Exploring the Negotiation of the Boundaries of Internet Privacy

Hayley Evans Finnemore

Thesis Submitted for the Degree of Doctor of Philosophy
School of Social Policy, Sociology and Social Research

September 2020

Word Count: 89,313

Abstract

Contemporary discussions around issues of data privacy tend to focus on the potential for data hacks and stolen identities, however, this is not something that many people will need to deal with. Individuals are much more likely to face issues around 'context collapse' (Vitak, 2012 p.451) and the daily work involved in negotiating the boundaries of internet privacy. Based on 26 interviews and over three-hundred internet surveys, this thesis examines concerns regarding how respondents feel about how much information they share with companies and online as well as their worries in terms of how much control they believe they have. I demonstrate how concerns tend to be around the contextual nature of privacy (Nissenbaum, 2010), in particular the type of information being shared and who it is being shared with. I make particular use of Raynes-Goldie's categorisations of privacy in terms of whether it is 'social' or 'institutional privacy' (p.81), as well as Floridi's (2005) categorisations of 'arbitrary' and 'ontic' (p.197/8) information.

Today, many believe they have little control over what happens to their data, however that is not to say that they have given up and I argue that small acts of 'evasion' and 'subversion' (Fiske, 1989 p.2) are employed to avoid sharing information when people do not want to. While these 'tactics' (de Certeau, 1988 p.185) can feel empowering to those employing them, ultimately, withdrawing from social media is not easy, particularly given the way in which it has become part of our daily lives. Eschewing social networking sites completely offers greater inconvenience, and potentially a loss of social connection with friends and family, leading to feelings of ambivalence for those opting to take this action.

Acknowledgements

First and foremost, I owe a debt of gratitude to my participants, who took the time to complete my survey or allow me to interview them, there would be no project without them.

A huge thank you also goes to my supervisors – Dr Vince Miller and Prof Adam Burgess, their support and feedback has been invaluable and has greatly improved my thesis. They were also instrumental in persuading me to continue when I was on the verge of giving up.

I must also thank Sophie Rowland, Emma Pleasant and Mel Lloyd, without whom this journey would have been a lot less fun, and a lot more difficult. Our WhatsApp group chat has been the source of much encouragement and amusement over the last five years. Thank you to my three newest friends.

On a personal note, I would also like to thank my two best friends, Cate Macdonald and Ann Taylor, who were always at the end of a text message, to offer reassurance and remind me that I could do this – even when I didn't believe it.

A special thank you also goes to my parents, Ann and Denis Evans, who, despite not being entirely sure what I'm doing have continued to encourage and support me throughout this journey – I hope I have made them proud.

Lastly, I dedicate this thesis to my husband, Andrew, who has been so patient and supportive throughout the last five years – I cannot thank you enough and I hope you know that I appreciate everything you've done to support me.

On a scale of 1-13, you are definitely an 8.

Table of contents

Introduction

In June 2013, Central Intelligence Agency sub-contractor Edward Snowden released documents regarding covert surveillance being carried out by the US and UK governments on ordinary citizens (Greenwald, et al., 2013) although it was widely reported on at the time, this was not sustained over a longer period. While I was vaguely aware of his claims at the time, I did not become particularly interested until I saw the film Citizenfour, the following year (CitizenFour, 2014), this film offered further details of the claims made by Snowden and his motivation for releasing the data. After I saw this film, I found it surprising that many of my friends and contemporaries did not appear to be interested or concerned by the claims Snowden had made. This caused a feeling of dissonance for me as I began to consider not only the volume of information I shared on social media but how much those around me were also sharing, seemingly without a second thought. When I spoke to people about Snowden's claims, many were unconcerned, citing national security concerns as being valid justification for the collection of information by the government. Whilst I understood this argument, it concerned me that there appeared to be such apathy towards the issues highlighted by Snowden and I began to wonder whether I was alone in my concern regarding this.

Given the apparent lack of interest from those I knew, my interest waned over time, and I gave the issue less thought, although I did reduce my sharing on social media. However, my interest was reignited late one evening in April 2015, when I saw an episode of *Last Week Tonight with John Oliver* which contained an interview with Edward Snowden (Carvell, et al., 2015). While the interview itself

was interesting, what was of particular note was that when people on the street were canvased regarding whether they knew anything about Edward Snowden or his claims, many did not know who he was. Regardless of whether they had heard of him or not, many were not worried about the claims that he had made, or what it meant for their data, however this changed when they were presented with a scenario whereby the government could view intimate pictures they had sent to others. At this point, people became much more concerned and/or angry, feeling that their privacy had been violated. This led me to consider the change in attitude that occurred when discussing specific information rather than the broad (and often abstract) notion of privacy itself. It was from here that I came to formulate the outline of my project and consider ways in which I could examine how individuals feel about their internet privacy.

It will be useful to pause here to briefly explain what I mean by two key phrases which are used throughout this thesis. When I talk about social media privacy, this is our privacy as it relates to social media sites, broadly in terms of information we share with other users of the site (but potentially also with the owners and/or developers of the site). This definition includes sites such as Facebook, Twitter and Instagram. While much of the work in this thesis focuses on social media and our privacy in relation to it, I do not limit myself solely to these sites and so often refer to 'internet privacy'. When I refer to internet privacy, I am talking about an individual's privacy in relation to the information they are often required to share with companies through websites, in order to gain access to a service or product. While this encompasses social media sites (and thus social media privacy), it is not limited to them, and also includes internet banking websites, consumer websites (such as Amazon) and so on. As such, I

employ the phrase internet privacy to encompass all information that we share (whether we know about it or not), when online.

It is important to consider issues such as our internet privacy and how this affects us because our daily lives have evolved and changed to such an extent that we have become accustomed to sharing our information on a daily basis with a multitude of companies, in numerous ways, such as:

- Checking our account balance using online banking;
- Updating our status on social media;
- Accessing and amending our tax details online;
- Applying for a job online.

We carry out various tasks online in the course of a day but have little appreciation of what happens to that information once we have shared it and are often oblivious to the potential repercussions of this. Contemporary concerns regarding data privacy tend to be around online accounts being hacked, or identity theft, however, data collection by commercial companies and sharing on social networking sites are potentially a greater issue. It is difficult to achieve control over the data we share, especially as companies are often able to generate income from collecting and selling information about their customers. Therefore, allowing customers to have more agency over what happens to their data may be detrimental to their business model and the income generated by it. Media advertising campaigns by companies and banks tend to highlight the importance of setting strong passwords to keep our data secure and to ensure that we do not fall victim to any kind of phishing scam or have our identity stolen. This,

however, distracts us from considering what the companies themselves do with the data we share with them. We worry about our Facebook account being hacked and a virus being spread amongst those on our friends list but may not think about what Facebook themselves are doing with that information; who they sell it to and whether we consent to that. We are often oblivious to the vast amount of data that is stored and shared in and between electronic databases, which are updated every time we carry out a task online.

Companies that we have chosen to share our information with (and even those we have not) often know more about us than the people we share our lives with, to the extent that inferences can be made regarding our likes, dislikes and even sexual orientation (although it must be noted that the accuracy of this varies) (Kosinski, et al., 2013). Despite this, we continue to share our information, often complaining and/or making jokes regarding algorithms, and how 'creepy' it is when advertisements appear on our social media feed for items that we have been searching for elsewhere. This suggests that we are complicit in this data collection and either do not mind, or do not care enough about it to take action, but is this the case? The introduction of the General Data Processing Regulation 2018 (GDPR 2018) and Data Protection Act 2018 (DPA 2018) offer individuals the opportunity to have some autonomy regarding their information and who they share it with. However, it is unclear whether this has happened or whether it merely served to confuse people as they received numerous GDPR notices prior to the introduction of the legislation which many felt unable to deal with effectively (Kelion, 2018).

When I began working on my project (in 2015), contemporary concerns were around the Investigatory Powers Bill/Act and what it might mean for individuals' data privacy. Concerns at this time were focused on the potential for Internet Service Providers to retain people's internet browsing history and how this may cause issues, depending on what sites an individual had been searching for and accessing. The Investigatory Powers Act 2016 (IPA 2016), was introduced in 2016 and extended the reach of surveillance in a number of areas (Travis, 2015). However, in 2018, judges in the UK high court ruled that the IPA 2016 breached EU law and ordered the UK government to make amendments within six months (Cobain, 2018). In October 2018, the government introduced the Data Retention and Acquisition Regulations 2018 (DRAR 2018), which dealt with the issues raised previously and reduced police powers in terms of when they could obtain information. It should be noted that the successful legal challenge against the IPA 2016 was crowd-funded by the civil rights group Liberty (Cobain, 2018), suggesting that individuals are not necessarily passive when considering their privacy and the information they share. This sequence of events belies the general belief that people's concerns are focused on ensuring that they do not say something potentially damaging on social media (Ronson, 2015) and suggests that we are invested in our privacy. Rather than individuals being unconcerned about their privacy, it is more likely that the potential for inaction arises due to the difficulty involved in gaining more control over our data. As noted above, it is not necessarily something that companies are in favour of, fearing a reduction in profits, if customers learn more about what happens to their information and as a result, withdraw their consent. It is also important to recognise that using the internet and sharing information in order to complete mundane daily tasks has become a habit which is difficult, if not impossible to break. We strive to make

our daily lives more convenient, especially if it reduces the amount of time we spend on necessary but boring tasks (Wu, 2018). Therefore, if gaining control over our data leads to reduced convenience, it may be deemed too high a price to pay for many. This is part of the reason that negotiating internet privacy can be particularly complex; we may want more control over our data, but not necessarily if it means that our lives become more difficult as a result.

The introduction of the GDPR 2018 and DPA 2018 suggests that the government is attempting to take action in a bid to restrict the actions of social media, as well as the sharing of data between companies, which individuals may not be aware of. It potentially offers us the opportunity to take back some control and have greater autonomy regarding what companies can do with our information. This can also be seen in the action being taken against Facebook in the wake of the Cambridge Analytica scandal in terms of fines that have been issued (BBC News, 2018a). At this stage however, it is too soon to be able to draw conclusions regarding the impact this has had on individuals' autonomy or their attitudes regarding their data privacy. My research, however, took place before these events and as such was carried out in the wake of Edward Snowden's claims regarding the covert collection of data by the US and UK governments (Greenwald, et al., 2013) in fact this is the event that sparked my interest in attitudes towards data privacy initially, as discussed previously. On the surface, it appeared that people were simply not concerned or interested, and suggested that privacy is not important to people, however, as I will demonstrate throughout this thesis, this is not the case, and this topic is much more complicated than it seems. This can be seen if we consider the impact context can have in terms of the type of information we are being asked to share in a given situation. There are likely to be certain pieces of

information that an individual would not mind sharing, while a different item may elicit greater anxiety. The type of information being requested makes a difference to the person being asked for it, for a number of reasons, however that is not to say that the type of information is the only factor here, and who the information is going to be shared with will also play a role. Therefore, contextual issues affect an individual's decision regarding whether to share information or not. It is important to point out that an individual's willingness to share some information with some audiences cannot be taken as a proxy for their sharing behaviour for different information being shared under different circumstances.

Research area

My thesis aims to gain a greater understanding of how individuals feel about their privacy in terms of the information they are asked to share online and with various companies. It explores this by considering how individuals negotiate their internet privacy, with particular focus on the role that context plays.

I aim to explore issues that are fundamental to people when they consider their privacy and the extent to which they feel they have control in these situations. This is a difficult area to explore and much has been written regarding the sharing that takes place on social networking sites. However, where my thesis differs and offers an original contribution is in my consideration of companies that we are often required to share information with, in addition to sharing that occurs on social media. This offers a different lens through which to consider how much choice we can truly have regarding whether to share our information or not. It also offers a deeper examination of the consideration made when people share

information on social networking sites. Previous research has tended to focus on concerns regarding other social media users' perceptions and how people attempt to hide or share information with other users (Nippert-Eng, 2010 and boyd, 2014), there has been little research into concerns regarding what the sites themselves do with users' data.

I am also interested to discover how individuals behave in situations whereby they are asked or required to share information that they are uncomfortable sharing. This raises questions regarding whether people share the information regardless of concerns they have or employ tactics whereby they attempt to withhold the information while still gaining access to the service they require. While some will share the information regardless of concerns, others may choose to either provide false information, which bears no relation to the actual data or refuse to share the information even if it means utilising a different service provider. This highlights the limited but often creative ways in which people exercise control over sharing (or not) information.

Counter to the commonly held belief that we are living in a post-privacy age, whereby those utilising social media or online companies do not consider or care about the implications of sharing information, I will demonstrate the nuanced nature of privacy, in particular considering the role that context plays. As such, I will highlight the impact that type of information being requested can have on levels of concern. Furthermore, the role of audience will also be considered and as such, the same piece of information can be considered to be problematic or of little concern, depending upon who is asking to see it. This is an area in which I am offering an original contribution in that previous research has seldom

considered the implications of the type of information being requested or the audience for that information. Therefore, I am offering the first in-depth exploration of the issue of context with regard to internet privacy, which will provide a foundation for future work to build upon.

Chapter summary

My thesis will be separated into five main chapters, with a conclusion drawn at the end. I will now provide a brief summary of each chapter.

Chapter One: Literature Review

This chapter will consider problematic nature of the public/private divide as well highlighting the difficulties involved in defining privacy itself.

The main discussion centres around the key issue of commercial surveillance, as this is the focus of my thesis. I will examine issues around how much control individuals can be said to have in terms of the data that is collected about us on a daily basis. This will be dealt with in terms of how companies commodify and aggregate the information they have collected to serve their own ends. It will also consider how we are persuaded to share information with companies and whether users can be said to be exploited in the current situation. Finally this chapter considers the importance of context in terms of the impact that the type of information has on how concerned people are when being asked to share data. There will also be a brief consideration of the effect that the type of audience has on concern levels. This chapter will highlight the research previously carried out in my area of interest, and how it offers a foundation for my project.

Chapter Two: Methods

Here I will provide details of my methodological approach, in particular my rationale for utilising a qualitative approach. I will consider the merits as well as the design process involved in the production of my interviews and surveys and highlight the relevance of the vignettes that were utilised in the closing section of my interviews.

My role as researcher will be examined, with particular focus on the interviews and the measures I put in place for the benefit of the participants. This will also include a discussion of the ethical implications of my research and the considerations made in terms of my treatment of participants.

Chapter Three: Standing in the way of control

This is the first of three analysis chapters, which examine the findings of my project. This chapter deals with issues of trust, particularly in terms of companies sharing information with unknown third-parties, after individuals have shared it with them. This is problematic for participants and often leads to a lack of trust in the intentions of the company. I will then examine the level of control individuals feel they have over their data more generally. It is felt that companies attempt to restrict control by making terms and conditions incomprehensible, ensuring that it is impossible to make an informed decision in terms of sharing information with them. I then discuss the potential barriers that exist when individuals attempt to gain more control, highlighting that it is not simply a matter of companies making things more difficult; maintaining the level of control we would like requires additional time and effort that we do not necessarily have. Finally, I address the often proposed solution to issues of control: opting out of using social media or refusing to share information with companies altogether, however, this is not as

straightforward as it appears, as there are a number of benefits to engaging with companies and social networking sites, which cannot be easily dismissed.

Chapter Four: Fight The Power

This chapter offers a further exploration of the decision-making process that people engage in when being asked to share information. I will consider how individuals employ tradeoff decisions in order to decide whether the benefits they will receive (such as greater convenience and social contact with friends and relatives) are likely to be greater than any costs incurred (such as a loss of privacy). I will provide counter arguments suggesting the use of bias and heuristics, which suggest that we are not necessarily making logical decisions. Finally, I will consider the 'tactics' (de Certeau, 1988 p.185) used by individuals in a bid to gain (limited) control over their data, focusing on methods which utilise 'evasion' and 'subversion' (Fiske, 1989 p.2).

Chapter Five: Context Matters

This final analysis chapter focuses on the importance of context, which is where my original contribution is located. I will consider the importance of context to individuals, particularly in terms of the difficulties many now encounter in terms of maintaining different contexts separately and the issues that can arise when 'context collapse' (Vitak, 2012 p.451) occurs and different contexts merge. I also utilise Raynes-Goldie's work (2012) to propose that levels of concern around sharing information differ depending on the type of information being requested. Here, Raynes-Goldie's distinction between 'social' and 'institutional privacy' (2012 p.81) will be particularly instructive and I will utilise it to argue that social privacy can be further broken down into 'intrinsic' and 'issued' information,

which, while not mutually exclusive categories, offer potential insights into varying levels of concern regarding different types of information. Finally, I consider the impact of different audiences upon levels of concern expressed by participants when sharing information.

Conclusion

Finally, I will conclude my thesis by re-visiting my research questions and demonstrating my original contribution to this field, highlighting the important role that context plays when we are asked to share data, particularly in terms of the type of information we are asked to share and who we are asked to share it with. I will also discuss recent events which have taken place (such as the Cambridge Analytica Scandal) and the impact this has potentially had upon attitudes. My project is exploratory in nature and so I will also offer suggestions for further areas of investigation while recognising the limitations of the current project.

Chapter One: Literature Review

In March 2018 news broke that Facebook users' data had been harvested and used to influence the outcome of the 2016 US Presidential election and the UK's 2016 EU referendum (Cadwalladr & Graham-Harrison, 2018). The accused company was Cambridge Analytica and although initial estimates regarding the number of users affected was 50 million, the final figure was claimed to be 87 million (Cadwalladr, 2019). When this story broke Mark Zuckerberg issued apologies, both in a Facebook post and in national newspaper advertisements in the UK and US. Many articles appeared in the media at the time, offering information regarding what happens to individuals' data once they have shared it, and suggesting that deleting their Facebook account may not offer enough protection (Anthony & Stark, 2018; Glance, 2018; Lin, 2018 and Mitchell, et al., 2018). For those deciding to remain on the platform, advice was offered regarding keeping their data safe from being harvested (Kleinman, 2018). While it initially appeared that there had been little impact on Facebook (revenues actually rose following the scandal), this did not last. Since the allegations were revealed, the FBI, US Justice Department and the Information Commissioner's Office (UK) (ICO) have all launched investigations into Facebook and the role it played in harvesting users' information. In July 2018, Zuckerberg announced that large numbers of users were leaving Facebook and that the stock value of the platform had been significantly reduced (Cadwalladr, 2019). Further to this, Facebook has been fined £500,000 by the ICO in the UK for not doing 'enough to protect users' information' (BBC News, 2019).

Although this has been a difficult period for Facebook, there are few signs that the issues related to this scandal will be so severe that the site will be forced to close down and it is still used by millions of individuals worldwide. In the time I have been conducting my research, various social media sites have gained prominence (such as Snapchat and Instagram), all of which offer new and interesting ways for users to connect. Despite various privacy issues, social networking sites continue to thrive, and while a scandal such as Cambridge Analytica may cause some to consider leaving, or actually leave Facebook, they may simply move to another site. Connecting with others via social media has become so engrained in our daily lives that it is difficult to imagine a time when we will no longer use these sites, as illustrated in the below comment from one of my interviewees:

> "…when I'm going about my day-to-day routine, on my phone, like, even when I wake up, I look straight on social media." (TJ, female, 23)

The Cambridge Analytica Scandal (as it has become known), has raised awareness and concerns regarding how much control we have over our information and what happens to it once we have shared it. Striking a balance between participating in the online world, while retaining the level of privacy we are comfortable with is an imprecise art, which many struggle to navigate. This is not new and before we are able to examine how people attempt to negotiate the boundaries of internet privacy, it is important to briefly consider privacy more broadly.

This literature review will be separated into three main sections, and will be organised by literary themes, which will then be further divided by questions I

utilise to interrogate these themes. The first section will define privacy, examining how various theorists have defined privacy previously and whether these definitions remain relevant (Westin, 1970; Nippert-Eng, 2010 and Spinello, 2017 [2003]). I will then consider the divide between public and private spheres and how this divide has been conceived, while recognising the difficulty in maintaining this separation.

The second section will then focus on the key issue of commercial surveillance, which is the focus of my thesis. Here I concentrate on the collection of data which has become a part of many people's daily lives and examine the issue of control. Moreover, I explore Bucher's (2018) work regarding programmed sociality and the impact this has on our relationships. I then consider how the work of Foucault (1977) has been developed and argue that it remains relevant in terms of our behaviour online. Following this, I will consider the aggregation of data and how this can reveal more about an individual than intended (Kosinski, et al., 2013 and Miller, 2016). The penultimate sub-section will contemplate debates around whether social media users are being exploited by the owners of these sites. Finally, I examine the opportunities available to individuals in terms of regaining limited control through small 'act[s] of defiance' (Fiske, 1989 p.9, and de Certeau, 1988).

The final section will review the complicating nature of context, and how it has been considered in previous research. I begin by focussing on the work of Nissenbaum (2010), particularly her theory around contextual integrity; this compelling research will be considered alongside that of other theorists who have attempted to categorise types of information. This offers a useful way of

considering the importance of type of information when examining how individuals feel about sharing data. It will examine how the sharing of different types of information may cause different levels of concern in individuals (Huberman, et al., 2005), as well as the impact that various audiences may have (Consolvo, et al., 2005). The second and final sub-section will examine explanations that have been put forth which attempt to explain why an individual's actions may not match their purported level of concern. This will include themes such as the privacy paradox, tradeoff decisions and the impact that the collapse of contexts can have on those concerned. Finally, there will be a summary of the literature review itself before moving on to discuss how my research will aim to reduce the gap in existing knowledge. The discussions throughout this literature review offer a starting point from which to consider not only the current and previous research on this topic but will allow me to identify the gaps in literature that my work will fill. This reflects the central arguments of my thesis, which are that the decisions and concerns that individuals have around their data privacy very much depend upon the context in which they are being asked to share information. Further, the use of social media sites, should not be taken to be a lack of concern regarding one's privacy, and individuals often implement measures they deem necessary and manageable when managing the boundaries of internet privacy.

Public versus private

Attempts to define privacy are not new, in fact, almost five decades ago, Westin offered an explanation of four types of privacy: '*solitude, intimacy, anonymity and reserve*' (1970 p.31). Within Westin's definitions, *solitude* refers to a state

when an individual is not part of a group; they are unobserved, and this is the most privacy that an individual can experience. Following this is *intimacy*, which is when a small group is separate from others, this is often seen in family relationships, but those involved do not have to be related. Thirdly is *anonymity*, which is when an individual is in public, but unknown to those around them, therefore they are literally a face in the crowd. In this context, the individual can be freely observed, but they are relaxed as they do not know those who are observing them (and they are unknown by the observer). The final type of privacy is that of *reserve*. This is when an individual wants to be left alone, and so restricts their communication with others; this is acknowledged by others in the act of allowing that person to be alone.

A common feature of all of these types of privacy is the element of control, while not explicitly stated, it is hinted at, in that the individual appears to be able to control access to themselves. Therefore, this is often deemed to be an important feature of privacy – the ability to control who is able to observe or identify an individual; the importance of control will be considered in much greater detail in the commercial surveillance section of this literature review. The theme of control links with Nippert-Eng's (2010) conception of privacy; she suggests that on a daily basis, individuals want to feel comfortable with how much they conceal or reveal, but it is an ongoing balancing act, rather than an absolute measurement. Further, she suggests three key themes around privacy: *control, solitude and autonomy*. She suggests that most of all, people want to be able to manage their privacy. Nippert-Eng argues that nothing is private by nature, and so in theory anything can be shared, although this raises questions regarding whether everything should be shared. The most important consideration is that individuals

have control over whether to share specific information with others; this is key. This simplifies what is acknowledged to be a very complex situation but does offer a foundation upon which to build. It is important to note that control is not easily achievable, and it takes a lot of work for individuals to achieve their desired level of control over their privacy, especially given that it is more difficult to be private than public (Nippert-Eng, 2010). It is often the case that privacy cannot be achieved simply because the individual involved decides to be private and it requires the assistance or support of others.

Spinello appears to agree with this viewpoint, suggesting that two popular theories when dealing with data privacy are 'control theory and restricted access theory' (2017 [2003] p.163). He argues that control theory relates to the work of Fried and suggests that an individual can only have privacy if he or she has control over his or her data while restricted access theory revolves around being able to limit the sharing of information about oneself in particular situations. Spinello also offers a number of types of privacy: '*secrecy, anonymity and solitude*' (2017 [2003] p.163). *Secrecy* relates to the ability of an individual to restrict the dissemination of information about themselves to others. *Anonymity* offers a shield from unwanted attention, while *solitude* gives individuals the ability to be physically distant from others. These definitions share the view that control is vital when considering privacy and is one of the key themes that I will explore within my research into how people navigate the boundaries of internet privacy. However, it is important to note that not all theorists in this area deem control to be vital. Nissenbaum (2010) goes so far as to suggest that, 'privacy is neither a right to secrecy or a right to control, but a right to appropriate flow of personal information', (p.127). From Nissenbaum's perspective, control is less

important than context, which dictates the type of information that can be shared with whom under which circumstances. Under the framework of contextual integrity, Nisenbaum suggests that when concerns are raised regarding contemporary data collection, it is not the lack of control that is at the root of this, rather it is how these practices 'transgress context-relative information norms' (Nissenbaum, 2010, p.186). These norms are important as they support the social contexts in which we live our daily lives, and interact with others, which in turn promote the information-sharing practices that are and are not acceptable. Therefore, control is not the issue, as we are happy to have less control in situations where it is contextually appropriate, however, where it is not appropriate, this is when tensions occur. This will be discussed further in the context section of this literature review.

Are public and private areas mutually exclusive?

The separation between public and private areas is not only taken for granted but is deemed to be mutually exclusive. Discourse around these terms is particularly problematic when it fails to recognise the complex nature and multiple meanings of these categories (Arendt, 1958; Weintraub, 1997 and Wacks, 2015 [2010]). Despite a lack of clarity around the terms public and private, they continue to be widely used in a way that suggests common agreement regarding what they represent (Habermas, 1989). In fact, Wolfe (1997) states that while the distinction between the two categories is not perfect, it is necessary. The reason for this is that there is behaviour which should be hidden, and thus kept in private; clearly if there were no private realm, this would not be possible. However, there is more at stake here than simply practical considerations of behaviour and Arendt (1958) suggests that we all need the private sphere as it provides the foundation for the

public sphere and is therefore vital for humans' existence. The mental health of individuals may depend on the existence of a private realm where they are able to relax and reflect while hidden from society's watchful gaze (Arendt, 1958; Westin, 1970; Berger, et al., 1977 and Goffman, 1980). Indeed, legal scholar, Cohen (2017) argues that privacy is essential to allow individuals to engage in 'boundary management through which they define and redefine themselves as subjects' (p.459), this is something that would be impossible to carry out in public and once again demonstrates how necessary the private area is.

The existence of a separate, private space is vital because people are required to be constantly engaged in impression management, in a bid to ensure that they give out the 'right' impression to others when in public (Goffman, 1990 [1969]). Often this means that individuals must hide their actual feelings when interacting with others for fear of showing their 'true' selves and losing the respect of others. Under this conception, the private sphere is necessary for people to be able to participate in society as it also offers them a space to be self-reflective. Arendt (1958) offers a similar argument, suggesting that privacy offers a hiding place for individuals, and a way to give their lives added depth. She puts forth that although those living in complete privacy almost cease to exist, those living in complete publicity fare no better, as they live a shallow life, which lacks meaning. As such, the private sphere is necessary to maintain well-being and to allow recovery from too much time spent in the public realm. Given this, it is perhaps not surprising that as the concept of the private space develops, it becomes inextricably linked with the home. As such it is broadly seen as a sanctuary where individuals can be themselves, sheltered from the outside world. However,

the link between the private realm and the home is not without issue, although a fuller examination of this is beyond the scope of this literature review.

The relationship between the public and private spheres is often characterised as being one of dependence, requiring balance (Westin, 1970; Weintraub, 1997 and Nippert-Eng, 2010). As discussed previously, Arendt (1958) subscribes to this view of balance, arguing that it is necessary for an individual to have balance between privacy and publicity in their life as any imbalance would be problematic. However, Lyon (2005 [2001]) suggests that the distinction between public and private is becoming more blurred due to increased surveillance in individuals' day-to-day lives. He puts forth that many interactions now take place regardless of physical boundaries and therefore it is harder to discern where the boundary between public and private space lies. There are also numerous electronic devices within our homes, which connect wirelessly to various external computer networks to pass on data. Examples of this include the Amazon Echo range of products which all feature their personal assistant 'Alexa' (Amazon, 2019) not to mention individuals updating their status on social networking sites. Given these examples, it seems that locating the line between the public and private spheres is becoming increasingly difficult.

While there is little doubt that a relationship exists between the public and private spheres, to treat these categories as mutually exclusive is a problematic approach, which has been pointed out by various theorists. Weintraub (1997) in particular suggests that the taken for granted nature of this dichotomy suggests that the two concepts can be easily categorised as binary opposites. Rather than there being a single divide between the two spheres, he argues there are a multitude of

frameworks in which they can be used, however, this is rarely considered by those using them. Given the problematic nature of this binary divide, Nippert-Eng (2010) offers an alternative conceptualisation. She puts forth that it may be more helpful to consider the public and private spheres as opposite ends of a spectrum. At one end there would be total privacy, which would be characterised by an individual's complete inaccessibility, while total publicity would be at the other end and would be characterised by an individual's complete accessibility. This is an idea that could be worth developing further, however, it may lead to the same issues of definition as we try to decide where different actions and information should be placed upon that spectrum. Further, I suggest that this boundary is context-based and as such is dependent upon each individual situation, which makes a clear definition impossible.

Nissenbaum (2010) contends that while it may seem obvious to restrict concerns about privacy to the private realm, this makes problematic assumptions about the relationship between privacy and the public/private dichotomy. Her framework suggests that it is ultimately reductive to suggest that we are limited to only two contexts – public or private, instead putting forth that there are numerous social contexts, each of which have specific rules which regulate how information should flow within that context. This framework allows us to consider each situation and context as a separate case, rather than having to use broad categories, which obscure the fundamentally nuanced nature of privacy and information-sharing. This recognises the multi-dimensional nature of appropriateness, rather than attempting to separate situations into private or public, which may be unhelpful.

