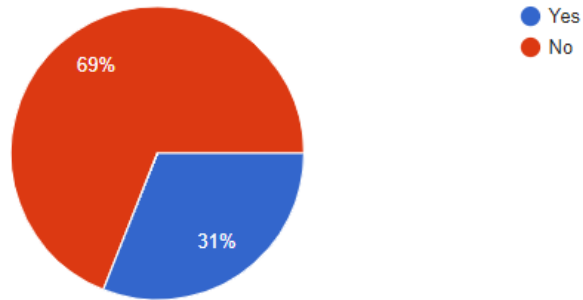
How comfortable (on a scale of 1-10) do you feel with LinkedIn storing your data and the use of cookies?

100 responses



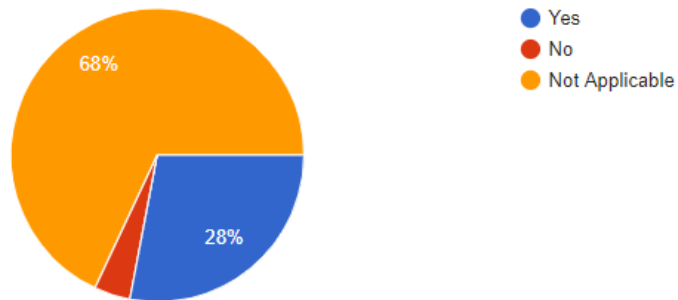
Has your employer ever requested to connect with you via LinkedIn?

100 responses



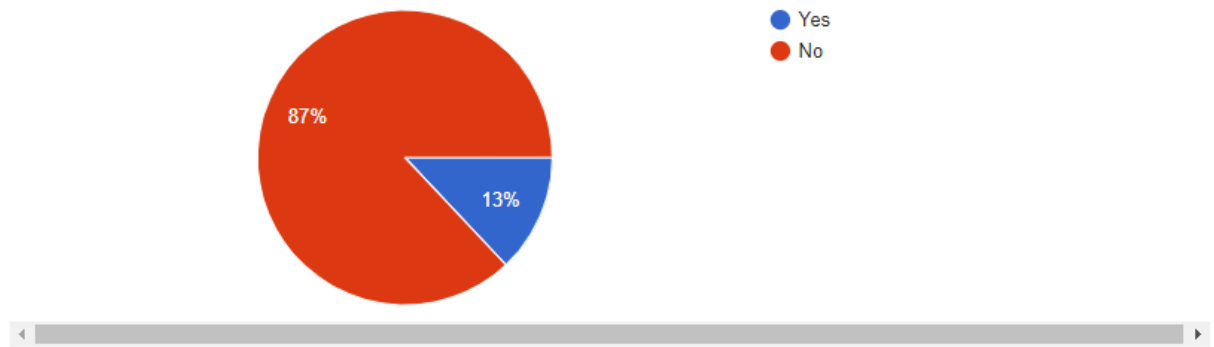
If yes, have you accepted them to connect with you?

100 responses



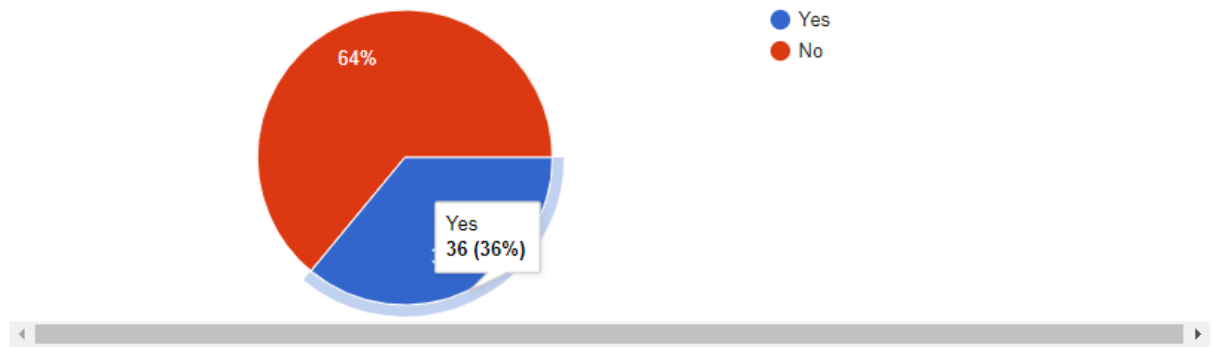
Do you read privacy policies for other sites prior to accepting cookies?

100 responses



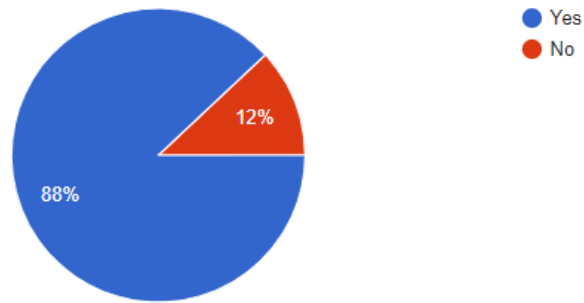
Do you understand how your data is used when captured online?

100 responses



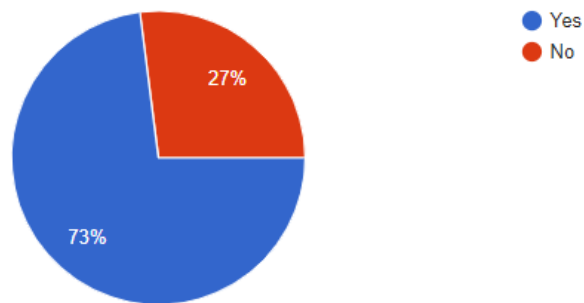
Do you believe recruiters view your personal social media sites?

100 responses



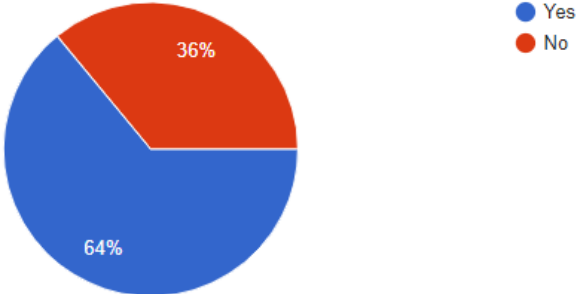
Have you used the added security features to restrict what people can see on your profile?

100 responses



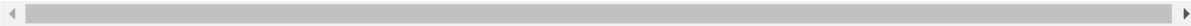
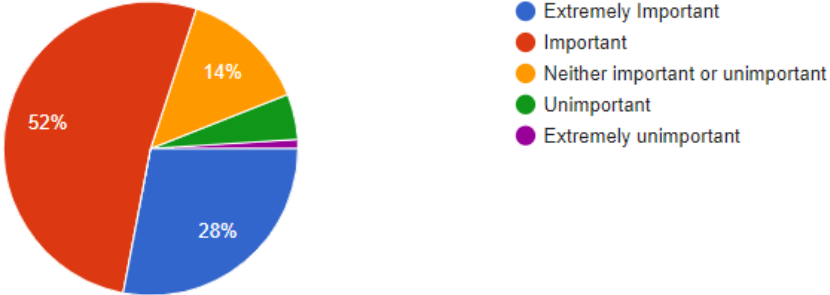
Do you feel as though you have a greater understanding of how your personal data is used online from working in the ecommerce sector?

100 responses



How important is it to you to control who views your profile online?

100 responses



Do you worry about your privacy and data when using the internet?

100 responses