Ultimately, the categories of public and private are not mutually exclusive, and the concept has shades of grey, which further complicates the task of defining privacy. Helpfully, Nissenbaum (2010) suggests that privacy can be linked with three areas of the public/private distinction. These areas are the *actors* involved, the *space* itself, or the *type of information* and each of these areas can be separated into public or private, which can be helpful. In circumstances where this approach is taken, there is often an emphasis on one of the above areas, however, issues occur when these dimensions become confused or they are not explicitly recognised. Essentially, this approach considers each context separately, on an individual basis, recognising the importance of considering the complicated nature of privacy, rather than attempting to use broad strokes to make sweeping categorisations.

Commercial surveillance

Historically, work around surveillance has tended to focus on government surveillance, not least because of the usefulness of this practice to the government. However, the focus of my work is commercial surveillance, in particular social media platforms and commercial companies. That being said, many of the discussions around government surveillance can be applied to the practices of commercial surveillance. Cohen (2017) suggests that those who study surveillance consider it to be 'a mode of social control' and rather than it being passive or reactive, 'surveillant attention is productive,' (p.456) highlighting the importance of considering what is produced by it. When considering the role of surveillance, it is important to examine the link between surveillance and economic development. Cohen highlights the importance of doing this as she

discusses how surveillance as a form of social control has contributed to the 'ongoing shift from industrialism to informationalism' (p.457) in developed countries. Increasingly, the way in which companies make money is by collecting, collating and selling users' data, thus highlighting the greater value assigned to information. This commercial surveillance is also beneficial to governments, who 'routinely access…and use flows of behavioral [sic] and communications data for its own purposes'. (Cohen, 2017, p.457). Therefore, Cohen (2017) suggests that it is not enough to consider this kind of surveillance as merely social control, contending instead that it is 'a mode of governance' (p.457) which is inextricably linked with 'the rise of informational capitalism as a model of political economy' (p.457).

Social connections

As discussed briefly in the previous section, control is purported by some to be vital to our ability to achieve the level of privacy we desire; however, this is problematic for those collecting our information for a number of reasons. The main issue is that companies collect vast amounts of data about their customers so that it can generate income; this is essentially the business model for many social networking sites, as well as large corporations such as Google. Previously, companies made money from selling items or services, and while this is still true for many, user data itself has become a valuable commodity (Lyon, 1994 [1988]; Lyon, 2000 [1994]; Nissenbaum, 2010; Miller, 2011; Pierson, 2012; van Dijck, 2013; Fuchs, 2014 and Miller, 2016). The value of this information lies in its ability to allow advertisers to allocate their resources in a more efficient way by targeting their advertisements towards those who are more likely to be interested in purchasing their products. In order to do so, companies need to collect as much

data as possible, as this then enables them to create profiles of consumers which can then be aligned with potentially suitable products. This is why companies often introduce a loyalty or rewards scheme for customers, as it allows them to collect a greater amount of data, and through the individual's account, link it together (Miller, 2011 and Cohen, 2019). Although some companies have offered premium services or content for a fee in order to generate profit, customer data is often much more profitable than subscription fees and so many are reticent to do this (van Dijck, 2013). Companies also join their data with that of other companies to create profiles of their customers and build a more detailed picture of them, their behaviour and habits, which can be utilised when marketing to them. This is the role that Big Data fulfils in that the aim of it is to collect ever-increasing amounts of data (Andrejevic & Gates, 2014). Proponents of Big Data suggest that more data offers greater insights, and as such any issue is deemed solvable if enough data has been collected. The issue for companies is that if individuals are granted greater control over whether to share information or not, they may choose not to share their data, thus reducing the effectiveness of these profiles and the targeted marketing.

This is not necessarily the case, particularly if we consider Chauncey Starr's concept of 'voluntary' and 'involuntary' (1969 p.1233) tasks. Starr suggests that tasks can largely be separated into two categories, those that we choose to complete (those that are voluntary) and those that we have no option but to complete (involuntary). In terms of sharing data, we are the initial decision-maker in that when a company requests information from us, we can decide whether to share the information or not. However, if the company then shares the information with a third-party that we have no knowledge of (and have therefore

not consented to), it becomes involuntary, and we lose control over our data and what happens to it. This offers an explanation for the concern expressed by companies, if they allow the further sharing of data to become a voluntary activity, people may exercise their control and refuse consent. However, Starr also suggests that 'we loathe to let others do unto us what we happily do to ourselves' (1969 p.1253), therefore, as individuals appear happy to share information with companies initially, if they were given the option of sharing with a third-party, they may also agree to it, the issue here is that the choice has been removed from the situation, rather than the sharing of data itself. This suggests that increased control for users may actually be beneficial to companies, despite their assumptions to the contrary.

Regardless of who has control in these situations, it is clear that we have become much more connected through our use of social media sites. Van Dijck (2013) considers the connections we are forming with each other through the use of technology and how this has developed into a culture of connectivity. Utilising the example of Facebook, he examines its ethos of sharing and openness and what this truly means for users. Essentially, the term 'sharing' does not have a clear definition. Taken at face value, it appears to denote users sharing information with each other through their use of Facebook, however, Facebook also shares user data with third-parties. It is also important to note that sharing itself is not a social norm, it is something that is negotiated between the owners of social networking sites and their users. This has not necessarily been straightforward and social media users have not simply followed the sharing norms set out by the owners of these sites (this will explored in greater detail later in this review). Nevertheless, van Dijck (2013) puts forth that due to its position as the leader of

social networking sites, 'Facebook's ideology of sharing…set the standard for other platforms and the eco system as a whole' (p.46). It is in the best interests of the platform owners to encourage users to be as open as possible (Couldry and Mejias, 2019b) as the more information they can collect, the more they have available to sell to third-parties. It also allows them to aggregate more information regarding each user, which creates value (aggregation will be dealt with in greater detail later in this review). Social networking sites encourage users to create and maintain connections through using the platform and it can be argued that 'Facebook's connective functions provide empowering and enriching social experiences' (van Dijck, 2013, p.47) for users. However, complete openness is not necessarily the best thing for the site's users, who may not want all (or any) of their information to be shared with third-parties. As such, it is in Facebook's interests to focus its users' attention on their social connections (to encourage greater sharing) while obscuring the third-party sharing. There is the potential for users to become disenfranchised if they learn more about what happens to their data. In fact, owners of these sites have an advantage in that they employ those who write the code, and so ultimately, they hold greater control over user-data than the users themselves. An example of this disparity is that following a user backlash after introducing Facebook Beacon, rather than reverting to the existing norms in terms of sharing data, Facebook began working on ways to alter the norm around sharing to expand what the term actually meant. This suggests that once a new routine becomes accepted as regular practice it becomes the standard against which all new systems are measured. This is problematic as it may take time for people to realise that they are uncomfortable with a new practice, by which time is it too late to challenge it as it has become

commonplace, rendering complaint or protest moot (Nissenbaum, 2010 and van Dijck, 2013).

Users are integral to social networking sites, because the information they provide (through status updates, liking others' posts and so on) is fuel for the algorithms, which are constantly changing in response to this (van Dijck, 2013). However, not all social media users are of equal value to the owners of these sites and those with more connections with other users generate more information and links and as such, more profit. To encourage this, Facebook has worked hard to ensure that its reputation encourages users to visit the site, spend time there and make connections with other users (van Dijck, 2013). There is a fine balance to be struck on these sites, between 'attracting and exploiting communities' (p.62). It needs users to enjoy using the site, but it also needs to encourage them to be active users, as this will generate greater profit through increased content and/or connections. However, this needs to be dealt with delicately as sites such as Facebook need users to be willing 'to contribute data and to allow maximum data mining' (p.64), this can be a difficult balance to strike and as such, Facebook employs creativity to encourage greater sharing. It has also been aided in this by other companies who are willing to allow Facebook to verify user credentials (though the 'Sign in with Facebook' button). This allows users to sign in to other websites, using their Facebook logon details, thus offering a frictionless experience, which makes the process much more convenient for users, who can create a new user account without having to remember yet another set of login details. This then links all of their activity on the new site with their Facebook account, thus generating further data for Facebook. This is also another layer of the culture of connectivity in that the companies themselves are inextricably

linked, just as the users are (van Dijck, 2013). As discussed previously, the connections between users provides fuel for the algorithms that social media sites rely on, algorithms, which in turn shape the experiences of those using the site.

Programmed Sociality

Through her exploration of algorithms, Bucher (2018) argues that 'platforms act as performative intermediaries that participate in shaping the worlds they purport to represent' (p.1), thus suggesting that these sites cannot be separated from our daily lives. In fact, she does not view platforms as neutral tools, due to the analytical work that takes place behind these sites, usually hidden from the users' view. Users receive numerous recommendations based on computer-aided analysis of their previous actions and preferences, which they may be unaware of. This is not problematic in and of itself, however, Bucher argues that this has led to our online lives becoming much more mediated, meaning that we are led in particular directions based on our past behaviour.

Bucher's (2018) work on 'programmed sociality' (p.1) is heuristic in nature, suggesting that we rely on algorithms in various ways. Social media platforms are a part of our social relationships, rather than merely offering a space for them to exist. Facebook prompts users to provide personal information as soon as they have set-up an account and to add people to their friends list. Templates tell users what information to enter and the format that these entries must take, which allows the algorithms to function efficiently. Facebook needs engaged and well-connected users and so it offers various ways for users to engage with the platform itself, as well as each other. Algorithms create value, offer accurate predictions and encourage users to engage with and continue to use the platform;

Facebook does this by reminding users of 'friends' that they have not interacted with for an extended period, for example. However, that is not to say that Facebook friendships are not authentic, rather Bucher (2018) argues that, they are 'highly mediated and conditioned by algorithmic systems' (p.7). It is also important to remember that people appear on a user's newsfeed regardless of whether they are close friends or acquaintances. This is because social networking sites are not interested in differentiating between these groups as it does not serve their mass collection of data (Blank, et al. 2014). As such the newsfeed will not show a user all updates by everyone on their friends list, rather it will show those calculated to be most important (and that will garner the greatest level of interaction and engagement from the user concerned). This demonstrates programmed sociality in action, as users' online experiences are shaped by algorithmic systems, and this is where the power lies in these exchanges. Bucher calls forth Foucault to suggest that 'this would be power seen as a form of political, social and economic domination, where one entity prevents another from seeing or doing something' (p.34 & 35). In other words, social networking sites employ algorithms that 'decide' which information a user sees and what is hidden from them. It is also important to remember that algorithms are programmed by humans, and so, the suggestion that algorithms have power, is not accurate. More broadly, it is important to note that there is more to this than computer code.

Bucher also raises the point that when we post on social networking sites, we do not just reveal information about ourselves, but others too. As such, from the perspective of these sites, 'friends are in the data delivery business' (p.13). Therefore, when a user posts little information about themselves, the algorithms

will utilise information posted by those they are linked with as friends to target and tailor the advertisements seen. Therefore, when an individual posts on Facebook, they are not merely affecting the content that they will be presented with at a later date, but also what their friends will see. Everything a user does on the site becomes a data point which is then utilised by algorithms, that are ever-changing based on the information they gather. As such, how users connect with friends is altered through their use of Facebook; this, Bucher argues is due to programmed sociality, which does not simply transpose friendships, rather it generates new ways for friendships to exist. In this sense, technology is productive; it produces friendships rather than offering a platform for them to merely exist on. However, it is important to note that programmed sociality should not be perceived to operate in isolation and 'their capacity to produce sociality always already occurs in relation to other elements' (Bucher, 2018, p.153). As such, people's behaviour changes in response to programmed sociality due to the way it guides their actions by reminding them of a friend's birthday or encouraging them to message a friend they have not interacted with recently.

Updating Foucault

It will be helpful here to consider Foucault's work regarding disciplinary power (1977) and offer an update of it, with regard to social networking sites and how contemporary theorists have linked this. Foucault argues that disciplinary power sets out the expected, normal behaviour which is rewarded. Further, given the way in which disciplinary power functions, individuals do not notice they are being restricted, however they feel pressure when they attempt to behave in a way which does not conform. Foucault puts forth that 'Discipline 'makes' individuals, it is the specific technique of a power that regards individuals both as objects and

as instruments of its exercise' (1977, p.170). Therefore, as discussed above, social networking sites make money from users' actions (in terms of what they post or like), and as such, moulds them to be active members of the site by sending users emails when they have not logged onto the site or posted an update for a period of time. This encourages them to share more regularly, and as such directs users to behave in the way that will generate the most profit for the site (because the more information users share, the more data the site has to sell to advertisers). Therefore, through the use of disciplinary power, users come to behave in the way that generates the greatest income for the site, while at the same time, believing that they are choosing to share information. This offers the illusion of control for users who believe they only post information when they choose to and fail to recognise the ways in which they are compelled to do so.

Foucault also argues that these systems function efficiently due to individuals being constantly observed; he perceives observation to be coercion (1977). While those subject to this kind of coercion need to be seen, the opposite is true for those carrying out the observations. Surveillance becomes embedded into the environment and as such the design of the environment centres around observing those within it, rather than any other function. Again, this can be linked to social networking sites, as the design of them facilitates and encourages the sharing of information, and/or linking individuals together (through 'tagging' them in a post or photograph), allowing observation to occur, while appearing to offer a space for individuals to connect with their friends and family. Social media users are observed by the site, so that patterns can be identified, and users' behaviour is not only predicted, but once the site has enough information, it can be manipulated (Bucher, 2018). This occurred in 2014, when findings were published from an

experiment that researchers carried out with Facebook (Kramer, et al., 2014) during which users' moods were manipulated by altering the proportion of positive or negative postings appearing on their newsfeed. This caused concerns to be raised regarding informed consent at the time (Booth, 2014) and highlights how useful observations can be to the social networking site itself. This is also the issue that is at the centre of the Cambridge Analytica Scandal (Cadwalladr & Graham-Harrison, 2018), in which those involved have been accused of influencing voting behaviour in both the US presidential election in 2016 and the EU referendum earlier that year. While it is important to note that as yet, there has not been any concrete evidence that individuals changed how they voted depending on the information they were presented with on their Facebook feed, it has caused a degree of concern for many regarding the reach and influence of social networking sites.

Foucault (1977) suggests that the environment thus becomes a tool for training those within it. Although Foucault's focus was upon physical structures and architecture, I suggest that his work can be applied to contemporary social networking sites and the online space they offer to users. As discussed above, the environment offered by social networking sites (the platform itself) trains individuals to behave in a particular way. For example, through suggesting others they may know, it encourages them to connect with more people, which will help the site's algorithms to make more accurate inferences about that individual. There are also ways in which users' behaviour is explicitly directed on these sites, in terms of how they can express themselves, for example, Twitter only allows 280 characters in a tweet, therefore users must restrict themselves to this or spread their thoughts across a number of Tweets. Similarly, up until 2016, Facebook

users could only express how they felt about a post through the use of a single 'Like' button however, Facebook introduced five additional 'reaction' buttons three years ago, which allow users to express a number of emotional responses. Therefore, Facebook is directing the way in which users are able to express how they feel about a post without typing a comment, while also allowing the site to collect more nuanced information regarding how users feel about particular posts. However, we do not question why we are restricted, instead, we are coerced into behaving 'correctly' without question. Cohen suggests that this is due to surveillance itself having become a norm for us, so much so that 'The awareness of surveillance fosters a kind of passivity – a ceding of power over space' (2017, p.461). In this situation, we come to expect to be watched, which is problematic, as this leads to the normalisation of 'the disciplinary effects of surveillance, making them more difficult to contest' (p.461), therefore, we no longer consider this type of surveillance to be a problem and may in fact internalise this so that we feel safer in spaces with greater levels of surveillance. As noted earlier, even if we do become concerned, it is often after the practice has become embedded and so it is too late to make any complaint or attempt to remove the practice.

Foucault suggests that under the rule of discipline, subjects become objects, who do not see power directly, but do feel it upon their bodies. I argue that this happens whenever an individual is unable to carry out a task in the way that they would like such as when registering with a website. This view is shared by Cohen (2012), who suggests that system 'design make some actions seem easier and more natural, and other activities more difficult.' (p.131), this tends to be done in such a way as to make it appear to be the norm, so that users do not question why they are directed a certain way when carrying out actions. This can clearly be

seen if we consider how Facebook has changed its structure from 'a database structure into a narrative structure' (Van Dijck, 2013, p.54). Originally, users were free to enter whatever information they chose to on their profile, however, as time went on, Facebook became more prescriptive. The introduction of the site's timeline organised everything a user had posted, uploaded or interacted with into chronological order, this makes every user's page appear more uniform, while also helping Facebook as it collects information that can be used to fuel algorithms (Van Dijck, 2013).

Foucault's work on disciplinary power is popular amongst various theorists when discussing issues around social media, and Bucher (2018) updates Foucault's work in her examination of algorithms. She suggests they are a tool used to govern populations of social media users by directing 'the flow of information and the practices of users' (p.38) to specific areas or activities. By doing so, users' attention is directed towards certain activities, often connecting with other users and/or generation of information for the site to collect and sell, and away from other activities, which are less valuable to the site owners. She goes as far as to suggest that they are 'political devices…that represent certain design decisions about how the world is to be ordered' (Bucher, 2018, p.68), thereby signalling to users what is or is not important. This is not necessarily noticed or considered by users, who deem this to simply be 'the way things are', rather than questioning the system, much less try to change it. In this sense, power does not reside with the algorithms, rather it is through 'algorithmic techniques and practices' (p.68) that 'power is exercised' (p.68). In this way, disciplinary power has become integrated and (to a certain extent) invisible. As discussed above, disciplinary power requires covert surveillance to take place and this is where social

networking sites come into their own, in terms of the level of surveillance they facilitate. Foucault suggests that 'The perfect disciplinary apparatus would make it possible for a single gaze to see everything constantly' (1977, p.173), and I argue that this is how social media operates. The sites record everything that users do there, including their status updates, other statuses that they like or comment on, as well as who they are linked with through their network and this information is not only collected and analysed, but also re-visited and repackaged to be sold to advertisers. As noted above, it is also used to predict and influence users' behaviour. This surveillance is largely invisible to users (or, at the very least, not considered by them).

This leads to disciplinary power being simultaneously 'indiscreet' (in that nothing is ever hidden because it sees everything) and 'discreet, for it functions permanently and largely in silence' (Foucault, 1977 p.177). Cohen (2017) also highlights the disparity between the transparency of the watched and the opacity of the watchers. Building upon Foucault's work, she suggests that surveillance works to generate categories based on various attributes, which can then be used to classify individuals and organise them into groups of those who share those attributes, this is then taken to be factually accurate. It is also important to note that this is effective without any official coercion and is not administered centrally, in fact this process is most effective when 'widely dispersed among civil and market institutions that govern everyday life' (p.460). In other words when they are covert, occurring in the background as we go about our daily lives, without considering it. In this way, everything is known about users through the information they share and the connections they make, however, little is really seen in terms of what social networking sites do with users' data. It often takes

large-scale media reporting, such as that around the Cambridge Analytica Scandal of 2018 to reveal the extent of the surveillance being carried out. Despite this, there does not appear to have been a mass exodus from Facebook, and although between July and October 2018, it lost a number of users in Europe, worldwide, the number of users continues to increase (The Independent Online, 2018).

Bucher (2018) also updates Foucault's (1977) theories around categorisation and how this can be a form of discipline when she discusses the way in which algorithms categorise users according to the information it has collected and processed. This then leads to decisions regarding which users are able to access which information, it is also used to categorise users hierarchically according to how useful the data they generate is, and this then determines how visible (or invisible) they are to others. Bucher (2018) also takes Foucault's concept of the panopticon further, in terms of the use of visibility. The way that the panopticon works is that those within it are regulated through the potential of visibility, and thus are encouraged to behave 'correctly', as they can never be sure whether they are being watched or not. Under the conditions of the panopticon, all individuals are equally likely to be watched at any given moment, which leads to uncertainty around visibility. However, Bucher (2018) argues the opposite is true when we consider Facebook, and so the concern is not around being visible at any given moment, but in being invisible. As such users are subtly directed to behave in certain ways to ensure that the content they post does not disappear, rendering them unimportant and invisible; this invisibility is both literal and metaphorical. By encouraging us to re-think the importance of visibility, Bucher encourages us to consider how within the panopticon, all were equally visible, however, this is not the case on social media. Algorithms work to prioritise some users over

others, creating a hierarchy of visibility, and so users are encouraged to post more information, to include photographs and so on, to remain important enough to be visible. In direct opposition to the punishment of being visible within the panopticon, visibility is the reward on Facebook, it is the goal of users. In this sense, visibility has become aspirational, as opposed to problematic. However, Bucher contends that this does not mean that there is no place for discipline under these circumstances, as she states: 'Discipline denotes a type of power that economizes [sic] its functioning by making subjects responsible for their own behavior [sic]' (p.88). This continues on social networking sites, in that users are disciplined to behave in specific ways (which is how Foucault argued disciplinary power worked) in order to be considered important enough to be rewarded with visibility. As such users appreciate that their behaviour will be rewarded if it is deemed to be 'useful' (in other words, if it generates profit for social media owners). However, it is important to recognise that Bucher (2018) is not suggesting that algorithms directly tell social media users how to behave, rather 'they shape an environment in which certain subject positions are made more real and available to us' (p.156).

When considering online spaces, it is impossible to ignore the role that algorithms play in terms of what is or is not visible to differently profiled users. Content can be withheld, and access mediated simply by the use of algorithms which allow or deny pieces of information to be accessed. More than that, algorithms are also able to alter how content is presented to different users based on their attributes and so on. Therefore, our experience of online spaces is mediated by algorithms which also offer different suggestions to us based on our defined characteristics. As well as normalising the collection of our information, these companies have

also made sure that they articulate the benefits of sharing our data, so that we are able to appreciate the advantages of engaging with these companies and sharing our information. As such Cohen (2017) highlights the importance of considering how useful this kind of data sharing can be, although to gain these benefits, 'the surveillance society demands full enrolment.' (p.462), suggesting that we gain more if we share more. There are also issues when we consider that rather than information sharing leading to a level playing field in which all can participate, the current system of information gathering is asymmetric, offering the greatest benefits to those who are able to collect, store and process the greatest volume of customer information. At the same time, the purported benefit of consumers being offered greater choice when purchasing items has become confusing, rather than empowering especially given that companies are able to manipulate customers, in terms of 'tailoring promotions and disclosures to consumers with particular profiles' (Cohen, 2017, p.468).

Aggregation of information

In order to tailor promotions and information, companies often draw data together from disparate sources to create a profile of an individual; this is known as aggregation. This can be problematic for individuals, who are often unaware of this practice. Miller (2016) hints at a loss of control by suggesting that those who possess data, possess power, therefore once individuals share their data with companies, whether they realise it or not, they are also giving them the power contained within that data. This occurs because the more data companies are able to collect and aggregate, they more they 'know' about individuals and this knowledge is then used to make decisions regarding these people. It is also possible to make inferences from data and so additional information can be

revealed despite not having been explicitly shared (Kosinski, et al., 2013; Hern, 2015; Ward, 2017 and Nurse, 2019). Given that many people are unaware of the sheer volume of data that are collected and stored about them and how they have been merged with other data, it is hard to characterise this as a situation in which the individual is in control. This is especially problematic because data is often collected for one purpose and then through the creation of profiles and utilisation of data brokers, is re-used for a different purpose (Garfinkel, 2001 and Miller, 2016). This causes problems related to consent, as an individual may consent to the initial use of data, but as they are unaware of the potential secondary uses, consent is impossible. This causes issues for people as they want to feel comfortable with how much they conceal or reveal on a daily basis (Nippert-Eng, 2010), however this control is simply not possible if they do not know what will happen to their data. Gadzheva (2008) puts forth that even when individuals are aware of what happens to their data, there is still little possibility for them to have control as companies are not particularly forthcoming in detailing who they will share an individual's data with or which other pieces of data it will be linked with.

A common defence of aggregation (by the aggregators) is that the information is already available, albeit in different places, and so putting it together should not be an issue. Further, they argue that the individual in question has already shared the information freely and so there should be no issue with pulling innocent information together. However, this misrepresents the revealing nature of aggregated information, especially as 'third-party harvesters are keenly aware of the qualitative shifts that can occur when bits of data are combined into collages' (Nissenbaum, 2010, p.203). This is problematic because numerous inferences can be made from seemingly disparate pieces of information (which may be accurate

or inaccurate). Aside from the issue of potential exploitation, there is the issue of whether the information held by the organisation itself is correct, this is another issue with Big Data's adage that more data is better, it assumes that data is reliable when it may not be (boyd & Crawford, 2012). Any decision based on incorrect data could be disastrous, leading to individuals being treated differently due to an assumption based on incorrect data. Although in theory, the Data Protection Act 2018 gives data subjects the right to check and correct data where necessary, given the burgeoning data broker industry outlined above, this is a very difficult task. People may know who they shared their data with originally, but it is unlikely that they will be able to trace every other company that the data has subsequently been sold to (Lyon, 2000 [1994]; Gadzheva, 2008 and Miller, 2016) in order to correct it. This issue is further exacerbated by the fact that data is now stored forever. Previously, hard copies of data had to be destroyed in order to make room for more recent data, however, given the increased storage capacity offered by technology, there is no need to do this anymore. As nothing is ever forgotten, incorrect data can follow an individual around for the rest of their life, without them ever being able to correct it (Miller, 2016). This can cause a loss of 'social forgetfulness' (Blanchette and Johnson, 2002 p.33), meaning that no one is afforded a second chance, either for mistakes that have been made in the past or to rectify inaccurate data. Individuals thus come to lack autonomy over their lives as discrepancies in the data leave them open to issues arising from acts they have never committed and can never correct (Westin, 1970, Bucher, 2018). Therefore, the aggregation of data can cause numerous issues for individuals, whether the data are correct or not. The subject of aggregation has also raised questions regarding who actually owns the data stored in these databases. While the individual data subject may believe that as the data relates to them, it is theirs, the

company who has created the profile by aggregating data from various sources, often believes that the data are theirs as they have created the profile.

This matter is further complicated by the fact that when data is drawn together from numerous sources, it means that context is lost and so a collection of details can appear suspicious, when they are innocent. Linked to the loss of control described above, individuals are not able to add context or provide any sort of explanation in these cases, as they do not know which pieces of data have been linked together, or what inferences have been made. As the government collects data in order to identify terrorist behaviour, for example, an individual may be classified as a potential threat simply for having a similar behaviour pattern to a member of a terrorist organisation (Miller, 2016). It is possible that an innocent individual could be misidentified, and harm may be caused, this highlights another issue with Big Data, in that the volume of information collected may appear to answer numerous questions, however, without context, it is meaningless (boyd & Crawford, 2012). A further issue here is that once data has been decontextualized, it is also very difficult to tell what the intentions behind the posting were, and so something that was posted in an ironic manner, or as a joke may not be seen as such once the context has been stripped from it. Context and meaning are necessary in order to fully understand the social world, if this is lost, then it is difficult to fully appreciate what the data are telling us, if indeed they are telling us anything at all.

Are social media users exploited?

An often-cited issue with social media and their encouragement of users to share as much information as possible is the potential for users to be exploited. In his

examination of Facebook, Fuchs (2012) suggests that the commodification of individuals' data is a way of exploiting users. He (2013) argues that this exploitation occurs due to the creation of surplus value by users. Profit is generated when items are sold for prices which are higher than the costs incurred in producing them. Zuboff names this accumulation of vast amounts of data 'surveillance capitalism' (2015, p.77), and suggests (as many others have), that people utilising these sites are no longer deemed to be customers; they simply supply the raw data that owners of the site repackage and sell for a profit. Similarly, Couldry and Mejias (2019a) argue that information is not a 'natural' resource that is simply collected by these companies, rather, the nature of our everyday lives are being altered to better facilitate the collection and capture of information. However, companies must do this in such a way that we barely notice it. If it is noticed and questions are raised by users, companies argue that we are simply sharing our data, while they have the expertise to render the information valuable (as in its 'natural' state, it has no value) (Couldry & Mejias, 2019a). This then allows companies to collect our information and sell it on without considering those supplying the information. As social networking sites do not pay users for the data they provide (which is then collected and sold), it generates a profit without requiring any investment from the owner (Fuchs, 2013 and Dyer-Witheford, 2015). Fuchs suggests that this process means that 'users are unpaid and therefore infinitely exploited' (p.218), because as long as users continue to share and generate content, they continue to generate profit and as such can continue to be exploited. If social networking sites had to pay employees to generate content (rather than relying on users to do this for free), staffing costs would increase, and so profits would be reduced (Fuchs, 2013). It is also worth noting that although users provide the content, which some take to

demonstrate a level of agency, they have no control over how it is displayed to others (van Dijck, 2013) or who sees it. Another issue for social networking sites would be if users were to stop sharing information (and thus withdraw their 'labour'), this would result in a loss of revenue for the company and if enough individuals stopped using a particular site, it would no longer generate any income and would cease to exist (Cohen, 2008 and Fuchs, 2010).

This links to the work of Dallas Smythe (2012 [1981]), who despite writing about media audiences at a time before social media and the internet, remains relevant. Smythe recognises that audiences are vital to the marketing system. He suggests that audiences are sold to advertisers, and although they are paid for their labour time while at work, the same is not true when they are at home. In effect, by watching television advertisements in their leisure time, Smythe argues that audiences' leisure time is being sold, but they are not seeing any return on that sale, which is the argument being made regarding social media sites and their users. This perpetuates the asymmetric power relations that exist between those who create content and those who sell it and make money from it (Cohen, 2008). In this sense, Andrejevic (2013) argues that exploitation takes place because the owners of the site use the resources they own to collect information from users. As owners of these resources, they have complete control over who can or cannot access the resource and what behaviour is or is not permitted on the platform once access has been granted.

The theory of exploitation regarding social media users is not without its critics and it is important to recognise that the term 'exploitation' in itself can be problematic. This is especially important when it is being used to describe those

using social media to engage with friends from the comfort of their own homes as opposed to those working in dangerous conditions in sweatshops around the world (Hesmondhalgh, 2010 and Andrejevic, 2013). In these cases, the argument is often made that individuals are not forced to join social networking sites and given the enjoyment that many gain from using them, it is not exploitation. The belief that participation in social networking sites is completely voluntary is one that works in favour of these sites, in fact the term 'prosumption' (Toffler, 1980 p.271) has been put forth in a celebratory manner. It is often suggested that it allows users to have a creative outlet that they may not have in other areas of their lives offering them the opportunity to create their own identity (Comor, 2010, van Dijck, 2013). In this sense it is perceived as almost being emancipatory for those choosing to express themselves by sharing their likes and dislikes and so forth using social media. Others suggest that users are able to take advantage of social networking sites for their own ends and utilise the tools available to push posts to go viral and crowd source opinions (van Dijck, 2013). Critics of the exploitation argument suggest that it is unrealistic for individuals to expect to be paid for everything that they do in their daily lives, as they are often happy to volunteer to carry out particular activities (such as volunteering on a community-based litter picking day), and as such, do not necessarily expect to receive a financial payment (Hesmondhalgh, 2010). It is also worth noting that financial recompense is not the only way to feel rewarded, and as such many social media users feel that the pleasure they gain from connecting with friends and family through these sites is reward enough for sharing some of their information. This offers a counterpoint to the exploitation argument and raises questions regarding how far we are willing to accept this loss of privacy. As such, part of this project will consider how

people attempt to negotiate the boundaries of their internet privacy and where they draw the line in terms of what is or is not acceptable.

Is it possible for individuals to achieve greater control?

The issue of control can be difficult for individuals to navigate and Fuchs (2014) suggests that Facebook, in particular merely offers the illusion of control through its privacy options. While these options allow people to choose who can see the information contained within their status updates on the site (Facebook, 2019), there are limited menu options which allow individuals to choose which data (if any) they are willing to share with advertisers (Raynes-Goldie, 2012; van Dijck, 2013 and Stoilova, et al., 2019a). This suggests that while companies are aware that control is an important issue to individuals, they are not willing to give users any tangible control, potentially fearing that they will opt out of sharing data, thus reducing revenues. As per the earlier discussion, this is not necessarily the case, and commercial research shows that when companies are more transparent, customers tend to be more willing to share information (Benson, et al., 2015 and Martin, et al., 2018). That is not to say that companies do not offer individuals any control over what happens to their data, and most apps and websites allow limited control over which information is shared with the company. Again, this is not as straightforward as it appears, and it is often the case that those who are the least familiar with software and how technology works are the most likely to leave privacy settings as the default options (Pierson, 2012). This is problematic as often the default settings are the least secure and so individuals may be leaving themselves open to having their data collected by companies without realising it.

To remedy this, awareness is often cited as an issue that needs to be addressed, with the belief being that if individuals are more aware of what happens to their data, they will do more to protect their privacy (Gadzheva, 2008 and Fuchs, 2012). However, the issue of awareness only tells part of the story, as people also need to have the necessary skills and knowledge to make changes which afford them greater privacy. It is not enough for people to want to do more to control their privacy, they also need to know how to put this into action (Buchi, et al., 2017 and Cohen, 2017). In research carried out by the Pew Research Centre (Shelton, et al., 2015) some respondents felt that they lacked the skills necessary to be able to protect their privacy, as such they may be more pro-active if they felt able do so. However, many of the methods available to protect their privacy are relatively straightforward and require very little technical knowledge. Therefore, this leads to questions regarding whether individuals lack confidence, rather than the skills needed to protect their privacy and as such, do they assume that anything involving computers will be too difficult for them? This is borne out in research carried out by Nippert-Eng (2010) who finds that those who are taking action to protect their privacy are often using tools that are sub-optimal but are not overly onerous to employ. This is another potentially interesting point, individuals may want privacy, but not if it disrupts their daily lives to an unacceptable level. Given the additional convenience brought to our lives due to making purchases online, or utilising social media, there is the potential that people are only willing to do more to protect their privacy until it makes their lives less convenient. A seemingly simple task such as reading the terms and conditions before signing up to create an online account has become onerous and it has also been suggested that individuals feel disempowered to protect their own privacy.

Most of the time, users are not concerned with what algorithms do with their data or with the data stored about them in databases (Nissenbaum, 2010). However, this changes when something appears on their page that is not in line with their preferences (or, paradoxically is too in line with their preferences), this causes them to pause and consider the algorithms that are working in the background (Bucher, 2018). Concerns are also raised, when individuals 'discover that they are "known" when they enter what they believe to be a new setting' (Nissenbaum, 2010, p.50). This causes individuals to feel unnerved by this sharing of information that they were unaware of and did not consent to. People do not like to feel that others know more about them than they have allowed. Broadly, platform owners pay little attention to any privacy concerns expressed by users, stating that they do not charge users to access their platform and users are free to leave and use an alternative platform if they wish to (van Dijck, 2013). However, this is not as straightforward as it seems and will be further explored later in this review. The other issue for users, is the terms of service for these sites, which have become onerous to read and understand. Further to this is that owners can change them as and when they choose to, and it requires a certain level of skill to amend privacy settings to make them more secure than the default setting. Additionally, while individual privacy and control is considered, the same attention is rarely given to the aggregation of data – there is little detail regarding this in the terms of service and so users are left with very little information in terms of what companies do with their data and who they sell it to. Therefore, the biggest issue facing users of social networking sites, is how opaque business models are in terms of the algorithms that are utilised by companies. As such, 'we do not know *how* connectivity is exploited' (van Dijck, 2013, p.171),

therefore as discussed above, transparency only applies to site users, rather than the site itself. As discussed previously, these platforms tend to highlight the human connections that users can create and maintain through use of the site, while obscuring the automated processes that occur in the background, particularly as it relates to the way in which these companies not only collect information on users' social connections, but manipulate them (van Dijck, 2013).

This lack of control is often deemed to be a strategy on the part of data collectors (Cohen, 2012; Blank, et al. 2014 and Coll, 2014) to ensure that people only have a vague idea of what happens to their information. Raynes-Goldie (2012) suggests that a site's terms and conditions are purposely made incomprehensible in order to discourage individuals from attempting to gain more control. She is not alone in this view and research devoted to this topic finds that, broadly speaking, people do not read terms and conditions (Milne & Culnan, 2004 and van Dijck, 2013). This is not necessarily because they are not interested in doing so, but because it has become an impossible task (Turow, 2003; McDonald & Cranor, 2008; Vitak, 2012; Hoofnagle & Urban, 2014; Obar, 2015; and Obar & Oeldorf-Hirsch, 2018). The time-consuming nature of reading terms and conditions is examined by McDonald and Cranor (2008) who calculate the amount of time it would take the average individual to read the privacy policies of the websites they visit regularly. Even though they only include each website once, they suggest that it would take the average individual over two-hundred hours per year just to read the policies; this does not include any time spent comparing policies between sites. This suggests that an individual needs to devote approximately four hours per week to reading privacy policies, before they access the content they are interested in. It also does not take into account re-reading privacy policies when they change and

so this is actually a conservative estimate. Therefore, it is clear that while the self-management of privacy is a good idea in theory, in practice, it is an unrealistic burden to place upon individuals (McDonald & Cranor, 2008; Solove, 2013 and Obar & Oeldorf-Hirsch, 2018).

This is an important issue because in order to trust others, we need to have sufficient information upon which to base this decision. Generally speaking, the more information we have when making a decision, the better able we feel to trust those involved (O'Neill, 2002; Benson, et al., 2015 and Martin, et al., 2018). However, this information must be meaningful, if we are simply given a barrage of information, it will not help us to make a decision as it will be overwhelming and so lose meaning (O'Neill, 2002). It can be argued that this is what is happening when companies supply lengthy terms and conditions documents; the information is so difficult to understand (or there is simply so much of it) that it becomes a hinderance in the decision-making process. There are a number of factors that can have an impact on the level of trust afforded to companies and it is unsurprising that those with good reputations are more likely to be trusted than those with a poor reputation (Jarvenpaa, et al., 1999; Swaminathan, et al., 1999 and Metzger, 2004). Given the discussion of issues around the Cambridge Analytica Scandal at the beginning of this chapter, this raises a number of questions. If people are less likely to trust an organisation with a poor reputation, why do they continue to use Facebook following the Cambridge Analytica scandal?

There are a number of potential explanations here, which suggest that decisions regarding the use of social networking sites are much more complex than they

appear. Aside from the privacy paradox, which will be discussed below, it is difficult to deny that social networking sites have become integrated into many people's daily lives to such an extent that it is almost impossible to eschew them. People often join social networking sites in order to maintain or create social connections with others, and once they have done so, there is external peer pressure from friends and/or relatives to remain a user of the site (as well as the sites themselves making it difficult for a user to delete their account) (Van Dijck, 2018). There are a number of potentially negative consequences which individuals may suffer if they delete or close a social media account including a loss of convenience (Nissenbaum, 2010; Vertesi, 2015; Hargittai & Marwick, 2016, and Anthony & Stark, 2018). There are also a number of social costs associated with not having a social media account (Dommeyer & Gross, 2003; Raynes-Goldie, 2012 Scholz, 2013 and Van Dijck, 2018), such as missing out on invitations to social events or losing contact with friends and family. These are issues that are likely to weigh heavily on an individual's mind when they are considering leaving social media and may be enough for them to decide that leaving would be too costly for them. The use of social networking sites has become so integrated in our daily lives that those choosing not to engage may appear suspicious to others, as it raises questions regarding what that person may be trying to hide (Acquisti & Grossklags, 2003; Bennett, 2012; Vertesi, 2014 and 2015). Blank, et al. (2014) even go so far as to suggest that because our social lives are maintained through these sites, individuals must share information on them despite existing privacy risks. Therefore, it may actually be more logical for people to continue to engage with social media despite negative media stories or wanting increased control over their data. This suggest that we have limited choice in how far we participate in social media, and will be revisited later in this

thesis, when I consider the ways in which individuals attempt to exercise greater control.

Aside from this it is also possible that those continuing to use social media platforms may face costs if their participation is not deemed beneficial enough to the owners. Bucher (2018) suggests that because social media sites need users to participate and interact with others using the site, Facebook uses techniques which train people to behave in the way that is most desirable to the site. As discussed previously, there is the 'threat of invisibility' (Bucher, 2018, p.89), which is a punishment for those who do not engage with Facebook in the 'correct' manner. This punishment is described above in the social cost of not being a member of a social networking site, according to Bucher, 'not participating on Facebook will get you punished by making you invisible, and not seeing what may be "the most interesting" content to you' (p.89). Therefore, users are trained to behave in the way that is in the best interests of Facebook in order to ensure that they do not miss out on important events, or even miss out on being a part of something that everyone else is participating in (using the site itself). While social media platforms do not name these issues as a punishment, it is clear that this is deemed to be a cost, and for many a cost that is too much to bear.

It is important to note that individuals are not necessarily resigned to sharing information and having less privacy than they would like, and small acts of defiance may offer a way for people to maintain some level of control. This can be difficult to enact, because, as Gillespie (2007; van Dijck, 2013; Cohen, 2017 and Bucher, 2018) suggests, technology guides us along a specific path, by restricting which options are available to us. We tend to use technology in the

prescribed way, often without question, however, there are ways around this that do not require technical knowledge, which we know can be a barrier to people. De Certeau (1988) suggests that individuals can utilise tactics in order to subvert the dominant culture in small ways. He argues against the characterisation of individuals as being submissive and instead suggests that subversion is possible and those who appear to have had a particular culture imposed upon them have not necessarily accepted this, in fact they have been able to subvert the dominant culture, in a subtle way. While they do not openly reject the dominant culture, individuals instead use the tools afforded to them to their own ends, while appearing to have accepted it. In this way, despite being unable to challenge the dominant power in any real sense, they can divert it through this subversion. In the words of de Certeau, 'they escaped it without leaving it.' (p.xiii), which means that although they may appear to have accepted the dominant culture in the expected way, in reality they have adapted it to give it greater utility for their own purposes. Those who utilise tactics in this way, are necessarily those without the power to affect the dominant social order and so have to operate within it.

Writing only a year later, Fiske (1989) offers a similar view, suggesting that through employing defiance at a micro level, people are able to gradually erode at the macro level, by working from the inside. He argues that people within society are disempowered and are only able to create popular culture through utilising the available cultural resources (as did de Certeau (1988)). This can be difficult as the cultural resources are put forth first and foremost to further the interests of those who are dominant, thus supporting the status quo. This view is shared by Cohen (2017) who argues that individuals will not simply accept the constraints they are faced with on an institutional or cultural level and will utilise the tools

available to them to develop their own strategies. However, resistance is a necessary part of this power dynamic, because if there is no mechanism for individuals to employ a counter-reading of the available cultural resource, it will not be accepted (therefore, they need to be able to create their own meanings). As such, it is important to acknowledge that the dominant message is not merely accepted without question. By employing tactics, when dealing with online companies, it is possible for individuals to feel that they are in control. For example, in their research, Hargittai and Marwick (2016) found that students utilised tactics to avoid sharing their real name on social networking sites. Much of the research into methods of subversion have dealt with the ways in which users hide information from other social media users (Nippert-Eng, 2010 and boyd, 2014), however, the usage of tactics to gain more control in terms of users' relationships with those collecting their data is an area that has yet to be fully explored. Research that has previously been carried out in this area has shown that individuals show a preference for refusing to share private information rather than sharing false information to obscure it (Dommeyer & Gross, 2003 and Preibusch, et al., 2013). Often users will use multiple tactics to avoid sharing more than they are comfortable with; this is not limited to adults, and young people often employ numerous tools too (Stoilova, et al., 2019a). It is also important to remember that these platforms will do whatever they can to maintain the level of data collection they deem necessary (such as ensuring that default privacy settings are the most open) and 'resisting or subverting default settings requires both technological ingenuity and persistent motivation' (van Dijck, 2013, p.53).

Van Dijck (2013) argues that how much action an individual decides to take ultimately rests on the level of concern they feel regarding the practices of the social media platform. He suggests that users fall into two categories: 'implicit and explicit' (p.160). Here he argues that those who are broadly satisfied with what the owners do with their information, are passive and as such, are classified as implicit users. Those, however, who question what happens to their data and feel concerned about the underlying motivations of the site's owners are categorised as explicit users. For van Dijck (2013), the implicit users will continue to use the platform as before, however, the explicit users will take action, which will generally take the form of supplying false information or making changes to the default privacy settings of the site. Some will even go so far as to actively hack into the site to make their disquiet clear, although this is usually dealt with swiftly by the platform.

What role does context play?

A complicating factor when considering privacy is that it is not a single category into which we can easily file everything that we do not want others to know; the situation requires a level of nuance in order to appreciate its complex nature. In the same way that we would not generally want to share everything with everyone, neither would we want to withhold everything from everyone. For example, I may have little concern when being asked to share my annual income with a financial institution, however, I would not necessarily wish for my friends or neighbours to know that information. Therefore, the same information can be deemed private or public dependent upon the situation.

Contextual integrity

'Context relative informational norms' (Nissenbaum, 2010 p.140) offer some guidance and indicate to us what type of behaviour is or is not appropriate in a given situation and are the reason we may feel uneasy when witnessing certain behaviour in a particular context. Issues can arise when we believe that we are operating in one context but find that others have taken us to be operating in a different one, leaving us with a feeling of discomfort. In a similar way, Blank, et al. (2014) agree, suggesting that contexts can be said to be represented by circles, in which different behaviour is appropriate. These circles 'have different norms for what is expected to be disclosed and what is thought to be private' (p.26). They argue that what is deemed to be private is not a universal standard, and very much depends on the social context. As long as these circles remain separate, there are no issues, however, increasingly these circles are beginning to overlap which is problematic as it can have a negative impact on how we are perceived by others. The issue, broadly speaking, is that information that is problematic in one context (or circle), is not an issue in another. When these circles or contexts overlap, it can cause an issue, which is referred to as 'context collapse' (Vitak, 2012 p.451), and will be discussed at the end of this section.

Nissenbaum (2010) suggests that personal information flows in accordance with rules and norms in specific social contexts. When she discusses norms, she suggests that 'context-relative informational norms define and sustain essential activities and key relationships and interests, protect people and groups against harm and balance the distribution of power' (p.3). Individuals become upset or concerned when information technology does not adhere to these rules, because the 'contextual integrity (p.3) of the situation has been violated. While

technologies that reduce how much control individuals have over their information cause concern, Nissenbaum believes that it is more problematic when these norms of a situation are ignored as this risks social life itself.

Nissenbaum (2010) argues that while everyone has different expectations regarding what information they would like to share or remain private, when context is applied to a situation, privacy expectations become much more similar. Accordingly, context-relative informational norms tell us what is expected in terms of the flow of information in a given situation. It is also important to note that an individual's role varies between each situation they find themselves in, this is in line with the context, such as the workplace, or family. These roles govern how we behave in relation to others in those contexts; however, it is the context itself that sets out the overarching expectations of that situation. Contexts are not necessarily set in stone and vary across time, place and the society that they exist in; the level of detail afforded to the characteristics of a certain context may even vary. Contextual norms function in that those involved in a particular context feel that they *should* behave in a certain way. There are various types of norm; some are moral norms (such as being faithful to a romantic partner), some are social conventions (such as purchasing a present for a friend when it is their birthday) while others are rules and/or procedures that are formally set out, and as such the seriousness with which the norms are considered also varies. The norms must be considered in conjunction with the system itself, rather than in isolation as it will make more sense when the context is taken into account.

In terms of the information that we share with each other, Nissenbaum (2010) suggests that when these norms have been adhered to, that is when 'contextual

integrity' (p.129) has been retained; the opposite is true when these norms have been ignored. When individuals are considering a new technology, and feel uncomfortable, it is often due to the potential for the new technology to violate 'context-relative informational norms' (p.129). Informational norms are crucial as they set out the types of information that can and cannot be shared between individuals in specific roles (this is governed by 'transmission principles' (p.141)). Transmission principles determine whether the data subject's permission must be sought before information can be shared, or they are merely given notice that it has been shared. Information can be bought, sold, traded or leased, depending upon the transmission principle. However, it is important to remember that transmission principles are one of many parameters within an informational norm in a particular context and work in conjunction with other parameters (such as actors and attributes). The contextual nature of sharing information has also been considered by Bucher (2018), who discusses the different views on algorithms in her work to suggest that an individual may view an algorithm to be 'problematic in the contexts of one platform but not seem to have a problem with a similar mechanism on another platform' (p.107), thus highlighting the potentially contextual nature of online platforms and their use of algorithms. Returning to the earlier discussion around the public/private dichotomy, Nissenbaum suggests that 'the framework of contextual integrity…postulates a multiplicity of social contexts each with a distinctive set of rules governing information flows' (p.141). As such, it offers a much more nuanced view of the privacy of individuals' information and offers a response to many of the issues cited by privacy sceptics who suggest that those sharing their information on social media are clearly unconcerned about their privacy.

It is also important to consider who is involved in a particular context. Within any given context, there will be three types of actor – the sender of information (which may be an individual or organisation), the receiver of information (which, again, may be an individual or an organisation) and the data subject (the individual concerned). In any situation, it is vital to ensure that the role of each actor has been identified as far as possible; this is important in terms of whether an individual feels that their privacy has been violated in a particular situation. It is important to note that when people talk about particular information being private, they do not necessarily mean that is it completely private, rather it is private from specific actors (and not others). The issue is usually 'that it [information] is shared in the wrong ways with inappropriate others' (p.142), this is when the sharing of information becomes an issue for the individual concerned. The relationship between people sets out what information it is appropriate or inappropriate for them to have or know about the subject. Another important factor in a given context is the type of information. Nissenbaum's approach does not follow the previously considered dichotomy between public and private, neither does it offer a scale to denote whether a particular piece of information is more or less private, instead it recognises the multi-dimensional nature of appropriateness, which she argues are 'simultaneously variable' (p.144).

While much of this literature review has discussed privacy in relation to control, there is not widespread agreement on this, as others suggest that privacy is a right to limit access, rather than an absolute right to control. This disagreement does not exist under the contextual integrity framework (Nissenbaum, 2010), suggesting that control is one of a number of transmission principles and as such the importance of control will vary depending on a number of factors within that

situation. Other research into context has focused on specific contextual matters, such as the type of information that is being shared. Nissenbaum highlights the importance of type of information when she discusses how restrictions should be placed on different types of information in terms of whether it's release could be harmful, whether it is intimate information and whether those wishing to view it are legitimately entitled to have access to it. Personal information cannot be shared without restrictions being in place and these restrictions will need to adhere to the 'appropriate flow of personal information' (Nissenbaum, 2010, p.127).

Research by Huberman et al. (2005) examines how sensitive different types of information are and found that people are often more concerned about information being revealed when it makes them stand out in some way. When they ask participants how much they would need to be paid in order for them to divulge different pieces of information, they find that weight is contentious. If an individual feels themselves to be below average or around the average weight for the group, they require little payment to reveal it, while those who feel they weigh more or much more require a much higher payment. Overall, weight is not the most sensitive piece of information and other types of data are deemed to be much more concerning for people. When the researchers rank pieces of information by the proportion of respondents who would require payment of over $100 to reveal it, they find that financial information is deemed to be of greatest concern.

Although it can be helpful to consider how people feel about specific pieces of information, others attempt to create meaningful categories, which can be applied more broadly to types of information. Stoilova, et al., (2019a and 2019b) suggest three different contexts which prioritise different types of data and thus offer a

potential explanation for different levels of concern amongst young people regarding the sharing of their data. For them, the 'Interpersonal privacy' (Stoilova, et al., 2019a, p.7) context is the area in which individuals create their 'data self' and as such, the most important data here is that which is given by individuals, actively through their online interactions and activities. Under the 'Institutional privacy' (p.7) context, which is when information is dealt with by public agencies, such as the government, 'data traces' (p.7) take priority, and these are the breadcrumbs that people leave behind, often without realising, when online; it includes items such as cookies and other metadata. Finally, the 'Commercial privacy' (p.7) context is the area in which businesses collect our information in order to further their marketing, and so the most important data here is 'Inferred data' (p.7), which is derived from inferences made through the aggregation of data, as discussed previously. It is important to note, that only 'data given' is consciously shared by individuals, the other two types of data collection are obscured, and so are less likely to arouse concern or suspicion (as people may not be aware that they are happening). This is a concern, particularly as research in this area tends to focus only on data that is knowingly shared (Stoilova, et al., 2019b). As discussed previously, under the guise of 'surveillance capitalism' (2015, p.77), Zuboff argues that companies collect as much data as possible which is then used to create profiles and sold for a profit. This may be information that is explicitly shared in the form of status updates or Tweets or incidental information that is left without thought; the so-called 'exhaust' (2015, p.79) that is left behind as a by-product of these interactions. Therefore, despite the lack of awareness shared by many users of the site, they are nevertheless supplying information to these companies without realising that they are doing so.

Raynes-Goldie (2012) has also put forth ways of categorising information and suggests that our privacy broadly falls into two categories: 'social' and 'institutional privacy' (p.81). She argues that of the greatest concern is social privacy, which relates to our identity and the impression we make on others. In this regard, she considers information we might share on social networking sites to be included in this category. Institutional privacy relates to information that institutions collect and store; information in this category is hidden from the public view as are the processes that the information is subject to. Raynes-Goldie suggests that people are more concerned with their social privacy (Sujon & Johnston, 2017), and as discussed above, social networking sites allow us much more autonomy in terms of what we share in this area (with fellow users) as opposed to what we share with the site itself and connected third-parties (where we are afforded very little autonomy). Floridi (2005) offers an alternative, but helpful categorisation, when he discusses how information can be categorised as 'ontic' (p.198) or 'arbitrary' (p.197). For him, ontic information is part of who we are, it consists of our values and beliefs and is akin to a limb, in that it cannot be easily separated from us. Information that is categorised as arbitrary is assigned to us by others, and as such can easily be detached from us, with little issue; it is deemed to be items such as account numbers, passport numbers and other items such as these. The distinction between these types of information is important because it affects how we feel about the information itself, and potentially offers an explanation for different levels of concern relating to different types of information.

It is important to remember that while the type of information is clearly important to individuals, this is not the only factor to consider. Limited research examines

how people feel about the audience who has access to their information and what impact that has upon levels of concern. In particular, Consolvo et al. (2005), suggest that when people are asked for information, they are concerned with not only who wants the information, but also why they want it. Another important finding from this study is that '*How participant feels* about the requester at the time of the request' (2005 n.p.) also has a bearing on their willingness to share information. Therefore, while initial research into this area has provided a foundation upon which to build, there is still much to learn in terms of the impact context has on how concerned individuals are when being asked to share certain types of information.

Alternative explanations

While Nissenbaum's (2010) contextual integrity framework offers a compelling lens through which to consider discrepancies between our concerns and behaviour with regard to our privacy, other theorists have offered alternative explanations for this. The term 'privacy paradox' (Utz & Krämer, 2009) is used to describe the difference between what individuals say and do in terms of their privacy. It is often used in situations whereby people express concerns regarding their privacy and the amount of data that companies collect about them, while at the same time, continuing to share that information, through using online shopping websites or social networking sites. Although it is not necessarily named in such terms, the privacy paradox is apparent in various pieces of research which examine individuals' attitudes towards and behaviour around privacy. A pertinent example of this is the research carried out by Preibusch, et al. (2013), which examines the choices made by consumers when presented with a choice between two online retailers in order to purchase a DVD. In one iteration, individuals are given the

choice between purchasing the DVD from one company which collects more personal data but charges less, or one that charges more, but collects less information. In the second iteration, the price of the DVD is the same regardless of seller with the only difference being how much data each company collects from purchasers. In both versions of this experiment, the company that collects more data makes the majority of the sales. While this was somewhat expected in the version of the experiment with a price difference, suggesting that individuals were happy to lose a little more of their privacy in order to save money, the researchers were very surprised that this was the case when there is no difference in price. Possibly the most startling part of the experiment is that when people purchase the DVD from the company which collects more information, they then complain about the amount of data they are asked to share. This reflects the privacy paradox and bears a resemblance to day-to-day situations whereby individuals often share data with companies even if they are not particularly happy about it. However, it is important to note that the researchers recognise that the study was carried out in an experimental setting and as such could not be assumed to represent the real world.

Further evidence of the privacy paradox can potentially be seen in commercial research carried out by Gordon (2003) and the EMC Corporation (2014). Gordon's research focused on those working in the computer security sector, and so there would be an expectation that these individuals would be more concerned with regard to their privacy and therefore behave as such. However, as with the research above, Gordon finds that those she spoke with express concerns regarding their privacy yet, they do not behave in this way, often doing very little to protect their privacy, despite having the technological capability to do so. This

suggests that technological knowledge or capability is not always a barrier to protecting an individual's privacy, especially given that those working in the computer security sector appear unwilling to take action to protect their own privacy. Research carried out by the EMC Corporation (2014) also appears to demonstrate the existence of the privacy paradox. The results of this research show that while individuals express a belief that their data should be stored securely, they do not behave in a way that would achieve this. Many had not changed their behaviour despite media reporting on data breaches and most said that they do not read the permissions they are allowing companies when installing mobile apps onto their smartphones. Perhaps most astonishing of all, was the fact that while almost two-thirds of participants stated that they do not trust websites which only use password authentication, one-third of respondents use the same password across numerous websites. This suggests that individuals place the responsibility for their security and privacy with the companies they are dealing with, rather than with themselves.

While the concept of the privacy paradox can be a useful tool in explaining the disparity between individuals' expressed concerns and their actions around privacy, it is important to note that the research above requires further unpacking. As discussed above, Nissenbaum's (2010) contextual integrity framework offers a resolution to the issue that those who say they are concerned about privacy, do not necessarily behave in a way that indicates that they do. She argues that the paradox is a fallacy, because a person is capable of:

> ‘caring deeply about privacy and at the same time, eagerly sharing information, as long as the sharing and withholding conform with the principled conditions prescribed by governing contextual norms’ (p.187).

As such, when a person is sharing their information it is governed by different flows of information and contextual norms and differs from a situation where they are not sharing their information. As discussed throughout this literature review, it is important to consider each situation separately, rather than assuming that if a person shares information in one situation, they will necessarily share it in all situations.

For those that subscribe to the privacy paradox theory, there are other explanations for the disparity between what people say and how they behave. It could be, for example, that people are less concerned than they state when completing a survey or being interviewed but feel they should be concerned and want to make a good impression on the researcher (Bryman, 2012) as such, they may over-state privacy concerns. Therefore, outside of the research situation, the person’s actions could be much more aligned with their concerns regarding privacy. It is also important to consider that while the above research has identified a disparity between concerns expressed by individuals and their behaviour, none of them appear to have delved any deeper to attempt to uncover reasons for this. It is also important to consider that individuals may not feel that they lack control and as such are happy with the choices they are making.

Individuals may believe that they are making logical decisions and so are willingly sharing their data. Further, it has been suggested that we are actually

much more aware of what is going on and simply weigh up the advantages and disadvantages of sharing data and make the decisions regarding whether to share data based on this internal calculation (Nippert-Eng, 2010 and Van Dijck, 2018). This would explain why individuals often comply with the collection of data, as it suggests that they believe that the advantages to be gained from sharing data outweigh the potential disadvantages from doing so (Giddens, 1991; Lyon, 2000 [1994] and Lyon, 2005 [2001]). Under this view, people are said to be willing to give up some of their privacy in order to gain greater convenience; therefore, it is deemed to be a price worth paying. This suggests that individuals are thoughtful, rational beings who make logical choices with regard to their privacy. It is also important to remember that as companies collect greater amounts of data, it means that they can target special offers and advertisements, therefore individuals are more likely to receive offers that are of interest to them. As such, individuals are willing to give up some of their privacy in order to gain special offers, or greater convenience (Gadzheva, 2008; Nippert-Eng, 2010 and Miller, 2011).

Theory around tradeoff decisions very much depends on the person involved believing that the benefit they will receive for sharing information is greater than the costs they will incur from doing so. This is often referred to as the 'calculus of behavior' [sic] (Laufer and Wolfe, 1977), and suggests that when individuals are offered a choice, they will internally calculate which behaviour is likely to reward them the most. Therefore, in this case, the calculation made will be based upon whether a person believes they will see greater benefits from sharing information than not. Aside from the issue of a lack of information, Acquisti and Grossklags (2005) suggest that it may be useful to consider potential biases that people may be unconsciously applying when attempting to make a decision under

uncertain conditions. These biases can lead individuals to believe that the benefits far out-weigh the costs (even when this is not true), as is often the case when a person is asked to share information with a company. This bias has been described as the 'availability heuristic' (Tversky & Kahneman, 1982 p.20). People use heuristics as a way to 'reduce the complex tasks of assessing likelihoods and predicting values to simpler judgemental operations' (Tversky & Kahneman, 1974 p.1124). In the case of tradeoff decisions, the availability heuristic suggests that when we are trying to assess how likely something is to happen, we attach a greater probability to instances that we can recall more easily. Therefore, in a situation where an individual is being asked to share information, if they can remember someone they know having an issue after sharing data, they would be more cautious. In situations where no real-life examples are forthcoming, an individual may move onto 'imaginability' (Tversky & Kahneman, 1974 p.1127), which is similar except that the bias is towards instances that the individual can more easily imagine (rather than recall). In both of these instances, bias can play a role and due to this, the individual may be overly cautious or not cautious enough depending on how easily they are able to recall or imagine the benefits and costs of following a particular course of action. This suggests that while tradeoff decisions appear to be rational to the individual making the decision they could be a reflection of biases held. It is also important to note that behavioural economics recognises that the rational actor model is limited and as such does not necessarily govern every decision that we make (Hogarth & Reder, 1987).

Nissenbaum (2010), however, suggests that contextual integrity itself is a decision heuristic. She argues that when there is a proposed change to socio-technical

systems and/or practices people respond in various ways, and these responses are prompted by contextual integrity. Essentially, if a new system is proposed and an individual's response is feelings of discomfort, it is likely to be because there is the potential for a violation of contextual integrity to occur. What is happening in this situation is that the current practice is being compared with the new practice under the guise of contextual integrity and thus concerns centre around the 'context, actors, attributes and transmission principles' (Nissenbaum, 2010, p.149). However, this is not something that necessarily happens on a conscious level, but because the framework of contextual integrity is integral to how people interact with each other, it nevertheless happens. This may also explain why it is so difficult for people to express the concern they feel when systems change, because they are unaware of contextual integrity on a conscious level. This is because it is 'rooted in convention, habit and custom' (Nissenbaum, 2010, p.164) and so is not necessarily something that individuals consider, due to its subtle nature. However, it will manifest itself in feelings of discomfort when the contextual integrity of a situation is being threatened.

Similarly, Lyon (2000 [1994]) also suggests that individuals find it harder to be concerned about the negative aspects of commercial surveillance if they have never suffered an invasion of privacy. This also links with the suggestion (Solove, 2009) that the benefits of reduced privacy, such as greater convenience, are often easier to express, than the potential issues. This is because people tend to feel uneasy when they have privacy concerns, but struggle to express exactly where this feeling of unease has come from or what it relates to. Garfinkel (2001) suggests that this could simply be because individuals have become used to this kind of data collection and so it is not really at the forefront of their minds,

especially as so much of it occurs in the background of our daily lives. It has become taken for granted to such an extent that we only tend to think about it when an issue occurs (Lyon, 2005 [2001]). This suggests that individuals only consider their privacy after it has potentially been violated, this is borne out in the concern expressed around the reporting of various data hacks in the media (BBC News, 2015a and BBC News, 2015b) and more recently, the Cambridge Analytica Scandal (Cadwalladr & Graham-Harrison, 2018).

However, this is not the only issue to consider when examining the tradeoff decision-making process. Another factor which complicates this process is that issues around sharing information tend to offer an immediate benefit versus a future cost (Acquisti & Grossklags, 2005 and Stoilova, et al., 2019b). Economists believe that we are '*time consistent'* (O'Donoghue & Rabin, 2000) and so we will make the same tradeoff decision regardless of when we will have to face the negative consequences of that choice. This highlights the issue that individuals have with immediate gratification more generally. O'Donoghue and Rabin (2000) suggest that we all struggle with self-control and as such have a tendency towards immediate gratification; they take issue with economists' assumption that we are all '*time-consistent'*. O'Donoghue and Rabin (2000) suggest that people tend to be *'time-inconsistent'* (p.233), meaning that they err towards immediate gratification and do not make the same decision at different times. This suggests that we are not as rational as we appear or would potentially wish to be. Therefore, even when we feel that we are in control, this may be an illusion, hidden by our biases or how soon we will have to face the consequences of our actions.

Research by Turow, Hennessy and Draper (2015) challenges the suggestion that individuals choose to share information with companies based on a trade-off between privacy and preferential treatment. Instead they put forth that individuals are actually resigned to the collection of their data, and in fact feel so overwhelmed by the volume of data collected that it has led to feelings of powerlessness. Turow, Hennessy and Draper (2015) contend that individuals often do not have enough information to enable them to make trade-off decisions and so can never be the well-informed decision-makers they are purported to be. This links with the above discussion regarding the issue of onerous terms and conditions and suggests a lack of control for individuals. Worryingly, they even go so far as to suggest that those who know the most about the level of data collection actually tend to be the most apathetic, which offers a potential explanation for Gordon's (2003) above findings. This is important as often companies take the use of their products as being tacit acceptance of an unspoken bargain between the two parties, however, this research suggests that the opposite is true, individuals use these products *in spite* of the reduction in privacy, not because the loss of privacy is deemed to be beneficial. The situation appears to be one in which we have very little control, suggesting that we are unable to have the level of privacy we would like, or to have any level of autonomy. Finally, it is important to note that for Nissenbaum (2010), there is no tradeoff decision to be made. Tradeoffs suggest that some privacy must be lost in order to gain an increase in another characteristic, such as convenience, however, under the contextual integrity framework, it is merely a case of information flowing in the prescribed way for that context, adhering to the expected and accepted norms, without issue. This means that there is no need for tradeoffs to occur as each context is already balanced.

As noted above, aside from the type of information being shared, the context in which it is shared can also have an impact. Although previously, it was relatively straightforward to maintain different contexts separately, this is becoming more problematic as the issue of 'context collapse' (Vitak, 2012 p.451) demonstrates. The potential for context collapse links with Goffman's (1990 [1969]) conception of the 'front' (p.109) and 'back' (p.114) regions, suggesting that our carefully choreographed performance in the 'front region' can be undermined if conflicting information is revealed to others. Due to increasing issues of social convergence (boyd, 2008), whereby numerous contexts overlap, individuals must now manage different contexts simultaneously which is not only stressful, but also potentially damaging. Nissenbaum (2010) also recognises the potential for conflict as people attempt to negotiate numerous contexts, often simultaneously. However, she argues that the real issue here is that 'the norms from one context prescribe actions that are proscribed by the norms of an overlapping context' (p.157), thus furthering her belief in contextual integrity and the rules that govern everyday situations. However, she is unable to offer solutions for when these conflicts occur, as they are often specific to each individual situation and as such cannot be generalised. In some cases, it may not be possible to find a resolution and so become challenges that everyone must face.

Context collapse can also be said to occur when information is aggregated as discussed previously. This is a form of context collapse, in that information that has been shared in different contexts is joined together to create a profile of an individual, without that person's consent or awareness. When data is aggregated in this manner, individuals become reduced to data points which can then be

reconfigured continually to look for particular patterns and correlations (Miller, 2016 and Cohen, 2017). It is also necessary to consider how individuals may share different pieces of information with various companies, never once considering that this data could become linked in one large profile and used to make assumptions about them. This can lead to issues particularly around how individual pieces of data on their own may not be particularly revealing, but when they are linked together in a profile, they can reveal a lot more than was intended when the information was shared initially. This is particularly worrying when considering that this data can be used to predict traits that the individual has not chosen to share (Gadzheva, 2008; Pierson, 2012 and Seneviratne et al., 2014). For example, when using a single piece of data (Facebook 'Likes'), a study was able to predict with reasonable accuracy various pieces of data which had not been explicitly shared, such as sexual orientation and religious beliefs (Kosinski, et al., 2013). While there were varying levels of accuracy in terms of what could be predicted, this demonstrates how individuals may share far more than they intend or consent to, when their data are aggregated into a single profile. This offers an example of context collapse which the individual concerned may be completely unaware of, although they will potentially have to deal with the repercussions of decisions made based on the aggregated profiles or inferred information.

As discussed throughout this literature review, this highlights a lack of control as individuals choose who to share information with initially, but once they have done so, control is lost as data is matched with other information shared with other organisations at different times and under different circumstances. It is also problematic in that any additional information that is inferred, even if it is correct,

it is not information that has been freely given by the individual concerned. Therefore, it is difficult to argue that control is something that people can be confident they have in terms of their internet privacy.

Summary and research questions

Much has been written about privacy, and despite changing conceptions, it remains a contentious issue. This literature review has examined various aspects of privacy in order to build an understanding of its complex nature. The three main sections dealt with various positions relating to privacy. In the first section I discussed the concept of privacy itself, with particular focus on how various theorists have attempted to define it (Westin, 1970; Nippert-Eng, 2010 and Spinello, 2017 [2003]). This led to an examination of the divide between public and private areas, where there is a considerable lack of agreement. This divide is not straightforward and the issues with it were discussed at length. This highlighted the problematic nature of this divide.

The second section focussed on commercial surveillance, and in particular, the issue of control, in terms of the collection of data. It began by discussing the commodification of individuals' data, which has led to large profits for social networking sites, amongst others. It also recognised how the use of online social media platforms has become a part of many individuals' everyday lives and as such requires critical examination. This led to a discussion of how our relationships are mediated through the online platforms that we utilise (Bucher, 2018). Next, I considered Foucault's work on discipline (1977) and how it has been utilised and updated by various theorists to offer explanations of how

commercial surveillance can be said to shape our behaviour online. This was followed by a discussion on to the aggregation of data and how this can reveal more about an individual than intended (Kosinski, et al., 2013 and Miller, 2016). This led to an examination of the debate around user exploitation. The final sub-section considered whether it is possible for users to gain increased control over their information and considered the opportunities available to individuals through small 'act[s] of defiance' (Fiske, 1989 p.9 and de Certeau, 1988).

The final section considered issues around the context in which an individual is being asked to share information, and what impact this can have. In particular, I focused on Nissenbaum's (2010) work on contextual integrity and the framework it offers in terms of offering an explanation for differences in responses from individuals when considering sharing information. It highlighted Nissenbaum's focus on the contextual norms related to a situation and considered this to be one of the defining factors in terms of the information we share and how we feel about it. Within my discussion of context, I also considered theories around the categorisation of information, with specific focus on the work of Raynes-Goldie (2012) and Floridi (2005). Both offer new ways of considering the categorisation of information and potentially explain why concerns may differ with regard to the type of data being requested.

The second sub-section considered alternative explanations for why an individual might be happy to share information in one situation but not another one. This included the 'privacy paradox' (Utz and Krämer, 2009), which is used to describe the difference between how people talk about privacy concerns and how they tend to behave. This was followed by an examination of the suggestion that

individuals make tradeoff decisions regarding the reward or benefit they will receive if they share information (Nippert-Eng, 2010 and van Dijck, 2018). Finally, this section considered the issues that can arise from 'context collapse' (Vitak, 2012 p.451), whereby previously separate contexts overlap, which can result in conflicting information being revealed.

As discussed in the introduction to this chapter, despite various social media scandals regarding user data being shared without consent, such as the Cambridge Analytica Scandal (Cadwalladr & Graham-Harrison, 2018) and the claims made by Edward Snowden (Greenwald, 2013), social networking sites continue to thrive. This raises questions regarding whether people care about privacy, and where privacy is considered, whether social connection is deemed to be more important than a potential loss of privacy.

As examined throughout this literature review, there has been a great deal of research carried out relating to individuals' privacy and how they behave in relation to protecting it. However, much of this research has left questions unanswered, particularly in relation to how people feel about privacy, and how they conceptualise it. It is clear that there is no overriding view of what privacy is, therefore, it is necessary to examine how individuals consider privacy in their daily lives. This raises questions regarding when it matters, when people are unconcerned about privacy and what they are willing to share and under which circumstances. At the root of this is whether individuals care about privacy in their day-to-day lives, the lack of resistance cited above suggests that they are unconcerned, but is this the case? Do they feel overwhelmed and powerless, or are they ultimately content with the amount of privacy they have? Do people

believe that to have more privacy would be to compromise their social relationships? With this in mind, my research questions are as follows:

- How much control do individuals feel they have over the information they share in their daily lives?
- How do individuals feel about the amount of information they share with companies and online?
- How do individuals negotiate the boundaries of internet privacy?
- In what contexts is privacy important to individuals?

These questions are designed to explore not only how individuals feel about the current pressure placed upon them in terms of sharing their information, but also to consider these issues at a more granular level. As discussed in this literature review, considering context and how it relates to privacy has been considered previously, however, my project attempts to update this work by examining how people feel about different contexts, and which situations elicit greater concern than others. By considering how individuals navigate the boundaries of internet privacy, I will highlight the considerations made to demonstrate that people do not simply consider their data privacy, but also take action to honour their boundaries when they deem it necessary.

Chapter Two: Methods

Introduction

The introduction outlined the issues at stake when considering how individuals negotiate the boundaries of internet privacy, while the literature review examined the current knowledge and identified the gaps that exist. This methods chapter will establish my methodological approach and how it answers the research questions. This project employs a broadly qualitative approach comprising of 26 qualitative interviews, which cover topics around sharing information online, how individuals attempt to maintain control over their data and how they feel about the types of information potentially being shared. The interview analysis is used to inform 359 quantitative surveys which explore issues regarding sharing information online, the collection of data, control, trust and context.

This chapter will be separated into six sections (plus a conclusion at the end) which discuss the methodological approaches taken in order to answer the research questions. At each stage, justifications will be given for the decisions taken. Following a reminder of my research questions, the overall research design will be discussed, specifically dealing with the use of intensive and extensive research methods and how despite appearing to follow a mixed methods approach, I define my research as broadly qualitative. The second section of this chapter will become more focused on the methodological tools employed, specifying the sampling strategy before the third and fourth sections each detail the interview and survey designs. In the penultimate (fifth) section, the research analysis will be explored, providing details of categorisations made and methods utilised. In the sixth section, I reflect upon my role as researcher, paying particular attention

to any potential influence I may have had on participants while carrying out interviews. Here, consideration will be given to the 'emotional labour' (Hochschild, 2003 p.ix) that I was required to engage in for the benefit of the project, in addition to the ethical implications of the research. A conclusion will be drawn at the end, which will determine the success of this project, particularly in light of the methods I employ.

As discussed in my literature review, while there is a wealth of knowledge in the area of data privacy, there are areas which would benefit from further exploration, particularly in terms of issues around the concept of context and data that is shared with online organisations as well as through social media. Therefore, the intention of this research is to find out how participants perceive privacy when sharing information and discover when it is important to them (and when it is not). With this in mind, the research questions are as follows:

- How much control do individuals feel they have over the information they share in their daily lives?
- How do individuals feel about the amount of information they share with companies and online?
- How do individuals negotiate the boundaries of internet privacy?
- In what contexts is privacy important to individuals?

Research design

Intensive versus extensive methods

Intensive and extensive methods are appropriate for different types of investigation with different kinds of research objectives. Broadly speaking, intensive methods involve few cases, collecting in-depth data, aiming to understand specific cases. Extensive methods, on the other hand, tend to consider a large number of cases, aiming to offer generalisable information. Although they generate different types of data, it is possible, where appropriate, to combine intensive and extensive methods, so that stronger inferences can be made. Combining methods can also be useful, if done in such a way that the strengths of each method ameliorate the weaknesses of the other (Johnson & Turner, 2003 and Cresswell, 2014). This means that while intensive methods offer more detailed information, which can provide explanations for social phenomena; extensive methods, can give an indication of how widespread opinions are (for example) amongst a particular group, thus adding robustness to the research. It is also important to remember that some 'social phenomena cannot be fully understood using either purely qualitative or quantitative techniques' (Teddlie & Tashakkori, 2003 p.16), therefore, it is sometimes necessary to employ both methods, which offer a more rounded research project than employing a single method. This is the case with my project, which required both intensive and extensive methods to gain a fuller picture of the issues outlined by the research questions. However, while I have employed traditionally qualitative and quantitative methods, my approach remains qualitative in nature, rather than mixed methods. This approach will be outlined in the next sub-section, and I will offer a justification for this choice.

Methodological approach

Historically, qualitative (intensive) and quantitative (extensive) methods have been considered to be separate methods which are difficult to combine due to the fundamental differences that exist between them (Spicer, 2016). In order to answer my research questions, I utilised both qualitative and quantitative methods sequentially, with each method offering different qualities. Qualitative methods make sense in terms of learning more about how individuals feel about their level of control and the amount of data they share. It is also useful to employ qualitative methods to uncover how people negotiate the boundaries of internet privacy. Qualitative methods are useful here, as they allow participants to provide explanations for their views and beliefs, thus allowing the researcher to gain in-depth knowledge. The results from the qualitative phase support the design of the secondary phase of my project.

Turning to my research questions it is clear that qualitative methods offer the most appropriate way to answer three of my research questions, however, for the final question (*In what contexts is privacy important to individuals?*) quantitative methods offer the most appropriate way of capturing data. Due to the individualised nature of context, using qualitative methods to investigate context could generate a different response for each person, and to explore a list of situations and ask each participant which of the situations would cause them concern would be tedious for interviewees and may cause disengagement (and a poor experience for them). However, by offering various combinations of information and audience within a quantitative method allows me to look for patterns in the data and to clearly see where there are areas of convergence or

divergence and to consider why this might be. It also allows the overall importance of context to be gauged, as participants are able to rate their level of concern for the context questions. Therefore, quantitative methods offer the most appropriate way of understanding the importance of context and when it is or is not important to participants. However, it is also important to note that responses from the extensive phase will be helpful in supporting responses to the initial intensive phase, therefore the usefulness of this phase is not limited to the final research question.

I begin with a qualitative method, which allows me to gain in-depth knowledge of participants' views, this is then analysed and directs the design of the quantitative phase of the project. The analysis of the intensive data allows the quantitative element to be moulded to ensure that it deals with issues that are important to participants, rather than what I assume to matter to them and ensures that the relevant variables are included in the quantitative phase of the research (Cresswell, 2014 and Spicer, 2016). This is particularly relevant to the exploratory nature of the project, as it allows a research tool to be developed to measure the strength of opinion from participants, which can then be developed further for future research. Therefore, the information provided by the participants in the first phase of my research is vital to the development of the second phase of research. It is important to note that while the qualitative stage is utilised in the design of the quantitative stage, it sets the tone and topics to be explored further here, rather than the detail of how the topics are to be measured by the quantitative tool. My project is sequential in nature, and broadly speaking, the design of each phase is not integrated and so each dataset maintains its original form and is analysed separately (further details of which will be provided

in the analysis section). However, the results themselves were merged 'at the point of inference' (Greene, et al., 2012). Therefore, although each phase of data collection is carried out separately, there is a link between the phases in that the qualitative phase directly impacts on the quantitative phase as the design topics are based on the initial analysis. Also, when reporting on my findings, the results of each phase are discussed together, rather than in separate sections, thus integrating the different methods. To the casual reader this may appear to suggest that I have utilised a mixed methods approach, however, this is not the case; my approach is broadly qualitative. Although I have used quantitative methods, I have limited my analysis of these to descriptive statistics and bi-variate analysis. The way in which I have employed the results of this analysis is qualitative in nature, especially as I have merged it with the qualitative analysis when considering what my data is telling me. Also, quantitative analysis tends to focus on creating models and predicting how groups of individuals will behave in particular situations, however, I have not done this, rather I have used all of the data that I have collected to posit suggestions and lay a foundation upon which future research can be built, therefore my focus is qualitative. Up to this point, I have offered general information regarding the types of research methodology employed, the next section will offer more detailed information regarding specific methods that I utilise in order to answer my research questions.

My project

As discussed above, this project employs a broadly qualitative approach which utilises tools traditionally defined as qualitative and quantitative, thus providing the most effective way of answering the research questions. In this section I provide further details of the precise methods utilised.

My preference in terms of qualitative method is interviews, as they allow specific questions to be directed towards the topic of interest, ensuring that the data collected will offer an answer to the research questions. They also offer the ability to capture participants' views on specific topics, and even to allow them to highlight situations in which their behaviour may not align with their beliefs and offer an explanation for this. It also allows the interviewer to probe responses given for additional information and/or clarification.

As stated previously, I employ both qualitative and quantitative methods to answer the research questions and this allows a more rounded approach than either of these methods would offer on their own. The use of interview analysis to inform the surveys was vital as it meant that I did not rely on my preconceptions and thus omit an issue that may be important to participants (Babbie, 1973). As such the interviews steer the survey in the direction of participants' concerns, rather than those they are assumed to have. This larger survey allowed me to gain broader views regarding internet privacy, in particular considering the contextual responses given, which would have proved much more difficult to do in an interview scenario without becoming repetitive. It also facilitated the collection of a wider range of views and allowed me to consider demographic differences in terms of gender and age group. However, it is important to note that the surveys were not used to 'test' the interviews, rather the aim was that each research tool would complement each other and work as a means of what Mason describes as 'mutual verification' (2002 p.18), not only allowing the comparison of 'different forms of data on the same subject', but also to 'generate theory' (Mason, 2002 p.18). As such, it provides a useful way of highlighting areas of convergence (as well as difference) between participants and

ensures that participants as a whole are less homogenous, thus removing some of the inherent issues with snowball sampling, as discussed below.

It is important to note that the use of multiple data collection methods does not necessarily improve the quality of the research findings. As such, it was important to ensure that both methods were integrated into the research, rather than being treated as separate entities, to ensure that there was value to utilising them both. The survey depended on the analysis of the interviews, as this gave the survey its focus and highlighted which areas should be probed further and which did not require additional examination. Without utilising the interviews in the survey design, the survey may have missed information of great significance to the research population and as such would be incomplete. Therefore, employing both methods ensured that this did not happen. By utilising both qualitative and quantitative methods, the intention was that each would mitigate any issues related to the other method, and as such they would provide a more rounded research project.

Sampling strategy and saturation

The sampling framework utilised for the interviews is a non-random, convenience sample in that there was a specific group that was of interest, due to their relevance to my research questions (Mason, 2002). I wanted to speak to participants who are aged between 20 and 40, use social media and own a smartphone. I chose this specific age range as much of the previous research has focused on teenagers (boyd, 2014; Marwick & boyd, 2014 and Pangrazio & Selwyn, 2017,), undergraduate students (Culnan, 1993; Spiekermann, et al., 2001;

Metzger, 2004; Acquisti & Gross, 2006; Tufecki, 2008; John, et al., 2011; Stutzman, et al., 2012; and Young & Quan-Haase, 2013), or, older participants (Braun, 2013 and Eleuze & Quan-Haase, 2018). This means that those aged 20-40 years old are rarely the sole focus of research, which led me to consider whether this age group represented something significant in terms of the way they think about their data privacy. This age group was of particular interest as it encompasses those who have grown up with the internet and those who remember a time before the internet. Also, recent data suggests that this age group is particularly active on social media, with the largest concentration of Facebook users in the 18-44 age group (Statista, 2019), suggesting that those in this age range are those that could be said to have the most at stake when we consider issues around data privacy and negotiating the boundaries of internet privacy. They are also of particular interest because as noted in the literature (boyd, 2014), it is often assumed that the sharing of data is a sign of an acceptance of a reduction in privacy, however, this project is exploring the complexities of this, particularly in light of the 'tradeoff fallacy' (Turow, et al., 2015). Therefore, as the research questions are exploring attitudes towards data privacy, it is relevant to speak to those who share their data and given the nature of the vignettes, (which will be discussed in greater detail later) it was more likely that those within the 20-40 age range would have experience of using the services discussed.

As well as the sampling framework, when determining the robustness of a piece of research, sample size is also considered. Sample size is a contentious issue and broadly the small sample sizes characteristic of extensive interviews can lead to concerns regarding representativeness which can make it difficult to carry out enough in-depth interviews for the results to be generalisable. However, it should

be noted that this project does not intend to be generalisable as it is exploratory in nature (Mason, 2010), and as such, the aim is for me to develop theories regarding individuals and their data privacy. As discussed above, the themes emerging from the interview stage of the research were used to generate the topics for the larger survey (which will be discussed in further detail below) and so when analysing my results, the aim was to reach 'theoretical saturation' (Glaser and Strauss, 1967 p.65).

Saturation offers an alternative measure to that of representativeness and occurs at 'the point at which no new information or themes are observed in the data' (Guest et al., 2006 p.59). There are various perspectives on the point at which saturation occurs but it is important to ensure that the sample size is not so small that theoretical saturation cannot be achieved, while, not so large that analysis is impossible due to an overwhelming amount of data being collected (Mason, 2002; Kvale, 2009 [2007] and Onwuegbuzie & Collins, 2007). Given the type of sample that I utilised, I offer a suggestion of how things might be, when we consider how people negotiate the boundaries of internet privacy. Therefore, I utilised saturation as a way of deciding when enough data had been collected, employing NVIVO to assist in the identification of themes. The use of NVIVO was key in identifying when saturation had occurred, as it allowed me to identify the themes emerging from the data and recognise when new themes ceased to present themselves. At this point, it was clear that saturation had been achieved. The identification of themes and coding of responses will be discussed in greater detail in the analysis section of this chapter.

The same sampling framework was utilised for the survey, as for interviews and as such this limited participants to those who are aged between 20 and 40, use social media and own a smartphone. This is because I want to explore whether the views uncovered during interviews could be said to be those of a wider group of people with similar characteristics. Therefore, it would not make sense to choose a different group, as their concerns may differ from those originally interviewed by virtue of them being characteristically different. However, having identified the pertinent themes in interviews, it is also important that the same participants did not complete the survey, as this would merely serve to duplicate the initial results and would have offered no new information and might 'introduce confounding factors into the study' (Cresswell, 2014 p.226).

Due to the nature of the sample, survey results are not generalisable and as such are only intended to be indicative of issues which may warrant further investigation. The purpose is to examine the contemporary concerns of individuals in terms of their data privacy and how they negotiate the boundaries of their online privacy. My particular interest in the contextual aspects of privacy mean that work of this nature has rarely been carried out previously and so generalisability is not a realistic outcome. The survey is cross-sectional in nature (Babbie, 1973) and so offers a snapshot of respondents' views at a particular point in time, while also allowing patterns of association to be identified. This is a potential limitation as it offers no information regarding how opinions and attitudes have changed, in response to the Cambridge Analytica scandal, for example. However, this study has allowed me to develop preliminary theories in this field which may inform future research in this area.

Interview design

As discussed above, interviews were utilised initially for collecting data as they provide interviewees' interpretations of the world, which can be extremely difficult to access in any other way (Lawler, 2002). However, they do not come from the individual, rather, 'culture provides a repertoire' (Lawler, 2002 p.242) of acceptable narratives which individuals are able to choose from in order to tell their story. The narratives offered by my participants tell me how they view the world and their place within it, and as such, this research is interpretivist, as it focuses on individuals' interpretations of the world (Lawler, 2002). Broadly, I approach this research from an 'adaptive theory' (Layder, 1998, p.viii) perspective, which offers an alternative to other, more well-established perspectives. This approach allowed me to utilise the data from the initial stages of my research to shape the next phase of the research, while at the same time leaving the initial research open to adaptation should I uncover new perspectives in the latter stages of my data collection (Layder, 1998). Therefore, the interviews provided provisional theoretical models, against which I was able to design my surveys, while still being able to feed the data from my surveys back into the analysis process, if necessary. This means that I was able to consider pre-existing theory, and utilise my data to refine it, rather than ignoring prior concepts, as grounded theory requires (Layder, 1998). By taking into account the existing theories, and merging them with my emerging data, I was able to generate new theory which bridges the gap between what has gone before and what I have discovered.

Using my research questions as a guide, I carried out 26 structured interviews, whereby participants were asked the same set of questions, in the same order. The majority of these interviews were face-to-face, although it was necessary to conduct four via FaceTime/Skype and one via telephone. The face-to-face interviews tended to take place in public places such as libraries, cafés, and on the University of Kent campus, I generally tried to accommodate locations that were convenient for the participant. All interviews were voice recorded utilising my iPhone, and lasted an average of 36 minutes, with the longest interview lasting 1 hour and 15 minutes and the shortest being 19 minutes long. Most of my interviewees were female (61.5%), the overall ages range from 23-40 years old, with a mean age of 31 years old; the majority of my participants were aged between 30 and 40 years old (57.7%). Although I attempted to recruit participants using traditional methods such as displaying posters in public places and asking friends and family to display the recruitment poster at their workplaces, this led to the recruitment of a single participant. Therefore, it became necessary to utilise other methods, such as social media (Facebook and Twitter) and word of mouth. As such, I asked friends and relatives to share the recruitment poster via their social media pages or to mention my research to any friends or family that they thought may be interested in taking part. I also posted details of my research in various groups on Facebook including the University of Kent and British Sociological Society Post Graduate forum, in an attempt to reach a wide range of participants. As an incentive, I offered participants the opportunity to be entered into a prize draw for a £25 iTunes (or similar) voucher. I utilised snowball sampling to recruit additional participants by asking interviewees if they knew anyone who may be interested in participating. Although there are potential issues with using snowball sampling, in terms of participants either knowing each

other and/or being a homogenous group (Mason 2002), I attempted to ameliorate this by also sharing my recruitment information amongst various groups on social media as well as asking those I knew to share it and as such did not rely solely on snowball sampling. This also allowed for geographical diversity, as I was able to reach individuals who did not live or work locally, which should have increased diversity. I am aware that given the self-selecting nature of my recruitment, there is also the potential for self-selection bias, in that only those who are particularly concerned about or interested in issues around internet privacy would have volunteered to take part, however, this was not necessarily the case. A number of my participants spoke of their lack of concern regarding privacy and mentioned that they had not given the topic any more than a cursory consideration prior to the interview taking place. It is also important to remember that there are a number of reasons why an individual may choose to participate in research, such as enjoying the process itself and the opportunity to 'explore their own thoughts and feelings to an interested and respected other' (Clark, 2010 p.406-407). Therefore, while participants may have had a particular interest in the topic, it is also possible that it was something they wanted to explore for themselves during the interview.

The interviews follow a specific structure, with each participant being asked the same questions in the same order. This was important because the addition of new questions could generate new themes, which would have hindered my ability to reach saturation. The questions posed were narrow to begin with, so as not to overwhelm participants by asking a broad question that would be difficult to answer (the interview schedule is included as Appendix C), however, follow-up questions were asked, where needed, and this encouraged participants to provide

further details. The interview schedule went through a number of iterations and was tested with a number of volunteers to ensure that the questions were appropriate and allowed me to gain useful insights into how people might interpret them. When refining my interviews, I spoke to individuals with varying levels of expertise in terms of carrying out research, including fellow postgraduate students at the University of Kent, but also others who have not had any research methods training and were representative of my potential participants. Following the standard interview questions, participants were asked to consider a number of vignettes, to gain an insight into the role context might play in decisions around data privacy.

Vignettes

Vignettes were initially suggested to me by my supervisors during one of our early meetings and were deemed to be a useful and interesting part of my data collection. After I had completed my interviews, I discovered recent research that had utilised vignettes in order to explore concerns around sharing different types of data in different situations (Rainie & Madden, 2016). This highlighted the importance of using vignettes in this area and provided confirmation that I was not alone in employing this research tool. Following much deliberation, five vignettes were employed during the interviews to examine how participants feel about privacy when considering particular scenarios. These were included as a way of making the potentially abstract topic of data privacy more tangible for participants by asking them to consider detailed, specific situations. Vignettes were used because they include all of the complexities related to real-life situations and allow individuals to explore and talk about values as related to that situation (Lee, 1993; Barter & Renold, 1999 and Jenkins, et al., 2010), while

giving an insight into their normative values. As such, they offer respondents the opportunity to consider a situation in a more reflective way than may be possible in their daily lives. These vignettes offer a number of situations in which a piece of information was shared and varied in terms of whether the information had been illegally accessed or was being requested by a company through an app. The vignettes will be included in the appendix with the interview schedule (Appendix C).

The vignettes are based on real-life situations, which had either been reported on in the media or heard anecdotally; this is important because they will elicit a more realistic response if participants believe them (Hughes & Huby, 2004; Jenkins et al., 2010; Bradbury-Jones et al., 2012 and Jackson et al., 2015). The scenarios remained the same for each interview, as with the preceding questions, this was partly to assist in the identification of the point at which saturation was reached, but also to allow comparisons to be made between participants' responses to identical situations. This allowed me to 'highlight areas of commonality and disagreement within and between' (Jackson, et al. 2015, p.1405 and Barter & Renold, 1999) participants. For this reason, the vignettes were followed by a simple, open-ended question, asking participants in very broad terms, what they thought of the situation, this allowed individuals to discuss their views and feelings, without being directed in a particular direction by the interviewer.

Following the discussion of the five vignettes, participants were asked to rank them in order from those they would be the most concerned about to those they would be least concerned about. This highlights a contextual element when individuals consider their data privacy, because the vast majority of interviewees

had very little issue with ranking the types of information and offering explanations for their decision. This also allowed me to compare how different individuals ranked different pieces of information which meant that it was possible to identify pieces of information where there was agreement in terms of their importance. This is also useful because the vignettes illustrate to participants which pieces of data are available to others and so allow them to consider what may be known about them, while defining which pieces of data matter the most to them. This was also interesting because even those who had given little thought to their privacy prior to the interview had little difficulty in ranking the vignettes, suggesting that while it is not necessarily something that is at the forefront of their minds, they do consider it on some level.

The vignettes were based on a combination of anecdotes I had heard from friends and a number of real-life news stories which were amended so as not to be exactly the same as the original news story but would make sense to the participants. As with the interview questions, these vignettes went through several iterations, with a pilot of the scenarios being carried out with a volunteer to check that they made sense to someone not involved in the research project. Following this, a small focus group was conducted with fellow postgraduate students at the University of Kent, during this, both the interview schedule and vignettes were discussed. This allowed the ordering and content of them to be considered to ensure that these research tools were appropriate to examine the issues outlined by my research questions. This led to further consideration of what was meant by key phrases and the interview schedule and vignettes were much improved from doing this. Towards the end of the design phase, a final pilot interview was carried out with a volunteer, who was treated exactly as participants would be. The only exception

here is that the interview was not audio-recorded, as the volunteer did not consent to this and it was not deemed necessary, as the research instrument itself was the focus of this exercise. Both parties reflected on the interview immediately afterwards, and this led to an additional question being added. This iterative approach to designing my research tool was vital to ensure that the interview experience was worthwhile for participants and myself. As discussed previously, the interview responses supported and directed the design and development of my online survey which will now be examined.

Survey design

The themes identified during the analysis of the interviews were used when deciding on which topics my survey should cover. When designing my survey, I also utilised previously carried out surveys, as these are instruments that have been tested and were relevant to the topics I was exploring. Although some of these questions were taken from prior research verbatim, this was rarely the case, and I often utilised my own phrasing or used the question but supplied different response options. The questions that were inspired by previous research included questions related to the measures individuals had taken online to protect their privacy, questions regarding the supplying of false information or refusing to supply information to companies. I also utilised previous research when working on the questions regarding tradeoff decisions - sharing data to receive personalised recommendations, access free services or whether the participant would be willing to pay to share less information (Dommeyer & Gross, 2003; Madden, 2014; Shelton, Rainie & Madden, 2015 and Rainie & Duggan, 2016). Other questions were related to whether participants would like to have more

control, how they feel about their information being passed on to third-parties and the questions in the Trust section of the survey (Madden & Rainie, 2015 and Rainie & Duggan, 2016). These questions offered a useful basis and gave me greater confidence when developing my own instruments, as I was able to utilise these questions to guide my survey design. It is also important to note that responses from my interview participants were utilised when I was developing the response options to questions regarding issues previously experienced around privacy and measures that participants had taken in order to protect their privacy. The format for the context question was brand new as little work had been carried out in this area, in the same way that I was doing it, and as such there was no prior data collection instrument that could be used to form a basis for this.

The design phase of the surveys also allowed me to utilise the skills I had gained while undertaking my Research Methods Certificate, particularly the Quantitative Methods unit. This allowed me to consider the response options offered to participants and contemplate what I was attempting to measure and whether the options would offer a reliable tool with which to measure it. While the vast majority of the questions did measure what I was attempting to, looking back at the survey questions I can see now that the first question (regarding how often the participant thinks about their online privacy) did not. This question was attempting to measure the frequency with which participants consider their online privacy, however the options offered do not necessarily correlate with this and it is clear that it is possible that there are situations in which more than one of these responses could have been true, despite the survey allowing only one response to be selected. This is something that will be given more attention in the future.

My survey was carried out online, hosted by Qualtrics. It was launched on 1st December 2017 and closed on 28th February 2018, during this time, 373 individuals took part, and after data cleaning, the number of participants was reduced to 359. It is also important to note that none of the questions in the survey were compulsory, this was a decision I made to reduce the burden on participants who may decide not to complete the remaining questions in the survey if they were faced with a compulsory question that they did not feel comfortable answering. I did however attempt to mitigate this by offering the 'Prefer not to say' option, however, participants were still able to move on to the next question without selecting a response. Given the issues I had with recruiting interview participants, I recruited survey participants via social networking sites, through a page I set up on the 'Call for participants' website and by asking friends and relatives to forward the link to my survey within their workplace, via email. The most successful method of recruitment was Twitter, which yielded 59.2% of my respondents, followed by those who were forwarded the link via email (19.5%). The success of recruitment via Twitter was due to asking those I knew to re-tweet my link (as well as tweeting it myself), In addition to this, I sought a number of Twitter users with a large number of followers to retweet the link to my survey, many of them did this, and so this increased my response rate. As with my interviews, I offered participants the opportunity to be entered into a prize draw for a £25 iTunes (or similar) voucher, as an incentive. The criteria for eligibility was the same as for the interviews, in that participants had to be aged 20-40, own a smartphone and use social media. As with the interviews, the majority of respondents were female (67.2%), 2% identified as non-binary and 1.6% did not reveal their gender. Interestingly, while the majority of interview participants were aged 30-40, the opposite is true for survey participants, with

54.7% being in the 20-29 age group, and 43.5% being in the older age group. As participants were given age-bracket options for this question, it is not possible to calculate the mean age of survey participants. It is also not possible to offer any information regarding where participants live or their nationality, as this was not something they were asked to reveal. Also, given that the focus of my research is data privacy, it was important to me that participants remain anonymous, and so I did not enable Qualtrics to collect any information in the background that could have been used to infer nationality. This is something that in hindsight could have been interesting and useful to collect, particularly given the different concerns regarding privacy in different countries (Costa, 2018), depending upon the overall context nationally and the level of privacy individuals expect. However, as my survey was in English, I would assume that my participants were largely from the UK, and if not, certainly English-speaking countries; it is clear from the free-text responses that everyone who typed in comments understood English well enough to complete the survey. Therefore, it could be argued that my research serves to increase the volume of data that exists regarding Western conceptions of privacy and as such fails to take account other, more diverse uses and conceptions (Costa, 2018). Due to the use of social media as a recruitment method, it is impossible to calculate the response rate for my surveys, as I am unable to measure how many people saw my survey and thus how many people chose to participate or not. However, where response rate appears to be an issue for specific questions, this will be dealt with in the discussion around that question.

The survey took the form of an online self-completion questionnaire, which offered various advantages, particularly in terms of reducing social desirability bias, as there is no interviewer present and so the participant may be less inhibited

in their responses. It also offered greater convenience for the respondent as they could choose when to complete the survey, rather than having to agree on a designated time and place with an interviewer. There are, however, issues with this method, in that due to the absence of an interviewer, no assistance could be offered if the respondent was unclear regarding what a particular question meant. However, as discussed previously, as my interviews informed my survey design, there should have been less need for clarification, given that any initial confusion would have been dealt with during the interviews. The absence of an interviewer meant that consideration needed to be given to the types of questions posed during the survey. Therefore, it was important that restraint was exercised when posing open questions, to ensure that this did not place undue burden on the respondent, therefore, many of the questions used a 4-point Likert scale. This type of question was chosen due to their ability to capture individuals' attitudes; they also allowed for strength of feeling to be measured, which can be particularly useful when dealing with a nuanced concept such as that of privacy. The scales used ranged from 1-4 for many of the questions; the absence of a central option meant that participants were compelled to offer a definite view when answering these questions.

Other survey questions were a combination of specific options and free-text responses, although as stated previously, these were used sparingly. The contextual section of the survey was used as an alternative to the vignettes because even though the vignettes worked well during interviews, I believed that given the large amount of text and detail required for these to really 'set the scene' for participants, this may discourage participants from offering responses or even reading the entire vignette and so sought an alternative. The design of the

contextual section of my survey was the most challenging, as it required various views from participants regarding how concerned they would be about various types of information being seen by different groups, such as friends, neighbours and the government. It was important to ensure that I was able to access the relevant information, without making the questions too repetitive or complex; this was a difficult balance to strike. To assist the design, I spoke to various colleagues within my department, in addition to sending the proposed format of the questions to various volunteers to ensure that the question would be something that participants could answer without difficulty. While it was invaluable to obtain support from colleagues, it was also vital that the questions were tested by those unfamiliar with carrying out research to ensure that it would be meaningful to the eventual research participants. Again, for these contextual questions, I employed Likert scales, however, this time I utilised a 5-point scale. The questions in this section asked participants to consider a specific piece of information (such as their medical data) and rate how concerned they would be about that piece of information being revealed to a number of groups; the scale ranged from 1- not at all concerned to 5- extremely concerned. As these questions were considering the contextual nature of privacy, a 5-point Likert scale was used to allow a more nuanced response from participants. For these questions, it was less important for responses to be as definite as the questions described previously, therefore, the middle option was offered to participants, as a way of measuring the level of concern around a particular piece of information and the potential audience for it. A copy of the survey questions will be included as Appendix D.

Analysis

While completing my interviews, I began to consider the emerging themes, through the use of NVIVO software, which allowed me to retain a full copy of the transcript of each interview and highlight areas which appeared to be useful themes. I did this by going through each interview and highlighting potential themes, where new ones emerged, I employed an iterative process to reconsider previous interviews in light of the new themes. A number of strong, clear themes appeared, which were prevalent in a number of interviews, however, as the number of interviews increased, the incidence of new themes was reduced until it became clear that I had reached the point of saturation. At this point, I went over the themes in NVIVO to consider them in relation to my research questions and discern how well the data provided was answering them. Once I was satisfied that the data generated from the interviews was relevant to my research questions, I embarked on the design of my surveys, as detailed previously.

I carried out the analysis for my surveys using SPSS Statistics, which allowed me to run the relevant statistical tests for my data. As my sample is not representative, I did not consider it necessary to carry out the calculation of confidence intervals, as these are most appropriate when results are based on a representative sample. Once I had cleaned the data to ensure spurious results were removed, I generated descriptive statistics for each question; this provided me with a starting point to identify where the particularly interesting and counter-intuitive responses were. I also categorised any free-text responses utilising NVIVO software, to generate themes, until a set of categories became obvious which I then generated descriptive statistics for, to aid with analysis. At this

point, I referred to the analysis generated by my interviews, to identify any points of convergence or divergence between interview and survey respondents, this allowed me to consider potential patterns and areas for further investigation.

I performed a chi-square test for one of my context questions with gender and then did the same for age, however, the values produced were very high (46.7% for gender, and 73.2% for age), suggesting that there is a high probability that any differences are due to chance, and therefore it was not necessary to continue to perform further tests on the remaining context questions. The majority of my analysis for the contextual questions was carried out through ordinary least squared regressions in terms of gender and age. This allowed me to look at the relationship between each of these independent variables and the dependent variable, which was the type of information and audience. This permitted me to calculate the co-efficient, which shows how much the dependent variable increases when the independent variable does the same. For the majority of my survey results, I calculated the p-values to identify where results showed signs of statistical significance and the r-square value to calculate what proportion of the result is likely to be predicted by the independent variable. For the context questions I also used a paired sample t-test to compare the means regarding concern levels for different audiences. The statistics offered by this research are inferential and so offer guidance on whether this topic is worthy of further investigation.

My role as researcher

Since completing my fieldwork, I have had the opportunity to reflect on my role as a researcher, particularly in relation to carrying out the interview phase of this project. While it is often assumed that the interviewer and interviewee will not know each other, there were some participants that were known personally to the me, but only as an acquaintance. Although a number of friends volunteered to participate, I did not consider this to be appropriate as they would know my feelings regarding internet privacy, and as such may have felt that they were only able to respond to questions in a particular way. However, I did not have this concern when considering acquaintances as research participants and deemed our pre-existing familiarity to be a benefit in terms of building rapport and ensuring they felt comfortable in the interview situation. However, not all of my interviewees were known to me and so it was important that I consider the impact I might have upon their experience. As such, I tended to dress in a relatively smart-casual manner when interviewing, as I wanted to strike the balance between putting them at ease, while also expressing that the interview was to be taken seriously. It was important to get this right as I did not want to make interviewees nervous and thus reluctant to speak at length. Nevertheless, there is a power dynamic involved in conducting interviews, as I am clearly 'in charge' in that I develop the interview questions and decide which responses to probe and clarify. To attempt to offset this, I gave participants ample opportunities to clarify their responses or to ask questions if they were unsure of anything. We also met in a mutually convenient location that was suitable for carrying out an interview, while being safe for both myself and my interviewee.

A number of my interviewees seemed nervous at the outset, intimating afterwards that they had been a little concerned regarding what I was going to ask them; however, many seemed to become more comfortable and relaxed as the interview progressed. An interesting and surprising phenomenon occurred during a number of interviews, whereby the participant appeared to realise for the first time, the amount of information they share on a daily basis. This was an unexpected 'process' to witness and in some ways demonstrated in a tangible way the lack of consideration people often afford their privacy and suggests that this may not happen until individuals are confronted with it. Participants stated that the interview itself was encouraging them to reflect on privacy issues that they usually put to the back of their mind. This occurred for a number of interviewees, who appeared to be processing this 'new' information and re-evaluating their privacy in the moment, as the interview was taking place. Interestingly, this only occurred with participants who I knew to be undertaking a PhD at the time, and this has led me to wonder whether this 'realisation process' was due to the reflective nature of university study in general, and PhD candidates in particular. There is often a great emphasis placed upon being reflective and thinking critically during the process of obtaining a doctorate degree and so it is possible that this 'live' realisation is indicative of this. It is possible that as the discussion progressed, these participants began reflecting upon what we had already discussed as well as their practices and started to draw upon their critical skills to re-consider their privacy-related behaviour while we were discussing it. This is something that may be worthy of further research in the future, as there may be other explanations for this, which relate to other factors, that I was unaware of. This realisation often occurred with those who had begun the interview with an unconcerned attitude towards their privacy; they spoke of not worrying about their

privacy and being relatively happy with how much information they share. However, as the interview progressed, they began to realise what was at stake, with one participant stating:

> "I'm completely oblivious of it, day to day life, not aware of it whatsoever, bringing it to discussion now, I'm overly aware, I want to hide under a rock! Erm, my anxieties about it are only when I'm aware, [HEF: Mmhm, yeah] I go on day to day blissfully unaware of the, the amount of things that are being watched, and monitored, and, until it causes a problem, I guess I'd never know it was a problem." (MJ, female, 25)

This suggests that privacy is not at the forefront of individuals' minds on a daily basis and often only becomes a concern when we are confronted with it. This highlights the complex nature of privacy, when considering what is and is not shared on a daily basis and demonstrates how some participants had not necessarily agreed to participate because they had a particular interest in privacy.

Although it was a structured interview in that I had a specific set of questions that I asked each interviewee (in a specific order), I allowed participants to discuss topics that were less relevant to my area of interest. This was a decision I made at the outset, as I was concerned that it may make them less willing to provide lengthy answers if I interrupted them to steer them back to the topic. This appeared to have the desired effect and one of my participants (who spoke at length about various unrelated topics), admitted to enjoying the opportunity to speak uninterrupted about subjects that interested him. While some participants spoke in great detail, others, (often those with very definite views) offered shorter,

much more decisive answers, with less explanation. Other participants who had little to say were less definite in their beliefs and appeared quite nervous initially, however the vignettes offered them something specific to focus on and have an opinion about, even if they had appeared unsure of what to say earlier in the interview. The vignettes also offered tangible situations, which were less abstract in nature than the issue of privacy more broadly. This was beneficial in terms of providing participants with the opportunity to say more and feel more confident in their responses.

As discussed above, it is also important to recognise my place and the impact I could have on interviewees especially as I have a particular set of views around the subject of internet privacy and as such there were times when I found myself in complete disagreement with the views being expressed by my participant. This required a certain level of 'emotional labour' (Hochschild, 2003 p.ix) on my part to mask how I actually felt, so that participants did not feel that the answers they were giving were 'incorrect' or attempt to censor themselves to avoid disapproval or judgement from me. This appeared to work well, and at no point did it seem that interviewees were editing themselves. I broadly tried to remain neutral, so as not to reveal my personal opinions. However, this can be a barrier to building rapport and so at times it was necessary for me to appear to agree with their responses, even though this was not the case. Again, this is part of the emotional labour often required to ensure the success of qualitative research. Although this led to feelings of dishonesty and concerns regarding whether this was an ethical way to behave, my agreement tended to be tacit, in that I nodded in agreement with statements participants were making, rather than making statements which were untrue.

There are additional ethical implications to consider whenever carrying out research of this kind. First and foremost, it is vital that participants give informed consent to participating and this can only happen if they receive clear and accessible information prior to agreeing to take part. To ensure that this happened, I created an information sheet (Appendix A), which was approved by the ethics panel at the university but was also tested with a number of volunteers before being utilised. I also allowed my participants a period of reflection between their initial recruitment, and the interview taking place to ensure that they did not feel undue pressure to take part once they had agreed to.

The main risk with the type of interview that I was conducting is participant embarrassment, in terms of being asked to reveal something that they find embarrassing. Therefore, I made it clear to participants that they did not have to answer any questions that they were uncomfortable with, I also emphasised that they could withdraw their participation at any time without having to offer an explanation. This was also important for those completing the survey, although they may have felt less pressure to answer questions they were uncomfortable with, nevertheless each question gave participants the ability to select a 'prefer not to say' option. I also ensured that all participants (regardless of whether they were taking part in the interviews or surveys) had my contact details in case of any queries or concerns emerging following their participation.

Finally, it was important that I respect the privacy of my participants, especially as this is the area that I am researching. Therefore, I allocated random initials to my participants when transcribing their interviews and redacted the names of any

friends or relatives mentioned during the interview, replacing it with their relationship to the participant. This was not necessary for the surveys, as they were completed anonymously and so I did not know who my participants were. All interviews were audio recorded and transcribed verbatim. It was important to check these details with interviewees to ensure that participants' voices were heard and that I was representing their words and opinions in a way that reflected how they felt. As part of the consent forms (Appendix B), participants were offered the opportunity to receive a copy of their transcript and although 16 initially requested this, when I contacted them following completion of transcription, many no longer wanted a copy, as such, seven were sent to interviewees as encrypted files, with the password sent separately. When I sent the transcripts to participants, I reminded them that they could request changes, if they disagreed with the contents of the transcription, however, none of them did so.

Conclusion

The employment of a number of research tools has led to a rounded research project, which has yielded a number of interesting and at times, surprising results, suggesting that this is an area in which investigation was required. By utilising both qualitative and quantitative methods, I have been able to avoid a number of pitfalls which can lead to issues when utilising a single method. The exploratory nature of my research suggests areas which would benefit from further investigation while offering initial theories in terms of how individuals negotiate the boundaries of internet privacy.

This project has generated new knowledge regarding how individuals negotiate the boundaries of internet privacy and offers some new insights into how people feel about this. Had I chosen to employ only qualitative methods, I would have generated a large amount of intensive data, without knowing whether the views held were limited to my interviewees or could be said to be held more widely. However, if I had limited my research to quantitative methods only, I would have been able to identify trends and areas of convergence but may have directed my research instrument at the wrong issues, as I would not have had the interview analysis to direct the design. I would also have had a wealth of extensive data but would not necessarily understand the thought processes behind the responses given, which may have been detrimental to the knowledge I generated. Therefore, by employing adaptive theory (Layder, 1998), I have been able to develop and carry out a well-rounded research project which offers potential avenues to be explored while adding to the existing knowledge in this area.

This chapter has considered the methods I utilise in completing my project, with particular focus on the reasons for specific choices being made, as well as an examination of specific issues with the methods chosen. The preceding sections have examined my use of interviews, in terms of how they capture the narratives that individuals use to describe their feelings on the subject of internet privacy. This discussion also included an examination of issues around sampling and saturation and how these tests of robustness can be employed when carrying out qualitative research. This section was followed by a detailed evaluation of my surveys and how they complement the interviews, it also highlighted the exploratory nature of my study. Finally, I considered my role as researcher, particularly in relation to my interviews. Here, I examined issues of emotional

labour, as well as the ethical implications of carrying out the interviews. Therefore, this chapter has offered a comprehensive examination of the methods I utilised in my research, offering a rationale for the choices made, we will now consider the results yielded by these methods, as we move on to my analysis chapters.

Chapter Three: Standing in the way of control

Introduction

Control is a contentious issue when people are attempting to negotiate the boundaries of internet privacy and often leads to concerns around trust in companies, and the barriers that exist that reduce the level of control available to individuals. Trust plays a central role here, particularly in terms of shaping people's privacy choices, as their decisions regarding whether to share information with a company very much depend upon how trustworthy they believe the company to be (Rainie & Duggan, 2015). In order to feel comfortable with a decision to share information (thus reducing their level of privacy), it is vital that the person making the choice feels able to trust the company they are sharing information with (to a certain extent). It is important to note that no organisation is completely trustworthy, and so individuals should trust with caution, recognising that trusting an organisation does not mean that it will definitely behave in the desired way (O'Neill, 2002). If an individual is asked to share information with a company that they feel unable to trust, this will make them averse to doing so, as they would be giving up control of their privacy/information without any faith that it will be treated in the way they approve of. However, if the person trusts the company, they will be less concerned in terms of sharing their information as they will believe that though they are relinquishing control of that information, it will be treated in the way they expect. In order for individuals to feel comfortable in sharing information with a company, they need to believe they can trust that company to treat their information (and thus their privacy) with the respect they believe it warrants.

In order to examine these concerns around control, this chapter answers the following questions:

- Do people feel that they have enough control over their information?
- Would they like to have more control?
- What barriers exist that reduce individuals' abilities to have greater control?
- How can people have more control?

To answer these questions, I consider third-party sharing by companies and the mistrust this often engenders. This is particularly problematic to participants who feel that they trust companies with their information, only to discover later that their information has been shared with other organisations. This leads to a lack of trust in companies, with concerns centring around how companies deal with individuals' data once it has been shared. This reduction in trust offers an update to Starr's work regarding the concept of 'voluntary' and 'involuntary' (1969 p.1233) tasks and allows a different perspective regarding individuals sharing their data with companies.

To deal with the issue of control more fully, I examine the level of control individuals believe they have over their information. There are a number of issues around the theme of control, in particular the belief (shared by many participants) that they are unable to access the level of control they desire as companies make terms and conditions purposely difficult to understand in a bid to encourage individuals to agree to them without paying too much attention. Broadly, people feel that companies do not give them enough information to allow them to make

an informed decision regarding sharing data. People want to know more about what will happen to their information, but companies are reticent to do this in case it leads to less sharing, however, this is not necessarily the case (Benson, et al., 2015 and Martin, et al., 2018).

I also examine the role we can play in terms of taking greater responsibility for sharing our information, while considering a lack of time and/or knowledge as another barrier. I make the case that given how busy everyone is, with various apps and companies vying for our time and attention, it is difficult for anyone to truly consider the full implications of sharing information with a company. Aside from this, a number of participants have a false sense of security fostered by the fact that they have yet to suffer from any kind of issue regarding their data, therefore, they believe the measures they have in place are sufficient to protect them.

Finally, I discuss the often-suggested solution of opting out of using social media as a way of protecting one's privacy. This is not necessarily a straightforward option and I offer an opposing view to the privacy paradox which was outlined in the literature review. Instead, I argue that behaviour is not a reliable indicator of values when there is no alternative available (O'Neill, 2002), as is the case here with social networking sites. It is also important to remember that privacy is not necessarily a case of complete withdrawal, individuals want to have control so that they can choose which information they share with which companies.

Is it possible to trust companies?

The issue of trust is fundamental to the relationship between individuals and the companies they share their information with. In this context, issues are generally around what companies do with information once it has been given to them, with the main concern being third-party sharing. This is particularly problematic for participants, who regard companies with suspicion even at the initial point when data is being requested:

> "…you know a lot of the time they ask you for information that seems superfluous, obviously for marketing" (GM, female, 37)

> "But it's when they start asking your gender, how old you are, and it's like, 'Do you really need to know this?', but you know why they're doing it, it's so they can send you an e-mail, with the products in your sort of, sort of range" (VR, female, 28)

> "This is the problem, I think a lot of it is because they're obviously, they're very sneaky and they want to be able to sell your details and they want to you know….create a better erm, thing for us like create a better experience" (SM, female, 36)

Individuals are aware of the reasons they believe companies are asking for additional information, and as highlighted in the above quotes do not like it. This leads to a lack of trust in the companies that they are engaging with, because they

expect their information to be shared with third-parties (as this is common practice for many businesses).

The reason that many are unhappy with this situation is not only that they do not want their information to be passed on to third-parties, but also, they do not know who these third-parties are, and this is a source of uneasiness for them:

> "Who the hell are they [third-parties]? You know…you don't, you've got no idea who they are" (CB, male, 37)

> "Yeah, cos it's Facebook, yeah, it's the third-party companies, you don't know who they are, because it never states who they are, no matter what you go on, it just says, 'third-party companies', you, you don't know who it is!" (VR, female, 28)

> "Oh, I don't know to be honest, because I don't know exactly how much information would be shared. I think that they, I'd be happier if I knew exactly, like how and what cos it all seems a bit mysterious sometimes as well and you think 'Oh yeah, companies sharing information, that's bad', but you don't really know that much about it" (ES, female, 36)

> "Also not knowing about the company that has my data, I find it more unsettling that a company knows about me but I am unaware of who that company is, or what it's intention is. I would not mind so much if I was more informed" (survey respondent, female, 20-24)

Therefore, concerns regarding control over their data (when sharing information with companies) are around how widely their information will be shared once they have relinquished control of it. Of particular note are the final two quotes above, in which the participants suggest that if they knew more, they might not be so concerned; for them, the issue is around the unknown element of what happens to their data.

This mirrors Benson, et al.'s study of social networking sites (2015). They find that where users 'have better knowledge about the use of personal information, they are more likely to disclose personal information' (p.431). A similar finding is also put forth by Martin, et al., (2018) who suggest that it is important for businesses to be transparent and tell customers what information they are collecting and what they will do with it. They argue that in offering customers greater control (as well as being transparent), they would empower customers, who are then more likely to share data with them. This would certainly go a long way to allaying some of the concerns highlighted by my participants, who are uncertain about what happens to their data, and often simply want more information:

> "I think like when you're filling out something you should, it should be quite obvious with who they're sharing the information with, like it does say things like, 'do you mind sharing with our partner companies', well who are those companies? What do they do? that kind of thing."
>
> (AL, female, 36)

> "I think sometimes, some things should be more obvious. So, when they're asking you about, 'can you do this or can you do that?' Or 'do you wanna receive information from other people, or this, that and the other'."
>
> (CB, male, 37)

The issue of unknown companies is particularly problematic for participants, as they cannot gauge whether that company is trustworthy, and therefore whether they are happy to cede control of their data to that company. This is especially problematic as it could mean that data is being shared with companies that an individual would not choose to engage with:

> "What this data will be used for and what the third-parties are, as I may not agree with their ethical standards" (survey respondent, female, 20-24)

> "it being sold to a company that doesn't align with my personal views/values" (survey respondent, female, 30-34)

This highlights the issue of trust as being more than simply a lack of control or consent; individuals are concerned that they may be aligned with companies that do not represent their beliefs (or worse, are in opposition to them). These are companies that an individual may not choose to engage with if they were given a choice. However, when information is passed on via another company, choice is removed and the individual knows very little about this additional sharing unless they are contacted by the third-party. Broadly, this can lead to feelings of surprise and confusion, especially (as is often the case) if it is not clear where the third-

party obtained their details from. However, in a situation where the third-party's ethos does not align with the individual's values, this can be compounded (as highlighted in the above quotes). This is problematic as the person concerned may want to remove any link with that third-party but given the lack of information regarding where they obtained the information from, it is an impossible task. In some cases, inferences are made, based on other available information. For example, using Facebook 'Likes', it is possible for advertisers to infer that individuals will like their brand and so suggest to their friends that they do (Ward, 2017; Hern, 2017 and Nurse, 2019). The person concerned remains unaware of this, unless one of their friends chooses to ask them about it. This 'hidden' sharing of information may lead to negative feelings towards the initial company as the person feels that they have been misrepresented to the third-party. These concerns were echoed in the responses given by those taking part in the online survey, who were asked the following question:

Are you worried about your information being passed on or sold to third-parties without your knowledge? (Rainie & Duggan, 2016)

The overwhelming majority (85.1%) say that they are worried; this rises to 90.0% for males and is just under 85% for females, suggesting that this is a concern that many face. When this is probed further and participants are asked to specify what particularly concerns them, almost a third (31.8%) are categorised as 'Uncertainty (lack of control/consent)'. This is followed by responses which come into the 'Spam/cold callers' category (26.8%). This confirms the widespread concern discussed by interview participants, and again, demonstrates that it is that lack of certainty around third-party sharing which is the greatest concern for participants.

While the categorisation of 'Uncertainty' may appear vague, the comments from participants are not:

> "Don't know what the info will be used for."
>
> (survey respondent, demographic information not supplied)

> "I don't know who they [third-parties] are and what they will do with my data." (survey respondent, female, 30-34)

> "I don't know who will access and for what purpose"
>
> (survey respondent, female, 20-24)

The issue with a lack of information is that it is difficult to trust in situations where there is very little information available, because it makes assessing the level of risk that we are potentially open to virtually impossible. In fact, Metzger argues that, "Trust is critical to this process [sharing data] because it is believed to reduce the perceived costs of such transactions" (2004). This is important because, as O'Neill (2002) argues, we need as much information as possible in order to be able to make judgements regarding when to (and when not to) trust others. Therefore, in situations where we are unable to obtain the necessary information regarding what a company will do with our information once shared, it is impossible to know whether to trust that company or not. It is important to note here that complete trust is not possible; it tends to be conditional, however, it is in the interests of companies to increase their trustworthiness (O'Neill, 2002) and so lessen the uneasiness that people feel in these situations.

To explore feelings of trust in a more detailed way, survey respondents are asked three questions regarding how they feel about the way in which companies deal with their information. The first question asks:

Overall, do you believe that online companies and organisations will keep your information secure? (Rainie & Duggan, 2016)

Participants were asked to select one of the following responses:

Yes – all of the time
Yes – most of the time
Some of the time
No - never

In response to this question, over two-thirds of participants say that they only believe this to be the case either 'some of the time', or 'never', with the majority selecting 'some of the time'. While this overall percentage is mirrored when responses are separated by gender, there is less parity when comparing the proportions selecting each of the separate options available. 12.9% of females say that they 'never' believe that organisations will keep their information secure, while 19.8% of males agree. This suggests that males are less trusting of companies than females when considering data security, and it is also worth noting, that for this question (as well as the two that follow), none of the male participants select 'Yes – all of the time'.

The above difference between females and males is particularly striking because previous research into gender and trust tends to find that either females are less trusting than males (Sheehan 1999; Van Slyke, et al., 2002; Rodgers & Harris 2003 and Fogel & Mehmad 2009), or that there are no real differences in levels of trust when considering gender (Kolsaker & Payne, 2002; Sebastianelli, et al., 2008 and Hernández, et al., 2011). However, my findings suggest that it is males who are less trusting, particularly when considering data being shared with online companies and organisations. There are a number of potential explanations for this.

Firstly, many of the previous studies took place when online shopping was in its infancy, and at that point in time, the majority of internet users are men. This increased knowledge and use of the internet by men, may lead to them having greater trust than women, who are less familiar with this practice. It is therefore possible, that as online shopping has become more commonplace for everyone, women are increasingly completing online purchases. In fact, a recent US survey finds that women are making more purchases online than men (First Insight, 2019). This increased use of online shopping can lead to increased familiarity and experience and therefore potentially increased trust for women, while men may be making fewer purchases online due to a lack of trust.

Further, Gong, et al.'s, 2018 study of users (in China) of the popular WeChat messaging app, finds that in terms of trust, there is a gender difference in terms of the value placed upon different aspects of the relationship with commercial technology. As such, females are more concerned about there being legal and technological protection for the user (items such as encryption are important).

However, for males, the reputation of the site and the existing social ties that the user has are more important. Therefore, levels of trust are impacted by different factors for each gender and this offers an explanation for my finding regarding the trust levels of females versus males. If females are more concerned about legal protection, they may be more trusting as they believe that the law offers sufficient protection for users. However, if males are more concerned about the reputation of the site, negative media stories regarding social media (for example, Greenberg, 2017; Kelion, 2017 and Glance 2018) are likely to have a far greater impact upon them and their levels of trust.

An important caveat here is that both of the above studies were carried out in Asia, and so may not be generalisable to gender differences in the UK. Also, my survey questions are asking participants about online organisations and companies, which can include social networking sites, but also encompasses any organisation that individuals deal with online. Therefore, my participants will not necessarily have been thinking solely about social media when answering these questions, making comparisons problematic.

Following the initial question regarding trust, survey questions deal with information sharing and third-parties explicitly:

Do you trust online companies and organisations that you share your information with to only use it for the purpose it was collected? (Rainie & Duggan, 2016)

Do you trust online companies and organisations that you share your information with not to pass it on to third-parties (unless you have authorised them to do so)? (Rainie & Duggan, 2016)

These questions are intended to access greater detail in terms of how participants feel when they are considering their own data. This is in response to many of my interview participants who mention the difficulty they feel in worrying about privacy if they have not suffered an issue personally, as the below quotes demonstrate:

> "Erm, but at the moment it's probably OK, cos I haven't experienced anything bad I suppose, so I'm not really that cautious of...Probably not, I probably wouldn't think about it. Unless it's right in your face"
>
> (CY, female, 24)

> "Erm, my anxieties about it are only when I'm aware…I go on day to day blissfully unaware of the, the amount of things that are being watched, and monitored, and, until it causes a problem, I guess I'd never know it was a problem" (MJ, female, 25)

> "Yeah, it's one of those things where yeah, if it's not close to home, then it's not close to home and it's something you put to the back of your mind."
>
> (TJ, female, 23)

As noted above, interview participants indicated that their data and the privacy of it was not necessarily at the forefront of their minds, and so I wanted to ensure

that when asking survey respondents about trust, it was not an abstract notion that they were considering. This is why the wording of the trust questions specifically asked them to think about the companies and organisations that they share their data with. It was important to ensure (as far as possible) that participants were placing themselves and their information at the centre of any questions or situations that they were being asked to consider. The responses received are shown in the table below:

Do you trust online companies and organisations that you share your information with to only use it for the purpose it was collected? (Rainie & Duggan, 2016)

	% All *(n)*	% Female *(n)*	% Male *(n)*
Don't know/Prefer not to say	2.74 *(8)*	2.69 *(5)*	0.00 *(0)*
Yes - all of the time	1.71 *(5)*	2.15 *(4)*	0.00 *(0)*
Yes - most of the time	24.66 *(72)*	27.42 *(51)*	20.99 *(17)*
Some of the time	48.63 *(142)*	48.92 *(91)*	49.38 *(40)*
No - never	22.26 *(65)*	18.82 *(35)*	29.63 *(24)*
Some of the time/never	*70.89 (207)*	*67.74 (126)*	*79.01 (64)*
Total [1]	**100.00 *(292)***	**100.00 *(186)***	**100.00 *(81)***

(r-square: 0.027, p-value: 0.006)

As with the previous question, what is striking here, is the difference in the levels of trust amongst women and men. When considering how much they trust companies to only use their data for the collected purpose, a much larger

[1] Please note, this question was not compulsory and so participants were able to move on to the next question without providing a response.

proportion of men select 'some of the time' or 'never' than women (79.0% versus 67.7%). Again, this highlights a potential gendered perspective when it comes to trust, which is, thus far, unexplained in the existing literature. A potential explanation for gender disparity is offered by the discussion above, which considers the different factors that play a role in women and men's trust in social networking sites. As noted, Gong, et al., (2018) find that the reputation of a site is more important to men's level of trust than women's, therefore it would not be unreasonable to suggest that the more the media reports on misuse of customer data by large companies, the less trust men are likely to have, while women may be less concerned as they believe that the legal protections that exist will continue to protect their data.

The final question in the trust section of the survey, asks participants:
Do you trust online companies and organisations that you share your information with not to pass it on to third-parties (unless you have authorised them to do so)? (Rainie & Duggan, 2016)

	% All *(n)*	% Female *(n)*	% Male *(n)*
Don't know/Prefer not to say	3.09 *(9)*	2.15 *(4)*	3.70 *(3)*
Yes - all of the time	2.75 *(8)*	4.30 *(8)*	0.00 *(0)*
Yes - most of the time	25.43 *(74)*	27.42 *(51)*	22.22 *(18)*
Some of the time	42.27 *(123)*	44.62 *(83)*	38.27 *(31)*
No - never	26.46 *(77)*	21.51 *(40)*	35.80 *(29)*
Some of the time/never	*68.73 (200)*	*66.13 (123)*	*74.07 (60)*
Total [2]	**100.00 *(291)***	**100.00 *(186)***	**100.00 *(81)***

Please note, percentages may not add up to 100 exactly, due to rounding
(r-square: 0.009, p-value: 0.063)

[2] Please note, this question was not compulsory and so participants were able to move on to the next question without providing a response.

As shown in the above table, the proportion of females answering ‘some of the time’ or ‘never’ is broadly in line with the overall proportion of all participants selecting one of these responses (66.1% for women, 68.7% of all participants), however, for males this is much higher at 74.1%. As with the previous two questions, this suggests that males are less trusting than females when considering how companies deal with their data. As discussed throughout this section, it is hard to know exactly why there is a lack of trust when considering males, especially as this has not been found in previous studies, however, I offer a number of potential explanations for this.

This lack of trust is also seen in interviewee responses and suggests that many occupy a position of distrust and it is through this lens that considerations of companies are made when information is requested. A number of interviewees express a lack of surprise when discussing companies potentially sharing their data with third-parties:

> “Erm, yeah, that, I dunno it just kind of pisses me off, like erm, that's, that's the thing, it's more like, it's not so much like a I'm really worried about what they're gonna do with it, because I'm like well are you gonna advertise to me, like neee, I don't really care, but it just irritates me that they have that information and like erm it really winds me up erm, like cynical kind of targeted marketing, when stuff pops up on your Facebook feed and on like YouTube, where it's like erm where it's targeted, stuff that you've been looking at something like.” (AQ, male, 26)

> "I feel that the amount I share with companies, is perfectly legitimate. I think the amount they share with other companies is not! [HEF: I see, yeah] Err, I always look for the box that says, 'Do you want us to share with third-parties?' and also the trick question they put on there, is 'Tick this box if you want us to share with third-parties'. [HEF: Yeah] or 'Tick this box if you don't' and they change it around, or they'll ask the same question in two different ways [HEF: Yes] and that's, that I think's really naughty." (DC, male, 36)

As illustrated in the above quotes, participants often express a dislike for it, but are ultimately not surprised by the possibility that companies might share their data with unknown third-parties. They are aware of the potential 'tricks' being used by companies, particularly in terms of the opt-out boxes. This coupled with the survey responses discussed previously suggests that individuals may be entering into relationships and interactions with companies from a base of mistrust and only beginning to trust them if and when they demonstrate that they are worthy of that trust.

As discussed in the introduction to this chapter, trust is a key factor in the relationship between customers and companies. However, the results of my study suggest that although trust is somewhat lacking, individuals are still sharing their information with companies. This hints at feelings of resignation amongst individuals and highlights how sharing data has become a part of our everyday lives (this will be discussed fully later in this chapter). Therefore, to opt out of sharing information has the potential to make our lives less convenient and could potentially lead to us missing out on certain things. As such, it is often with an air

of resignation and frustration that individuals share information with companies; we now turn to Chauncey Starr's work (1969) around the acceptability of risk to examine the potential explanation for this frustration. At the time of Starr's writing, this tended to relate to the government or official bodies, however, I suggest that this is relevant to the sharing of information with companies, especially third-parties.

Starr's concept of voluntary and involuntary activities offers an explanation as to why individuals are frustrated with the further sharing of their data. In their eyes, they have decided to share their data, based on the information available and whether they believe the level of risk involved in sharing that information is acceptable. Current data sharing practices, I suggest, offer a contemporary example of Starr's voluntary activity, in that the decision-maker (the individual) has the information required to make the decision and is choosing the course of action that they subsequently take. However, the dynamics of the situation change when companies go on to share customer data with third-parties; this is when it becomes problematic. When companies share data beyond their original request (generally with third-parties), they become the decision-maker and the individual loses control over their information. When this situation arises, it becomes an involuntary activity for those who initially shared their data. If the data is being shared without their consent, the individual concerned is excluded from the decision-making process, but not from the consequences of that decision. This is important because Starr suggests that assessing risk is a key part of this. Therefore, a company sharing an individual's data is likely to perceive very different risks and benefits to doing so than the individual themselves and so in this case, makes a different decision. A final point raised by Starr which is

relevant here is that, ‘we are loathe to let others do unto us what we happily do to ourselves’ (1969 p.1235), suggesting that it is the loss of control which is the issue for those involved, and reinforcing the point made earlier, that if individuals knew more, they may agree to share more information. Therefore the frustration felt by individuals is not that the information has been shared, for they may have chosen to share it themselves, but that they are not able to make the decision at the outset; someone else makes it for them and this removes their control and leads to feelings of mis-trust.

There are, however, issues with Starr’s dichotomy of voluntary and involuntary action and Douglas and Wildavsky’s examination of risk (1983) offers a useful counter point here. They argue that this distinction assumes that risks can be easily categorised as voluntary (and therefore acceptable) or involuntary (unacceptable). This could lead to moral judgements around who is to blame when risks are taken, depending upon which side of the boundary the activity falls. They argue that carrying this through to its logical conclusion, it is possible that all risks would be deemed to be involuntary, with all of those affected seeking compensation through the law.

While the point regarding the categorisation of risks as voluntary or involuntary is valid, and offers an interesting perspective, the suggestion that we are moving towards a situation whereby everything is deemed to be an involuntary risk has not come to pass. It is also worth noting that my participants are aware of where the boundary is for them, in terms of when they were making choices and when their control had been removed:

> "I feel that the amount I share with companies, is perfectly legitimate. I think the amount they share with other companies is not!" (DC, male, 36)

When this participant decides what information to share with a company (voluntary activity), he is in control, however, he loses control when that company goes on to share the information with a third-party (involuntary activity). This moment, when a situation goes from acceptable to problematic is clearly defined by this participant.

Another important point is that Starr suggested that when making risk-related decisions, everyone has their own personal criteria. Therefore, while many participants articulated the idea that there is a line for them, what counts as being 'over the line' very much depends upon the individual. Participants discuss when sharing data becomes an issue for them:

> "Err, with a company I've sign-….I usually think, err, that there's a line err, abou-….about the amount of information I should give them, erm, in, dependent upon, depending upon the nature of the transaction erm, or the nature of my relationship with them." (PW, male, 37)

> "So, it feels kind of like it's crossed a line for you?" (HEF)
> "Yeah, yeah but it's a line that you can't control, well that's what it feels like, see I've put it into something that's been passed on, but I can't, when I can't recall where that's been, or where that's stemmed from, that's an issue." (TJ, female, 23)

I argue that this demonstrates how participants are aware of there being voluntary and involuntary activities, when considering sharing data with companies, even though they would not use those words to articulate it. There is a feeling that they have control and the ability to make decisions up to a certain point, but once they are past that point (usually once they have shared information), it is out of their control and there is nothing they can do. I suggest that this line represents the boundary between voluntary and involuntary activities, which suggests an accord with Douglas and Wildavsky's suggestion that the boundary between voluntary and involuntary risks is not fixed. Issues of control will be dealt with more fully in the following section.

Another key factor in terms of trust is reputation. As noted above, previous research suggests that when making trust-related decisions, reputation is more likely to impact men than it is women. Broadly speaking, where a company has a good reputation it is likely to be thought of as reliable, and therefore trustworthy, while for those with a poor reputation, the opposite is true (Swaminathan, et al., 1999; Jarvenpaa, et al., 1999 and Metzger 2004). Previous experience with a company also plays a role and, in this way, when discussing the type of company, some interviewees feel that large well-known brands are more trustworthy than smaller companies, or individuals.

> "Yeah, it's just not worth, you know, cos the thing is, is most apps are made by people, not, not all of them are made by companies, so I tend to be a bit more careful of the ones that are just done by people, do not know why, cos companies are probably the worst for taking your information. You know, you always know it, but for some reason,

because it's a company you feel more trusted to the company, when it's probably, you're more trusted to the person, cos one, you know, Joe on his own in the corner, on his computer, trying to make an app, or you got like, you know, Atari, a big, massive company going, [sings] 'we're gonna steal all your data'." (VR, female, 28)

"Erm, I feel, yeah, I feel pretty comfortable but err when I know and you know it sounds kind of really middle-aged or something but big British brands, you know, I, I feel like they wouldn't do anything, which is really naive, you know, wouldn't be sharing anything, or they wouldn't have any problems, which is obviously not true, cos you hear about it all the time, leaks and you know, people getting hold of things. But I feel more secure doing that, I think it's the co-, the, the companies where it's quite new or erm from overseas, or you've just not heard of them before and you think, 'I'm not really sure, erm what their policies would be or, what the deal is' and that, erm is when I would feel less inclined to share information with them." (ES, female, 36)

Interestingly, participants discuss these feelings of trust towards established, well-known companies, but at the same time recognise their naiveté, because these are the very companies that have the most to gain from collecting and selling customer data. This often makes people laugh at the 'trap' they have fallen into in trusting these companies, despite them being much more likely to sell customer data. This does not necessarily cause a great amount of concern, as this is realised 'in the moment' of the interview, and more often than not, the interviewee in question simply shrugs this realisation off, as if to say, 'but what can you do?'. This also highlights the role that reputation can play in generating feelings of

trust, with both women and men, even when individuals realise that those they trust are potentially the least deserving of it.

Just as trust is key to decisions regarding which companies to engage and share data with, so too is the level of control an individual feels they have in a particular situation, as hinted at above. Often individuals do not feel that they have enough control over what happens to their data and want more. The next section will deal with the issue of control.

How do issues of control manifest themselves?

As discussed previously, there is a feeling amongst my participants that they do not have enough control over what happens to their data once they have shared it with a company. Many recognise that we can only ever be as in control of our data as companies allow us to be. Raynes-Goldie (2012) discusses Facebook's privacy settings and the lack of control offered to users of the site. She argues that 'The design of social media does not make the data collection obvious, nor does it provide any method to opt out.' (p.70-71). Interestingly, when research offers recommendations to companies, it puts forth that customers are likely to share more information when they perceive a company as transparent and allowing them greater levels of control (Benson, et al., 2015 and Martin, et al., 2018). This advice has yet to be heeded though, as individuals still feel that companies work hard to maintain control over data, particularly in terms of making it difficult for customers to opt out of having data shared with third-parties.

There is a general belief that companies purposely make terms and conditions documents difficult to understand or utilise other strategies to make the task of opting out a more onerous one. Indeed, Raynes-Goldie (2012) highlights this issue in her work, putting forth that privacy settings on Facebook are confusing to users, making them so difficult to understand that users are not sure what they are agreeing to when they join the site. This hints at the trust issues discussed above, as individuals have little faith in companies to act in their best interests, particularly as there is so much money to be made from selling customer data. Given the difficulty in understanding terms and conditions and so on, many participants speak of how it is much easier to agree without reading or understanding them:

> "Yeah, I think if maybe they just like kind of like really like concisely like summarised the key points, rather than like all the jargon, then like, yeah that would make it easier and you would know what you're accepting but I think because you don't want to read through all of it and sometimes you don't understand it, you just press accept. Erm, so I think, yeah, like in in that sense like maybe it could be a bit clearer and a bit easier language."
>
> (SA, female, 23)

> "Yeah, well the thing is, you give your information to, to their organisation because you agree to their terms and contracts, and there we go, the most, the, the biggest lie on the internet is have you read and agreed with the terms and conditions? Because who is actually going to actually read if you put it in a Word document like six pages of terms and conditions?" (DM, female, 31)

For my participants, there is no expectation that anyone reads the terms and conditions, although they are not alone in this. Raynes-Goldie (2012) cites Scott Buchanan (an intellectual property lawyer) and his suggestion that it is unreasonable for Facebook to expect that users read their Terms of Service, given their length and complexity. Therefore, when dealing with companies, convenience plays a role, as per the quotes above, it is often too difficult or bothersome to make sense of the terms and conditions. Again, this is felt to be no accident, in that businesses make it much more difficult for customers to fully appreciate what happens to their data once they have shared it.

In terms of third-party sharing, it is impossible for individuals to either know who holds data about them or to make amendments to incorrect data. This is problematic because when considering data control, the onus is usually placed upon individuals to take the first step when there is a problem (Gadzheva, 2008). However, it is impossible for individuals to begin to address this problem if they do not know who the source of the incorrect data is. This is particularly troubling as individuals have a right to ensure that data held about them is correct (Data Protection Act 2018) but are prevented from exercising this right. This can lead to a power imbalance between those collecting and storing the data and those to whom the data actually relates, whereby the data collectors have much more knowledge and control over what happens to the data (Coll, 2014). This power imbalance will be discussed in further detail in the next chapter.

As discussed above, there is a suspicion amongst interviewees that companies are attempting to collect superfluous information from them in order to sell it to third-

parties, therefore, survey respondents are asked how they feel about the amount of information that companies collect from them. 73.3% of participants believe that the amount being collected is unreasonable, and of those who believed that it is reasonable, 83.7% would not want to share further information. There is an air of frustration when I ask interviewees how they feel about the amount of information that they share with companies.

> "I'm in control as much as I feel I can be." (DC, male, 36)

> "Erm, I should decide who gets to see kind of what. Erm despite me being very open about everything, I still, it's me who decides to, to be like that and, and to, to share whatever I want to share…" (DM, female, 31)

As reflected in these, quotes, there is broadly a feeling that we should be able to decide what we want to share with companies and refuse to share anything that we are not comfortable sharing. Many of my interview participants feel that they share too much with companies but are unable to take action which would change this. This was one of many barriers described by my participants, which hinder them in being able to have the level of control that they desire.

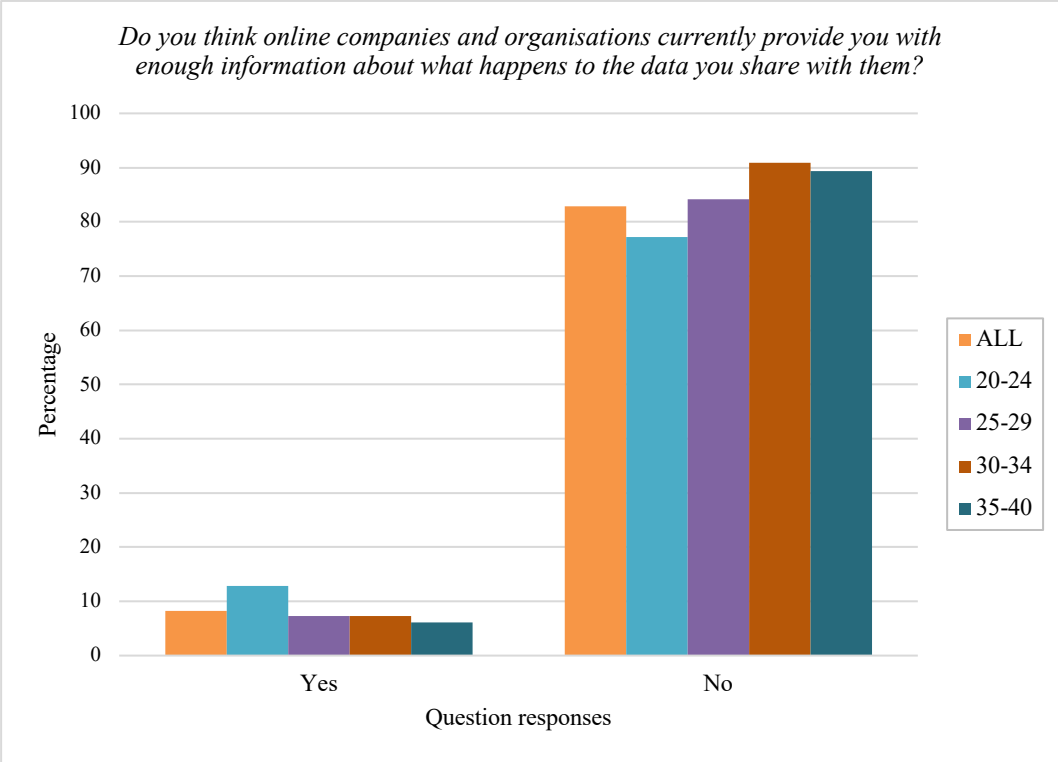
Despite the erosion of control, it is of central importance to individuals' perceptions of privacy (Culnan 1993; Nippert-Eng 2010 and Sujon & Johnston 2017), particularly as they want to be able to manage their privacy in a meaningful way; it is vital that we are able to control who has access to us in our daily lives. When our privacy is invaded (in the case of cold callers, for example), we are reminded that we are only afforded privacy when someone else allows us

to have it. It is not enough for us to simply decide that we want to be left alone and we are often reminded that we lack control or power over our own privacy. This is why there is such an issue around third-parties being sold our data, because it allows unknown organisations not only to know things about us, but to then invade our privacy by interrupting us at times when we would like to be left alone (Nippert-Eng, 2010). It also hints at the power imbalance between the person whose privacy is being invaded and whoever is invading it; in this situation, those being interrupted have low privacy and thus, low power as they are unable to control their own accessibility. This is becoming more important as we no longer need to occupy the same space to be able to interact with each other and therefore, it is much easier to be interrupted in our daily lives (regardless of whether we welcome this or not). It also serves to remind us that while we have acted in good faith, in trusting a company with our information (thus ceding control over it), this trust has not been repaid.

This issue of access relates to more than simply others being able to access us and our attention when we do not want to be disturbed, it also relates to who has access to our data, which again, is why third-party access to our data is so troublesome to many. It speaks to the reduction in privacy that we are facing, in that more and more is known about us by a greater number of individuals and groups; the issue here is that we lack knowledge of those groups and so cannot decide whether we want them to access our data (Nissenbaum, 2010 and Proferes, 2017). This is the main issue when information is shared with third-parties.

To explore this concept, survey respondents are asked the following: *Do you think online companies and organisations currently provide you with enough information about what happens to the data you share with them?* (Rainie & Duggan, 2016, p.7)

The graph below shows the responses to this question, by age group:



[3]

(r-square: 0.043, p-values: 0.002-0.044)

It is clear that the overwhelming majority (82.9%) say that they do not, this is especially pertinent, when considering the responses given by different age groups. As indicated on the graph, the proportion of participants selecting 'No' increases with each age group, peaking with those aged 30-34 (90.9%). While there is a dip in the proportion of participants saying that they do not think companies give them enough information in the oldest age group, it is a relatively

[3] Please note, percentages do not add up to 100 as those responding 'Don't know' or 'Prefer not to say' have been excluded

small reduction (1.52%), and so not enough to suggest radically different opinions in those aged 35-40. The overall results are mirrored in a commercial study carried out by Groopman and Etlinger (2015) in which many of those taking part express a wish to know more about what companies do with their data. This is echoed in comments from interview participants, who feel that companies could do more:

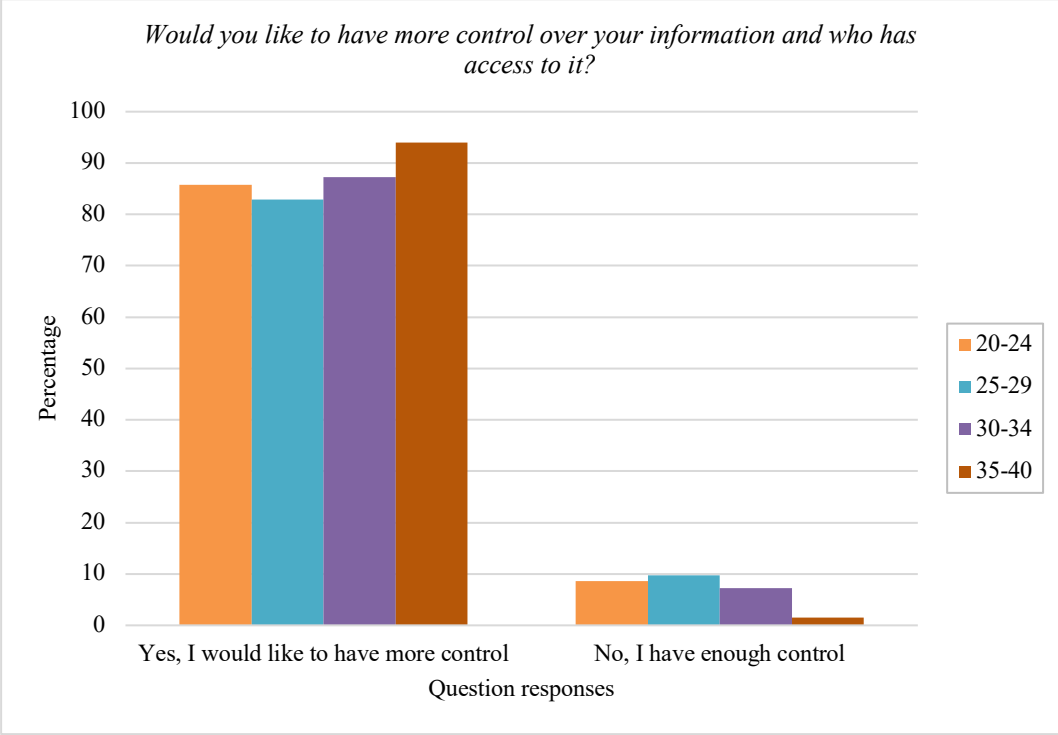
> "I think sometimes, some things should be more obvious. So, when they're asking you about, 'can you do this or can you do that?' Or 'Do you wanna receive information from other people, or this, that and the other'. That, rather than that stupid little micro-font at the bottom with that little tick-box, erm that should be more obvious, as maybe a pop-up box or something like that." (CB, male, 37)

This links with the work of Phelps, et al. (2000), whose study of attitudes towards mail order companies with regard to privacy finds that many participants want more information about how to have their details removed from mailing lists. At this time, the idea of companies sharing their mailing lists with other companies was unacceptable to many of those taking part. Phelps, et al. found that consumers' level of control over further dissemination of their data is one of the main concerns and in the context of this study, it is linked to consumers believing that they receive more advertising mail.

When my survey respondents were asked: *Do you feel that you are in control of your data and what it is used for?* (Madden, 2014). 85.7% say that they feel in control only 'sometimes', 'rarely' or 'never', with 10.0% of participants saying

that they 'never' feel in control of their data. This is comparable with the results of research carried out by the Pew Research Centre (Madden & Rainie, 2015), who find that 88% of Americans feel they had 'some', 'not much' or 'no control at all', with 13% believing they have 'no control at all'. Although the response categories are not exactly the same as those utilised in my survey, this suggests that feelings of having little control are potentially widespread.

To gauge feelings around control, participants were asked whether they would like to have more control over their information and who has access to it, again, the majority said that they would like to have more control (86.5% of all participants). While this was broadly mirrored when breaking down the responses by gender, it is worth noting that there was an interesting trend when separating the responses by age group, as shown below:

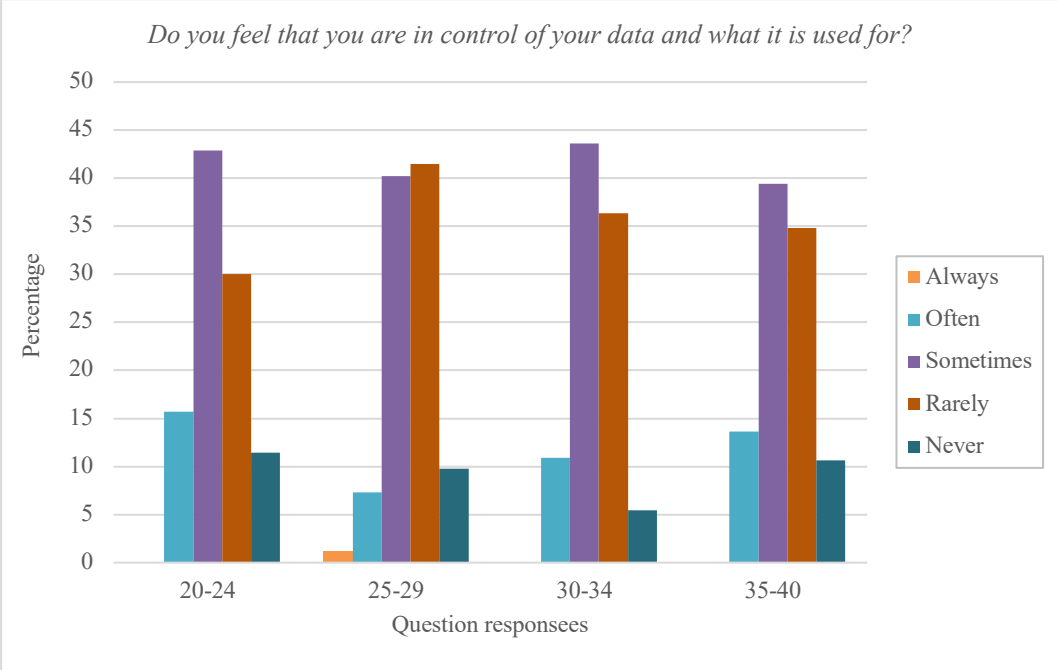


[4]

(r-square: 0.02, p-values: 0.000-0.997)

[4] Please note, percentages do not add up to 100 as those responding 'Don't know' or 'Prefer not to say' have been excluded

When examining those selecting the 'Yes, I would like more control' option, there is an increase of 11% from those aged 25-29 to those aged 35-40, suggesting that as individuals get older (from their mid-twenties onwards) they want more control over their data. However, this increase does not appear to be mirrored in responses to the previous question, which asked whether individuals feel in control of their data and who they share it with. For that question, it was those aged 25-29 who were the most doubtful about when they have control (in terms of those selecting 'sometimes', 'rarely' or 'never'). This is surprising, given the trends shown here, however a closer examination reveals some noteworthy results.



[5]

(r-square: 0.01, p-values: 0.211-0.779)

Those aged 25-29 are the only group where the proportion of those saying that they 'rarely' feel in control of their data is higher than those saying that they 'sometimes' feel in control. This is counter-intuitive, as this age group has the

[5] Please note, percentages do not add up to 100 as those responding 'Don't know' or 'Prefer not to say' have been excluded

lowest proportion saying that they would like more control over their data and it would be expected that those who feel the least in control would also want more control. However, it may be that while participants recognise that they have little control, they are resigned to this, accepting (to a certain degree) that to have more control may lead to less convenience. It is also possible that although individuals feel that they are lacking in control, they have little choice but to trust these companies and supply the requested information, because there is no practical way of avoiding doing so (O'Neill, 2002). The belief that being more concerned about privacy could lead to missing out on some parts of everyday life will be examined in the next section.

It is also important to consider that while issues around third-parties cause concern for individuals, it tends to be at the level of annoyance or frustration, rather than being something which demands a change in participants' behaviour. However, this may have more to do with feelings of resignation, rather than a lack of concern. This could be a sign of pragmatism, in that individuals believe that there is little to be gained from worrying about how little control they have, given that there is little that they can do to change that.

When we discuss control, interviewees tend to focus on social media, while the subject of sharing information with companies does not seem to be something that they think of until prompted. This is potentially because individuals feel they are able to control the information that they post on social media and so this is more at the forefront of their mind, whereas they are less able to control the information they share with companies. It is also possible that the effects of losing control of data on social media sites would be more readily felt, and this is often what gains attention in the media, therefore this is at the forefront of individuals' minds when

considering this issue. In line with this, the next section will focus on the various barriers that individuals face when attempting to have more control over their data.

Which barriers restrict control?

As discussed in the previous section, the majority of my participants feel they have lost control over what happens to their data and would like to regain some. In an attempt to unpack this, survey respondents were asked what they believe stops them from having more control and provided a free-text response which were then categorised as follows:

	% All *(n)*
Companies don't allow control	**44.00 *(33)***
Lack of awareness/transparency	17.33 *(13)*
Impossible to participate in digital culture without sharing info	14.67 *(11)*
Misc.	13.33 *(10)*
Legal issues	10.67 *(8)*
Total responses [6]	100.00 *(75)*

Typical responses from participants were:

> "…because the business model of online companies is set up to limit the amount of control" (survey respondent, female, 30-34)

> "Companies don't give me control" (survey respondent, male, 35-40)

[6] Please note, this question was a filter question and so was not all participants were asked this question.

"It [control] is not offered, not possible or accessible"

(survey respondent, male, 25-29)

"It is simply not a possible option. Everything that is digitized, automated, and leaves a digital trail will ultimately risk being out of my control"

(survey respondent, female, 25-29)

"…you know, you're clearly not in control, it's, it's a false sense, it, kind of gives you the sense of being in control and in reality you're not, in reality they [companies] are in control" (TP, female, 40)

This suggests that there is an issue in terms of the company-customer relationship, particularly in terms of not only the level of control that individuals believe they have, but whether it is possible for them to access greater levels of control, should they wish to. As discussed previously, the advice to companies to tell customers more about what happens to their data (thus allowing them greater control) is not being heeded. This is because companies fear that if they offer customers the ability to opt out of sharing data, they may do just that and the company will lose revenue (Turow et al., 2015). Instead, where companies offer a mechanism for customers to opt out, it is often very difficult to find out what action is required to do so and as such, individuals are essentially required to make a conscious effort to achieve the level of control (and therefore privacy) that they desire (Nippert-Eng, 2010).

As examined previously, individuals feel that companies do as much as possible to make it difficult for them to opt out of sharing data and want companies to make opting out much more obvious and explicit. This lack of information from

companies, is highlighted in responses to the following question: *Do you feel that you know enough to be able to fully agree to what happens to your data after you give it to an online company or organisation?* 75.9% said they do not, and when this group were asked why not, the free-text responses given were categorised as follows:

	% All *(n)*
Lack of transparency (them)	**43.30 *(83)***
Lack of knowledge (me)	42.27 *(79)*
Hacks/no guarantee of privacy/security	10.31 *(20)*
Misc.	4.12 *(9)*
Total responses[7]	100.00 *(191)*

Many believe the issue lies with companies simply not giving them enough information to allow them to make an informed decision when sharing their data. This suggests that not only are individuals making decisions with incomplete knowledge, but they are aware that this is the case. In essence, they are not really choices, as those tasked with making a decision are not able to do so as they do not have the necessary information to make a fully informed decision. Again, this could lead to feelings of resignation for individuals who feel that despite their best efforts, they are unable to make a meaningful decision.

Related to this, another area in which it is felt that companies could do more in terms of clarity is the terms and conditions that potential customers must agree to before they can fully engage with a company. Numerous participants describe the

[7] Please note, this question was a filter question and so was not all participants were asked this question.

complexity and length of these statements as being off-putting to them. In fact, when survey participants were asked whether they have read terms and conditions before joining social media sites in the past, a mere 5.8% said that they had. There is no expectation that anyone reads these documents; they are seen as being overly long and complicated (which is deemed a purposeful strategy of the company, rather than an unintended consequence). While discussing the topic of trust, O'Neill (2002) points out that although it is important that individuals have access to information in order to make an informed decision regarding whether to trust an organisation, it must be relevant. If companies merely supply a large volume of additional information, in a bid to be transparent, this could become noise which is just as unhelpful in the decision-making process as too little information. Therefore, in situations where there is a flood of information, it becomes too onerous on the individual involved to wade through the entirety of it in order to make a sound judgement. The following quotes are indicative of the general comments being made by participants:

> "It's so confusing! This is the problem, I think a lot of it is because they're obviously, they're very sneaky and they want to be able to sell your details…I think they need to make it a lot clearer as to what you're agreeing to and who can see your details." (SM, female, 36)

> "losing control is part of the t&cs" (Survey respondent, female, 20-24)

> "We are not given the option of control. Design limits our agency" (survey respondent, male, 25-29)

However, it would be unfair to suggest that the blame should be placed with companies alone, and other barriers have been identified by those taking part in both the survey and interviews. Participants are aware of their own role in terms of increasing the level of control they have. This is clear if we consider the responses to the survey question: '*Do you feel that you know enough to be able to fully agree to what happens to your data after you give it to an online company or organisation?'* While many respondents (selecting 'No') say that the issue is due to companies not being transparent enough (43.3%), almost as many recognised that they could do more (42.3 %). Typical comments from participants include the following:

> "I don't keep up with technology" (survey respondent, female, 35-40)

> "I don't know enough to understand terms of service fully" (survey respondent, demographic information not supplied)

> "It all feels too complex to understand" (survey respondent, female, 30-34)

> "I'm not as much of an expert in privacy and data sharing/collection as I could be" (survey respondent, female, 25-29)

This view is not unique amongst those completing the survey, and my interview participants share these sentiments:

> "I just don't really understand it and it just changes a lot and you see a lot of the stories about, you know check, they've changed it, they've updated

the app so, make sure that you're doing this, or turn this off, and it kind of baffles me a little bit." (ES, female, 36)

"Yeah, I think if maybe they just…really like concisely…summarised the key points, rather than like all the jargon, then…that would make it easier and you would know what you're accepting but I think because you don't want to read through all of it and sometimes you don't understand it, you just press accept." (SA, female, 23)

As previously discussed, it has almost become a social norm not to read the terms and conditions, and many state that they do not read them, either because they do not understand them, or they do not have the time required:

"It's in the T&C's but I never read it" (Survey respondent, female, 20-24)

"Not having the time to read the T&Cs all the time"

(Survey respondent, male, 30-34)

"Most of the time, right, even in life, anyone, most of the time you're in a rush, you're never just sat down doing something, you're in a rush to, I don't know, you're late for work…and you're just doing it [HEF: yeah], just err, and you're not even thinking about it, like, paying bills."

(VR, female, 28)

Individuals' admission that they do not read terms and conditions suggests that they do not care about their privacy, however, the situation is more complicated

than it seems. These responses suggest that rather than people not wanting to make the effort to read terms and conditions, it is more a case of them feeling constrained by their lack of knowledge or time. The last of the above quotes in particular, draws attention to a feeling of being overloaded that many people have. There are many different things competing for an individual's attention, that signing up to a new online service (and agreeing to terms and conditions) happens while they are engaged in another task. This raises questions regarding the issue of agreeing to terms and conditions when not giving it our full attention. In the moment of attempting to access a website for a particular purpose (to pay a bill or access a game, for example), does the immediate task of accessing the website become more important than the principles of wanting greater control over one's information and thus privacy? It is also important to remember that when there are few alternatives (if any), we may behave in ways that appear to be in direct opposition to our values (O'Neill, 2002), however, we can only act on our values, when those options are open to us. This links with Bourdieu's notion of the 'choice of the necessary' (1984 p.372), in which he describes how conditions of necessity undermine other concerns, therefore in this case, the individual concerned is valuing the necessity of paying a bill (for example) more than their underlying privacy concerns. In this situation (and many other similar ones), the person involved is adapting to what is possible, and so the level of privacy they require is not possible, but the ability to deal with household administration without needing to physically go to the bank is possible (and broadly, preferable). As such, terms and conditions are not something that tend to draw our attention away from other items and so they are more likely to be agreed on in the background while we are doing something else:

> "Terms and conditions are often very lengthy and, even with the best will in the world, it can feel time consuming to read fully. I admit this is my failure!" (Survey respondent, female, 35-40)

> "Terms and conditions are very long and wordy. Often in legal language I don't understand or don't have the time to understand."
>
> (Survey respondent, female, 25-29)

> "Things are typically buried very deep in privacy notices. Whilst I am confident enough to find my way around one, it's typically too much effort to go looking when I just need to get a task done."
>
> (Survey respondent, male, 30-34)

Individuals recognise that they could do more in order to protect their privacy but are hampered because they do not have the knowledge or time required to be able to protect their privacy in a meaningful way. This has been noted in previous studies, whereby when individuals are given Privacy Policies or Terms of Service to read in an experimental setting, they either skip reading them altogether, or where they do open them on their screen, it is for such a brief period of time, that they could not possibly have read them (Obar & Oeldorf-Hirsch, 2018). The researchers state that:

> '…information overload [is]…a significant negative predictor of reading TOS [Terms of Service] upon sign-up, when TOS changes and when PP [Privacy Policy] changes. Qualitative findings suggest that participants view policies as a nuisance, ignoring them to pursue the ends of digital

> production without being inhibited by the means' (Obar & Oeldorf-Hirsch, 2018 p.1)

In other words, terms and conditions are seen as an obstacle that individuals want to get past, in order to carry out a particular task on the site. They do not want to have to stop part-way through the process of accessing a site of interest, to consider the implications of doing so. This is particularly problematic when the site being accessed is related something enjoyable, such as a social media site, or an entertainment website. On these occasions, people are accessing the site for entertainment purposes, and so do not want to have to consider any potentially serious implications for something that does not feel serious.

In fact, it has been theorised that it is actually impossible for individuals to engage in the self-management of their privacy in the way they are told that they should (Turow, 2003; Jensen & Potts, 2004; McDonald & Cranor, 2008; Vitak, 2012 and Hoofnagle & Urban, 2014;). The burden placed on individuals to be responsible managers of their own data privacy are deemed to be unrealistic for anyone with responsibilities outside of this (which is everyone). Obar, having read various recommendations for how individuals should be responsible data privacy managers in the USA stated, 'I do not see how anyone can escape the conclusion that the digital citizen must have the appetite of a data miner and infinite time at their disposal.' (2015 p.12).

This suggests that the bar is set so high, that it is impossible for individuals to reach it, which in itself could become a self-fulfilling prophecy as people become

disheartened with their efforts to maintain the level of privacy that they would like. This is highlighted in the below quotes from interview participants:

> "I'm not really sure…but yeah, maybe if I knew how to work better with my privacy. If I knew how to manage it, I probably would. If I knew, yeah, if I knew there was ways I could stop people, and it was simple, [both laugh] - not that, not that technically, you know, not gonna start coding everything that I write to the internet! But if it was a simple, way of managing my privacy that I was made aware of, I probably would for no reason other than it was a way of managing my privacy, not because I'm, I feel like I'm being targeted for something, but just because I could, I probably would." (MJ, female, 25)

> "Are you generally concerned about who has access to or knowledge of your activity on the internet and social media?" (HEF)
> "Yeah, I am, I mean I s'pose it's, it's one of those things where I, I don't really understand exactly how the privacy settings work, and I don't know whether I've actually done it properly, or not" (SG, male, 31)

These quotes highlight the difficulty for individuals to really understand whether the efforts they are making are having an impact at all, it seems to be too complicated to enact the level of privacy they would like, but even if they do manage to do so, they are never sure whether what they have done is enough. The first participant makes several mentions of the process being simple, she talks about wanting to manage her privacy, but only if it is something that is not beyond her capabilities and does not require her to learn new skills. This issue is

highlighted in work carried out by the Pew Research Centre (Shelton, et al., 2015), who find that overall 22% of all adults surveyed had changed their behaviour to protect their privacy following Edward Snowden's revelations regarding government surveillance programs. When they queried why individuals had not done so, 54% say that it is because they believe that it would be 'somewhat' or 'very difficult' to find tools or strategies that they could use to increase their privacy either online or on their mobile phones (p 5). This suggests that MJ is not alone in her concerns regarding the skills required for an individual to increase their privacy.

Aside from lacking the necessary time to protect their privacy, another barrier here is that individuals may develop a false sense of security if they have not suffered an issue with regard to their privacy. This can lead them to believe that they are not at risk, and that they do not need to take any additional measures. This is something my interview participants are aware of:

> "That's it, it's yeah, it's saying, ' Oh, that's never gonna happen to me, I've been fine for 23 years so far, why's it ever gonna happen now? I'm not gonna do anything different, I'm not gonna change my behaviour, so I'm not at risk.' That's, that's such a ignorant perspective, but it's true and I think that's what a lot of people do, it's just yeah. We just don't stop and think. And also, busy schedules as well, you don't, do you?"
>
> (TJ, female, 23)

> "Err, no I've never had any like credit card hacked or anything like that either, so I guess, maybe again, if that happened to me, it may make me feel a bit more nervous about it" (TS, female, 37)

Both of the above quotes suggest that these participants feel that the measures they have taken must be working to a certain extent, as they have yet to suffer an issue, this can lead to individuals feeling that they do not need to take any further action to protect their privacy. In fact, the second quote suggests that if an issue occurred, it may be enough to encourage this participant to take further action, but until that happens, she is happy enough to continue with the measures she has in place. This is a common theme amongst interviewees, who (as discussed above), do not want to be burdened with worry about their privacy, especially as there are few options available to them if they want more privacy.

When discussing potential actions that could be taken to increase privacy a number of participants spoke of the only real option being to close down social media accounts, or make other similar 'drastic' changes, but these are felt to be unrealistic, particularly because the use of these sites has become a part of everyday life. This is interesting, because this is often purported to be the solution when individuals complain about losing control over their privacy; critics suggest that rather than complaining, they should simply delete their account. However, this is not the straightforward option it appears to be, particularly as these sites have seamlessly become part of the fabric of my participants' daily lives, and so to suggest that they simply do not engage with them anymore is to suggest that they make their lives unnecessarily inconvenient (Nissenbaum, 2010;

Vertesi, 2015; Hargittai & Marwick, 2016 and Anthony & Stark 2018). Interviewees recognise this:

> "I do feel like modern living basically, is not conducive to erm caring or doing anything above the minimum [about my privacy]" (GM, female, 37)
>
> "Yeah, I think, I think it's just one of those things, because we, we're fed so much information, and I think where technology has become such an integral part of our lives, it's almost hard to look at it as something that might be sort of dangerous or problematic to privacy and things like that. I mean, privacy is one of many other issues that you could face [HEF: Of course, yeah]. But I think because it's such a integral part of, particularly, well of my life, like I said, I wake up and look at, the first thing I do is look at social media sites, which is sad. [HE laughs]. Erm, that it's hard to then take a step back and go, 'oh, actually I should think about this, this this' because it's become so normalised" (TJ, female, 23)

As these quotes suggest, my participants find that using technology has become a part of their lives that they are unwilling to manage without; they enjoy the benefits of using social media, and so do not necessarily want to give up using it. Facebook, for example offers various 'social benefits' (Raynes-Goldie, 2012 p.213) and as such some participants speak of people being considered weird if they were not on Facebook. This is also highlighted by Vertesi (2015) when she attempted to hide her forthcoming pregnancy from social media sites and found that, while it is possible, it is very inconvenient, and at times aroused suspicion from others. She states, 'Thus, avoiding data capture…can appear antisocial, immoral or criminal. There is no evasion without repercussion' (n.p.). Therefore,

eschewing technology can have an impact in terms of an individual becoming stigmatised as others wonder what they are attempting to hide (Acquisti & Grossklags, 2003).

Refusing to engage in social media is not only inconvenient to the individual themselves, but their friends and family. Participants complain about the difficulties involved in having friends who are not on social media, and some even admit that they do not keep in touch with these friends due to the additional effort required:

> "Erm, but yeah, I guess someone, maybe I shouldn't be like I don't, I guess it's kind of bad, but like why, why would you not be on Facebook? [both laugh] It sounds terrible, but like honestly, cos like you get, it's really annoying then when you're trying to organise something and stuff cos then you've got those like two friends that you have to, you just create a Facebook event and you're like, 'right, that's sorted' and then you go, 'oh, I've gotta e-mail Steve because he's...' you know? And then it changes and you've got to remember to e-mail Steve and then, then those people get annoyed about not being invited to things" (AQ, male, 26)

This encapsulates the general feeling around having friends that are not on social media, while my participants stated that they understood why some people might choose not to be on Facebook (usually due to having an issue with an ex-partner), it is still something that caused them some level of inconvenience and frustration. It is also interesting to note this participant's question – 'Why would you not be

on Facebook?', he is genuinely puzzled by this and it hints at Raynes-Goldie's suggestion that:

> "there can also be significant social costs involved in Facebook refusal…the ensuing network effects mean that a refusal of Facebook is also a refusal of the norms of social behaviour in one's group" (2012 p.214)

Given the benefits being offered by having an online presence, the costs of shunning these are seen as undesirable. This leaves individuals with very little choice, but to continue using these sites, rather than developing new habits, which make their life less convenient (Vertesi, 2014) and potentially mean that they miss out on social events with greater regularity. The issue is that we have become so reliant on the level of convenience offered by these websites, that it is difficult to imagine not using them, and going back to doing things the way we did previously (Wu, 2018). This highlights the difficulty felt by individuals in terms of balancing the ability to take part in modern life while maintaining a level of privacy that they are comfortable with.

Concerns regarding this issue are also apparent amongst survey respondents, when asked for free-text responses to the question: '*What do you think stops you from having more control?'* (Shelton, et al., 2015). While concerns regarding participating in digital culture are not the greatest concern, as shown in the below table, it is the third highest concern:

	% All *(n)*
Companies don't allow control	44.00 *(33)*
Lack of awareness/transparency	17.33 *(13)*
Impossible to participate in digital culture without sharing info	**14.67 *(11)***
Misc.	13.33 *(10)*
Legal issues	10.67 *(8)*
Total responses[8]	100.00 *(75)*

This category warranted comments such as:

> "It is not possible in this day and age to keep your information private and also have a public presence online. I want to have both"
>
> (Survey respondent, gender not supplied, 30-34)

> "Need to provide information to participate in digital society"
>
> (Survey respondent, female, 25-29)

Therefore, it has not escaped my participants' attention that opting out would not only be difficult (if not impossible) but may additionally leave them at a disadvantage in terms of their social life. It is also important to stress that some enjoy the services afforded to them by engaging with social media and the internet and do not want to delete their account.

[8] Please note, this question was a filter question and so was not all participants were asked this question.

It is also important to recognise that the responses given here may go some way to highlighting how the concept of the privacy paradox (Utz and Krämer, 2009) is not all that it seems. This concept is often used to suggest that people do not care about privacy as much as they say they do, because behaviour is perceived to be a greater indicator of beliefs (Preibusch, et al., 2013). However, as seen here, part of the discrepancy between an individual's beliefs and actions may be that they would like more control but feel constrained by companies, who will not allow them the level of control they desire. As discussed above, this can be in the way that companies lack transparency when informing their customers what happens to their data once they have collected it, as well as making terms and conditions or privacy notices oblique and difficult to understand. Many perceive this as a way of ensuring that customers agree to what the company wants to do with their data, without really understanding what they have agreed to.

Even when individuals are concerned enough to take action and make changes to their privacy settings on social media (for example), they could still be in a situation whereby they do not have the level of privacy they desire. This is not the same as taking no action; in situations where there are no options or alternatives (as I suggest is the case here), behaviour cannot be taken to be an indicator of how an individual feels about the situation (O'Neill, 2002).

It is also worth noting here that various issues affect an individual's behaviour in terms of the action they take (or do not take) in order to increase their privacy. Buchi, et al. (2017) suggest that it is simply not enough for individuals to want to do more to protect their privacy or to care about their privacy, if they do not have the necessary skills to take action, their concern will be insufficient to elicit any

action. This highlights why users do not always amend the default privacy settings on social media, for example, believing it to require a lot of additional time and effort in order to implement the level of privacy they would like (Vitak, 2012), as discussed previously.

It is also important to remember that privacy is not necessarily a case of complete withdrawal from a situation; people can want privacy and want to be on social media sites, the two are not necessarily mutually exclusive. Privacy is not a dichotomy, it is nuanced, and as such individuals often want different levels of privacy in different situations, this is where the complexity of the situation is revealed. It is too simplistic to simply state that if an individual is a member of a social networking site or shops online, then they do not care about their privacy. This is not the case and the nuanced concept of privacy will be examined in greater detail in the 'Context Matters' chapter.

Finally, opting out of utilising social media sites may not offer a reasonable solution (Hargittai and Marwick 2016) for many individuals (as discussed above). If we consider the lack of trust around how companies behave with our data once we have shared it with them, and the lack of options available to us, this can lead to individuals having a sense of cynicism and apathy, which at times is expressed by my participants, but is by no means their only response. Many, in fact discussed the tactics that they employ when engaging with companies to resist the control of the company in one way or another. This resistance and its effectiveness will be examined in the next chapter.

This section has investigated the barriers to control put forth by my participants when sharing information with companies. This is often a case of companies not allowing them to have the control they desire, through a lack of transparency, particularly when considering the terms and conditions that people are presented with when creating an online account. These agreements are often long, with confusing language and are felt to be purposely onerous by participants who have neither the time nor inclination to sit down and read the whole document before agreeing to them. This is believed to be a strategy on the part of the company to ensure that individuals will agree to the terms and conditions without paying too much (if any) attention to the clauses contained within them.

However, it was also recognised that individuals are lacking in the necessary knowledge to be able to understand the terms and conditions they are being presented with. There is often too much vying for our attention and so agreements are clicked on and accepted without a great deal of consideration of their contents. In fact, studies (McDonald & Cranor, 2008 and Obar & Oeldorf-Hirsch, 2018) demonstrate that the requirements placed on individuals to manage their information are impossible to reach.

Individuals also often feel that although they would like to do more to protect their privacy, they lack the necessary skills to do so, therefore rather than a lack of action being a sign that individuals do not care about their privacy, it is more that they do not feel able to take the necessary action. There is also the belief that if an individual has not suffered a problem in the past, they are protected, and need take no further action. This can lead to a false sense of security as individuals feel

that the default privacy settings and so on are enough to keep their information safe, although this is not necessarily the case.

It is often suggested that the only way to really have control is not to engage with social media sites to begin with, or to close down any accounts that an individual has. However, social media has become such an integrated part of our lives, that many believe this would only serve to make our lives more inconvenient, and potentially lead to missing out on social events and family news. This is often deemed too high a price to pay. Therefore, it may make more sense to share information in order to access the convenience offered, even if this leads to feelings of frustration and/or resignation.

Chapter Four: Fight The Power

Introduction

The previous chapter examined issues of control, in particular the concerns many have regarding a potential loss of control when sharing data with companies and on social media. As a counterpoint to this, I will now offer a detailed examination of the decision-making process itself and consider how individuals are able to utilise (limited) autonomy in specific situations. Given the discussion above, regarding the reticence people often experience while sharing information, it is important to understand the circumstances under which people might continue to share information. This is considered in relation to making tradeoff decisions and how this may involve bias, rather than being what many would perceive as a logical decision. The focus here is on the difficulties faced by individuals when attempting to decide whether to share information with a company. This draws on work around the 'availability heuristic' (Tversky & Kahneman, 1982 p.20) as well as issues around many people's preference for instant gratification, (O'Donoghue & Rabin, 2000) when faced with particular decisions.

A further issue with tradeoff decisions involves the recent phenomenon of the fear of missing out, which can be a motivating factor in terms of remaining a user of social media and is often prioritised over privacy concerns. There are, however, other issues which play a role when decisions are being made, such as the convenience offered by sharing data and individuals' willingness to pay for privacy; these will be examined fully in this chapter. I also use the lens of Foucault's concept of disciplinary power (1977) to suggest that we are not as in control as we believe. Although it may appear that there is little opportunity for

people to exercise control, I will offer signs that there are small, everyday ways in which individuals do attempt (and succeed) in creating their own pockets of control, whereby they are able to resist the rules imposed upon them while appearing to submit to them. This will be considered through the lens of de Certeau (1988) and Fiske (1989).

How are tradeoff decisions made?

As discussed previously, individuals believe that companies ask for too much information from them, and as such, when faced with a request for information, they attempt to consider whether they actually want to provide it.

As such, a calculation is made regarding whether any potential benefit outweighs any potential cost and thus makes sharing the information worthwhile. It is the view of many participants that sharing information is to be expected when utilising social media for free:

> "Erm, I think the problem we have is that people don't like information being collected, but they want all the, all the nice and quick services and everything else to be able to do that…So, it's kind of a hand in hand. If you want the tech, and you want the advancements, you have to surrender a little bit of personal information." (CB, male, 37)

> "Yeah, and also cos like, yes, you could like completely stay off any kind of social media but for example, I like Facebook, cos it's free messaging and people are, because everyone else seems to have like data, it's a really

> handy way of getting hold of people [HEF: Yeah]. So that's, that's one of the things, and I just like getting information about stuff I'm interested in, so I'm, I'm getting something positive out of it as well." (JZ, female, 25)

> "I see it as a tradeoff that I want, they want some information from me to improve their data collection and who's using it and therefore how they market their and having a business and how they market their product based around their main client-users, but I'm getting to call America for free anytime I like, for as long as I like. So, for me, that's fine."
>
> (CB, male, 37)

This is borne out in previous research on the subject, which shows that individuals are often willing to share information with companies, to gain access to a variety of benefits (Phelps, et al., 2000 and Acquisti & Grossklags, 2005). This ranges from receiving a more personalised service (Chellapa & Sin, 2005) to greater convenience (Hann, et al., 2007 and Rainie & Duggan, 2016). Broadly, it is seen as being a bargain that individuals must enter into in order to take part in consumer society, as recognised by my interviewees. As the quotes above demonstrate, many are happy to participate in this bargain, and broadly feel that it is a fair exchange in order to access the service or information they require. This relates to the discussion around the 'calculus of behaviour' (Laufer & Wolfe, 1977), in my literature review and highlights the potential for individuals to carry out internal calculations regarding the costs and benefits when being asked to share information. This is one of the findings of research carried out by Rainie and Duggan (2016), who find that '…consumers understand and appreciate the benefits of sharing – at least under certain circumstances' (p.7). The qualification

is of interest here, because it suggests that there are only particular situations in which individuals deem the benefits of sharing information to be of value. The contextual nature of such decisions will be examined in the next chapter.

While much of the theory around tradeoff decisions suggests that individuals are making rational decisions, this is not always the case. Acquisti (2004) highlights how difficult it is for individuals to behave in a rational way when attempting to make privacy-related decisions. People are often unable to access all the information required to make a meaningful decision regarding what should happen to their data (as discussed in the previous chapter). This means that the conditions under which people are attempting to make decision in this area are uncertain.

Aside from this issue of a lack of information, Acquisti and Grossklags (2005) suggest that it may be useful to consider potential biases that people may be unconsciously applying when attempting to make a decision under uncertain conditions. These biases can lead individuals to believe that the benefits far out-weigh the costs (even when this is not true), as is often the case when a person is asked to share information with a company. One such bias is the 'availability heuristic' (Tversky & Kahneman, 1982 p.20). Heuristics are used by people as a way to 'reduce the complex tasks of assessing likelihoods and predicting values to simpler judgemental operations' (Tversky & Kahneman, 1974, p.1124). In the case of tradeoff decisions, the availability heuristic suggests that when we are trying to assess how likely something is to happen, we attach a greater probability to instances that we can recall more easily. Therefore, in a situation where an individual is being asked to share information, if they can remember someone

they know having an issue after sharing data, they would be more cautious. However, if they cannot recall any issues (or can only remember the benefits described by friends), they would be more likely to accept the benefits and apportion them greater weight than the costs of sharing information.

In situations where no real-life examples are forthcoming, an individual may move onto 'imaginability' (Tversky & Kahneman, 1974 p.1127), which is similar to the situation described above, except that the bias is towards instances that the individual can more easily imagine (rather than a real example that they can recall). In both of these instances, bias can play a role and due to this, the individual may be overly cautious or not cautious enough depending on how easily they are able to recall or imagine the benefits and costs of following a particular course of action.

This suggests that while tradeoff decisions appear to be logical from the outside (and even to the individual making the decision) they could be a reflection of biases held by that person. However, this is not the only issue to consider when examining the tradeoff decision-making process.

What role do free access and fear of missing out play?

When making tradeoff decisions, one of the benefits is deemed to be the free access to a particular social network or website (as discussed in the previous chapter). As reflected in the quotes at the beginning of this section, many participants feel that that it is not only fair, but to be expected that in order to access a service or social network without any financial cost, they must be willing to share some of their information. As demonstrated in these quotes, it is deemed

unrealistic to expect to pay nothing whatsoever to gain access. Floridi (2015) is less accepting of this explanation, suggesting that online services appear to offer us 'gifts' in terms of being able to access a particular site or service for free and we are encouraged to accept this at face value. However, issues arise when these services become a ubiquitous part of our daily lives; we come to rely on them, and struggle to imagine our lives without them. This raises questions regarding whether the tradeoff decision is as much of a choice as my participants believe and is recognised by one of my interviewees in particular:

> "…if err Google tracks everything you do and records it and then sells that information off. I don't doubt they do that, but I'd prefer they didn't. [both laugh]. [H.E.: yeah]. Erm and the other way for me to stop them doing that is to not use Google and there's no way to do that in today's society [H.E. laughs], you need Google, [H.E. laughs], which sounds like a drug addiction!" (GD, male, 25)

Although this participant is making a joke when he suggests that his reliance on Google is akin to a drug addiction, what he says is not without foundation, as highlighted in my discussion of Raynes-Goldie's (2012) work in the previous chapter. She highlights how these sites have become a part of everyday life and for individuals to eschew this, is to miss out on something important. She is not alone in this view, as Nissenbaum (2011) also questions how realistic a choice is when it is dichotomous. Individuals are given the option to participate in social media or not to participate, and she argues that this is not as much of a choice as it may seem. She also draws attention to the costs that individuals are likely to suffer if they choose not to participate, in terms of being socially excluded.

Again, this highlights how we might feel that we are making decisions regarding whether to share our data, but we are potentially much more constrained than we realise. This complicates the tradeoff decision as individuals are no longer simply deciding whether to share their information or not. The choice becomes whether to reduce our privacy (through sharing information) and thus be able to maintain our social relationships or to retain our privacy, but to miss out socially on the events occurring in our friends' and families' lives. This can be made even more difficult if the maintenance of these relationships rests upon being a member of a particular social network. As stated by Scholz (2013), for an individual to refuse to engage with social media, 'would be tantamount to social isolation' (p.8).

This suggests that coercion plays a role, because although those using social media are not physically forced to participate, that is not to say that they are not being coerced into sharing information on some level. As discussed in the previous chapter and above, social media has become a part of our everyday lives, and without the access offered by these sites people may suffer socially. If all of my friends and relatives are Facebook users (for example), it is harder for me to maintain a relationship with them, if I am not also a member of Facebook (Andrejevic, 2013). This represents a potential cost for those refusing to engage with Facebook and as such, users are being compelled to participate in social media through a fear of being socially excluded if they do not (Dyer-Witheford, 2015).

This fear of missing out socially plays a role in the decision-making process. Nippert-Eng (2010 and Stoilova, et al., 2019b) discusses how her participants speak of there being a tradeoff between this concern and privacy fears, and as

such, fear of missing out is often prioritised over fears related to their privacy. This is not the only concern that is prioritised in this way and the fear of paying more for products is also important. Therefore, if a person decides to sign up for a loyalty card, it may indicate that they place greater importance on saving money (through special offers) than on their personal privacy. It will be useful here to offer a brief reminder of the issues discussed in the 'Commercial Surveillance' section of my literature review, in particular how data has become a commodity for many companies, including social media sites. The collection and selling of user data has become an important income stream for many companies and as such offers advertisers a way of allocating resources much more efficiently by targeting them at those who are likely to be interested in the product being sold. As such individuals receive personalised offers based on their previous behaviour and so are less likely to be faced with advertisements for items that are of no use or interest to them. Given how lucrative this practice has become, it is of little surprise that personalisation has led to increased data collection, as companies believe that the more data they have, the more accurately they can predict consumer behaviour. Companies have also gone to great lengths to extoll the virtues of the collection of data in order to placate consumers who may feel concerned about their data being collected and utilised in this way. The main way in which this is communicated is in highlighting the benefits of personalisation to individuals, while obscuring how this data is often sold on to third-parties to make it even more valuable to companies. This message regarding the benefits of personalisation appears to have resonated with my participants and is mirrored in the below comments:

"…thinking about maybe Tesco Clubcards, I know there was a big thing around that and, and people feeling violated, but, I, that's tailoring in a good way." (ES, female, 36)

"They collect data on what I buy then they suggest things that I want to buy and that can be handy sometimes, or Ocado obviously does that, collect all the information in terms of groceries and then they tell me what I'll probably want to buy that week and they're usually right!" (GM, female, 37)

"…sometimes I will offer up information and sign up to things, speculatively, not even when I'm buying something, if I feel like that's an organisation or a you know, a company that I'm really interested in and therefore, would want them to, to have my information and let me know about things, or pass it on to other people." (ES, female, 36)

Therefore, these participants feel that they are able to access tailored offers or shopping lists through sharing information with a company, in this way, their loss of privacy is felt to be 'worth it' for the offers that they then receive.

However, others show greater reticence when discussing items such as personalised advertising:

"…I sit on the fence with a little bit like Facebook erm, ads and kind of giving people access to the sort of things you host and like and therefore tailoring ads around that. Part of me is like, 'Well there's gonna be ads anyway, they may as well be tailored around the things that I like. Erm,

you know, I might as well see stuff that's relevant, than see stuff that's not relevant, I suppose',” (ES, female, 36)

“…so like it's funny because you know, the idea of all the adverts that come up on my Facebook, they, they are tailored to either website searches or erm, if I've put my e-mail into something else, it comes up with something else. Now, whilst I think that's an invasion of my privacy, I also see it as quite convenient, [both laugh] because, it knows from my searches that I like certain things, so if I like New Look or I'm looking for this type of dress, it will come up with all different types of dresses… But I do feel most times, nine times out of ten it's just it is harmless, it's there, they use it then it’s found me the dress I needed [HE laughs], there we go!” (MJ, female, 25)

Therefore, participants struggle with two opposing issues, the fact that supplying information tends to lead to advertisements and website experiences being much more personalised (and so more meaningful to them) is broadly deemed to be a benefit of sharing information. However, there is still discomfort in companies knowing so much about them, as highlighted in the above quotes. While the first quote appears to be positive, the use of language such as ‘might as well’ and ‘I suppose’, suggests that there are more complex feelings below the surface. Similarly, the second interviewee states, that to her, the personalised advertisements on Facebook constitute, ‘an invasion of my privacy’, but she then seems to dismiss this as it is also useful to her.

It is also important to remember that while use of force is not necessarily obvious, it is broadly indicative of existing power relations. This can be seen when we consider that as noted above, the benefits of personalisation for individuals are highlighted by companies while the benefits that the companies themselves experience (particularly the revenue generated from third-party sharing) are less widely known. It is also important to note, that when companies hide the third-party sharing that occurs, individuals are being asked to share information for one purpose, while the true usage of that information is hidden from them, offering them very little agency in this situation. This asymmetry of power is more obvious when considering the terms and conditions that we **must** agree to in order to access social networking sites, especially when considering how little information we are offered regarding the practices of social networking sites (such as amalgamation of user information and so on) (Andrejevic, 2013).

How are time-consistent/inconsistent decisions made?

As examined in the previous chapter, individuals are not always able to access all of the information they require when attempting to make tradeoff decisions (O'Neill, 2002). This leads to uncertainty about the potential costs and benefits, meaning that they can never be completely sure of what the potential outcome will be. As discussed previously, an individual may underestimate or overestimate the likely cost or benefit in a given situation. This adds a level of complexity to the decision-making process, particularly as immediate gratification can play a role here and so a person may make a decision that makes sense for them now (to receive an immediate benefit), but in the long-term, will actually have a more detrimental impact (thus leading to a future cost) (Acquisti & Grossklags, 2005).

This echoes the work of O'Donoghue and Rabin (2000) who suggest that people tend to be 'time-inconsistent' (p.233), meaning that they err towards immediate gratification and make different decisions at different times. In terms of an individual's privacy, this means that a person will have a specific preference, such as to protect their privacy by sharing as little information as possible with online companies. As such they may decide that they will not share information such as their date of birth when they open an account online with a new company in the future. However, when the future arrives, that person's preferences have changed, and in the moment that they are trying to access a website and so when asked for their date of birth, they will share it (O'Donoghue & Rabin, 2000). This can be seen in the below quote:

> "but I'm one of the worst ones for doing this, by putting in my card details and saving them. I really wish I wouldn't, but I always forget to tick the box that says you don't want your card details saved, always. Most of the time, right, even in life, anyone, most of the time you're in a rush, you're never just sat down doing something, you're in a rush to, I don't know, you're late for work…and you're just doing it [HEF: yeah], just err, and you're not even thinking about it, like, paying bills." (VR, female, 28)

This quote highlights the issue with time-consistency examined by O'Donoghue and Rabin (2000). VR does not want to save her card details with companies and intends to select the option that means that her card details will not be saved, but in the moment, she is in a hurry and so forgets her intentions. The immediate gratification offered by paying a bill takes precedence over her intention to protect

her privacy and ensure that her card details are not saved.

Unfortunately, people do not always behave in a way that will generate the least costs for the greatest benefits. As such, while an individual may logically want more privacy, as per the time inconsistency approach examined above, when the time comes to make a decision, it may not be so straightforward. Choices often need to be made between options that offer gratification now, with potential costs in the future or something that has a potential low cost now, but a greater benefit in the future. So for example, if a person has a choice of behaving in a way that is easy and convenient now (but offers less privacy) or in a way that will afford them greater privacy in the future (but is less convenient now), they are more likely to select the convenient option which may ultimately lead to less privacy. This can be seen when considering areas such as healthy eating, when individuals will decide that they want to lose weight and eat more healthily, however, the immediate gratification offered by a chocolate bar is often too difficult to resist, especially because the benefit of losing weight and becoming healthier, will not be noticeable for quite some time (Thaler & Sunstein, 2009). This is similarly true for increased privacy, except, it is possible that the benefits may never be felt, particularly as a benefit in this case often involves the absence of something, such as the absence of annoying spam emails or the absence of our data being hacked. Therefore, we may go to the effort of increasing our privacy for no tangible benefit, thus making the immediate gratification offered by providing the information all the more attractive.

As noted, VR is discussing how she does not have the patience to go through and read the terms and conditions when she is trying to download a new app, at that

time, her priority is accessing the app, and her future privacy is of very little (if any) concern to her. She is a busy person and as such does not have the time to worry about these potential future issues. This relates to the point above regarding the difficulties faced by individuals, who want to be able to protect their privacy (delayed gratification) and only share the information that they are comfortable with, but at the same time, they want to access a website or app (immediate gratification). This highlights the inherent difficulties involved in attempting to make tradeoff decisions, in ensuring that the decision we make is the one with the highest benefits and lowest costs. Acquisti (2004) suggests that this is due to psychological distortions and this offers an explanation for why individuals do not behave in privacy protective ways despite claiming that they want to. He goes as far as to state that, 'The conclusions we have reached suggest that individuals may not be trusted to make decisions in their best interests when it comes to privacy' (2004 p.27). As highlighted above, this also demonstrates the difficulties that many people face in terms of time-inconsistency in that they intend to protect their privacy in the future, but when they arrive in the future, they do not do so.

That is not to say that individuals are sharing information without any concerns, and it is important to point out that many of my participants are sceptical about the benefits offered by sharing data:

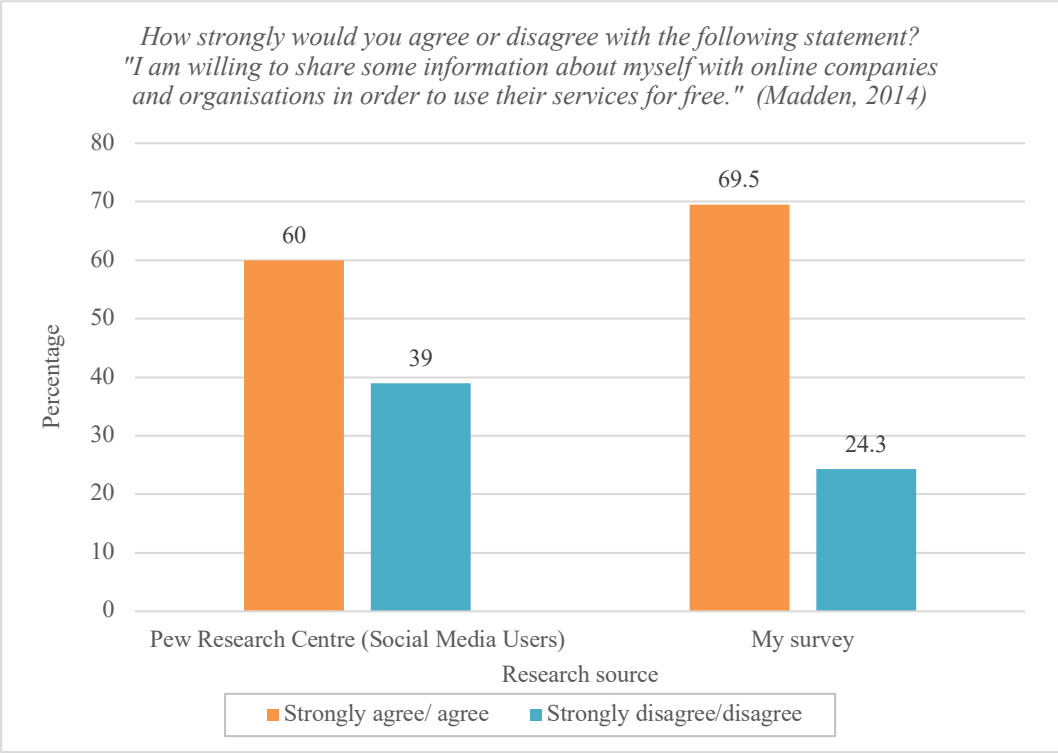
> "Erm, it's basically kind of like an intuitive thing of things [information] they don't need to provide me this service. Err, and I get that some, some companies, they, they, they get their money from, from information gathering and, and targeting people, and whatever they are doing, erm, but that, there's no kind of benefit in it for me, in a way that I, I don't expect

anything, to get anything from it, but erm, as I said if it doesn't feel right that they should have that information its…it's a no go" (DM, female, 31)

"So, yes, I could do without it, but I like what I'm getting from it so that's why I use it [social media]. If I wouldn't like what I was getting from it, I wouldn't be using it" (JZ, female, 25)

"Exactly, that's it, but like, I do think about that quite a bit, it's like, is it worth for a free whatever or to be entered into so, shall I, no, it's not worth it…if it's worth the option or you have the option of saying yes or no. Nine times out of ten, it's no to be honest with you, so, it's not worth it." (MR, male, 37)

These participants are aware of the bargain that they are entering into but are not necessarily convinced that the benefits outweigh the costs and as such do not always give up their information; they exercise a level of scepticism that Acquisti does not believe is possible. In the terms used by O'Donoghue and Rabin (2000), these individuals may be time-consistent and so immediate gratification is less of an issue for them. This scepticism is not limited to my participants and is demonstrated in work carried out by the Pew Research Centre (Madden, 2014), who found that there was a level of scepticism amongst their participants, particularly around the potential benefits offered by sharing information. However, they did find that in particular situations, individuals are willing to share their information if it allowed them to access a service or website without incurring a monetary cost. The responses are shown below, alongside responses to the same question in my survey:



[9]

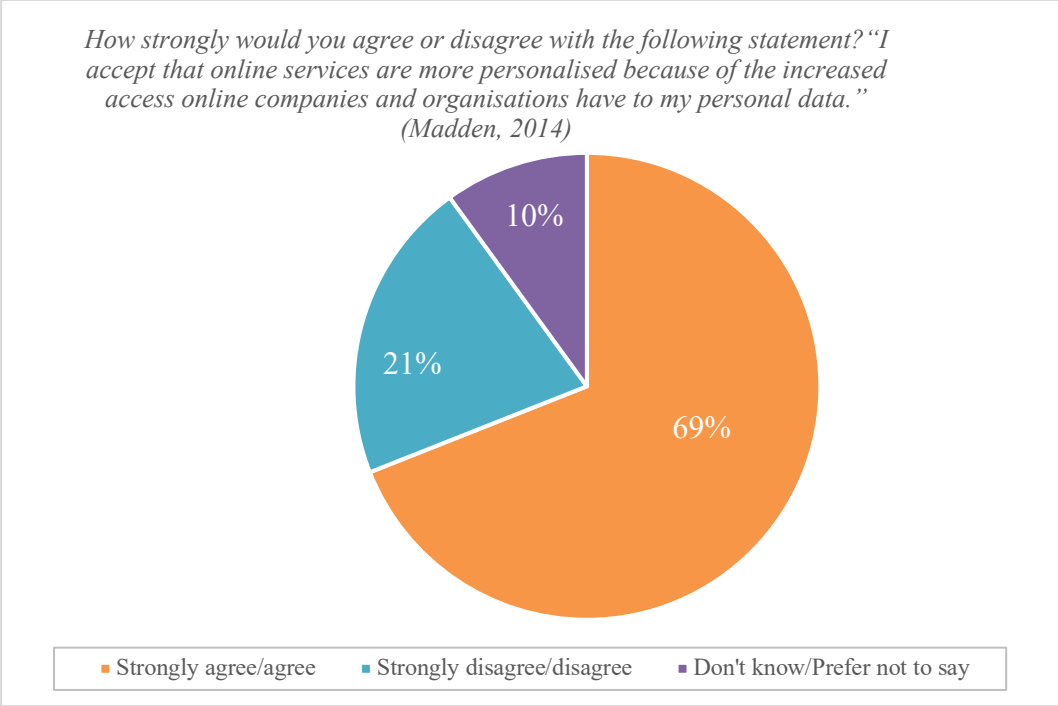
It is clear from this chart that opinion tends to be in favour of sharing information in order to access a site or service provided by a company for free. It is interesting to note that the level of agreement is higher for my participants than for the Pew Research Centre participants, however, this may be due to the surveys being carried out at different times (the Pew Research Centre survey was carried out in 2014, whereas mine was carried out in 2016/17). Therefore, attitudes may have changed over time, as we are increasingly making these tradeoff decisions in our daily lives. Another important point to note is that the respondents for the Pew Research Centre covered a wide range of ages, while all of my respondents were aged between 20 and 40, and so older adults may be more reticent to such a tradeoff, which could have lowered the overall level of agreement for Pew Research. Finally, it is possible that the difference relates to the fact that participants for each of these surveys were from different countries. The Pew

[9] Please note, percentages do not add up to 100 as those responding 'Don't know' or 'Prefer not to say' have been excluded

Research Centre carried out its research exclusively in the United States, while my survey was carried out online, and so would be largely completed by participants in the UK (although this cannot be guaranteed)

One further reason for the higher level of agreement in my survey could be that individuals feel that they are in control of what they share with companies and so believe they are able to choose how much information to reveal. This potential explanation will be examined in more detail later in this chapter.

Further to the above question, my survey also asks participants about another aspect of the tradeoff bargain - personalisation:



Again, here it seems that participants willingly accept that they will receive more targeted advertisements and recommendations if they share some of their data. As stated in one the quotes previously, individuals know that they are likely to face advertising regardless of what they do, and so it is often deemed to be preferable

for it to at least be something that might actually be of interest to them. There was the sense that advertising is inescapable, so it makes sense to them for it to be potentially useful, rather than for a product that is not. It is interesting to note that both of the above questions attract similar percentages who either agree or strongly agree with the premise offered as per the table below:

	% Free service *(n)*	% Personalised service *(n)*
Don't know/Prefer not to say	6.23 *(19)*	9.84 *(30)*
Strongly agree	5.57 *(17)*	20.00 *(61)*
Agree	63.93 *(195)*	49.18 *(150)*
Strongly agree/Agree	**69.50 (212)**	**69.18 (211)**
Disagree	18.36 *(56)*	16.07 *(49)*
Strongly disagree	5.90 *(18)*	4.92 *(15)*
Strongly disagree/Disagree	**24.26 (74)**	**20.99 (64)**
Total[10]	100.00 *(305)*	100.00 *(305)*

This bears out the comments made by my interviewees, in that individuals appreciate that in order to access particular services, it is only fair that they give up something, which, if it is not going to be money, will be something that is of value to the company, such as their information.

While the overall agreement and disagreement percentages are similar, when broken down further, there is much stronger agreement with the statement that

[10] Please note, this question was not compulsory and so participants were able to move on to the next question without providing a response.

focuses on receiving a more personalised service (20.0%), than the one regarding receiving a free service (5.6%). This hints at the view that while there is no monetary charge when accessing a service for free, that is not to say that individuals believe it to be completely without cost. This means that for all of the narrative surrounding free services being provided by social media sites (for example), this is not necessarily widely believed, and individuals are aware of the costs involved.

It also highlights that individuals feel that receiving a personalised service is of greater benefit than accessing a service or website for free, particularly if they do not actually believe that it is free. This may be because the benefits of personalisation feel more tangible to people than simply accessing a website for free. As Floridi (2015) highlights, we have become used to free access – very few websites hold content behind a paywall and so it has become the norm to access a website without having to pay for the privilege. As such, we have come to expect to access content for free, and so the benefit of doing this has become less obvious to us than receiving a relevant recommendation. Personalisation feels as if we have saved time and/or effort, because the advertisement (and by extension the item) has been brought to us, rather than us having to search for it.

Are individuals willing to pay for privacy?

Although many appear to accept that trading information is the price we pay for accessing some websites, views around paying for additional privacy are ambivalent. This is something that I wanted to explore, as it offers an alternative to the bargain individuals are currently presented with, in terms of sharing information in order to access reduced prices, and/or special offers. It also makes

sense given that companies treat our data as a commodity (as discussed at greater length in my literature review), and so it is important to consider how individuals feel about paying to retain a greater level of privacy, particularly as many would like greater control over their information. This is also a topic which has been discussed in online articles (Tufekci, 2015), as well as having been investigated previously (Preibusch, et al., 2013) suggesting that it not something that can be ignored or dismissed completely. It is important to note that in considering this, it is suggesting that privacy is property, which is not necessarily the way in which privacy is perceived by many, however I approach this from the perspective of the commodification of privacy and the way in which it has become a commodity to many companies (particularly, but not limited to social media (Fuchs, 2014)). This also links with the work of Zuboff (2015 and 2019) and Couldry and Mejias (2019a and 2019b) which were discussed in my literature review. Here, I offer a brief reminder of their pertinent points when we consider the option of paying for increased privacy. In her discussion around 'surveillance capitalism' (2015, p.77), Zuboff suggests that companies collect as much data as possible for each individual that utilises their site, thereby increasing their profits. Similarly, Couldry & Mejias (2019b) argue that the basis of our everyday lives have been changed in order to allow our data to be collected and collated, without us realising. Even when we are aware of the information being collected, companies are more than capable of convincing us of the benefits of sharing our information (Couldry & Mejias, 2019b). This then allows companies to continue to collect our information and sell it on without concern for those supplying it (this issue was dealt with in my literature review when I discussed the potential exploitation of users). As such, the question remains that if companies are able to make money from carrying out data collection and aggregation, does it not redress the

balance somewhat if individuals are offered the option of paying to avoid this? This point in particularly pertinent when consideration is given to Zuboff's claim that surveillance is not attempting to remove privacy rights, rather it is re-distributing them, so that they are no longer spread between all individuals but concentrated amongst surveillance capitalists. Therefore, if individuals are interested in paying for additional privacy, they are in effect paying to restore the original distribution of privacy rights. However, views on the subject are not clear-cut and there is ambivalence here, as highlighted in the responses to the below question:

How strongly would you agree or disagree with the following statement?
"I would be willing to pay more for a service or product if it meant I could share less information." (Madden, 2014)

	% All *(n)*
Don't know/Prefer not to say	19.67 *(60)*
Strongly agree	10.16 *(31)*
Agree	28.20 *(86)*
Strongly agree/Agree	**38.36 (117)**
Disagree	35.74 *(109)*
Strongly disagree	6.23 *(19)*
Strongly disagree/Disagree	**41.97 (128)**
Total[11]	100.00 *(305)*

There is little difference between those who would be willing to pay in order to share less information, and those who would not (3.6%), with a greater proportion

[11] Please note, this question was not compulsory and so participants were able to move on to the next question without providing a response.

of respondents unwilling to pay. This suggests that offering people the option of paying a premium for privacy is not necessarily the solution to concerns regarding the amount of information we share with companies. This also highlights the complex nature of our relationship and views regarding free services that we gain access to through sharing personal data, and the difficulty in finding a simple solution to this issue.

Previous work around the subject of paying for increased privacy is also unable to obtain a definitive answer. As discussed in my literature review, Preibusch, et al. (2013) carried out a series of experiments to test how the tradeoff between price and amount of data collected impacted on individuals' decisions when making a purchase and offered some surprising insights. Their study found that individuals do not necessarily choose to purchase items from companies that collect less information, even when the price is the same as companies collecting more information. The researchers offer the explanation that it may have been because individuals assume the collection of additional information would lead to greater personalisation if and when they revisited the site at a later date. This again suggests that the potential for personalisation is a much greater influence than is expected, although, the researchers could not say that this was definitely the reason. In terms of price, they find that for those individuals who are already concerned about their privacy, price is not important and they are happy to pay more to share less information.

This is borne out by other research, which suggests that those who are already concerned about their privacy are willing to pay more to share less information (Tsai, et al., 2011). However, they are unable to say whether the price should be

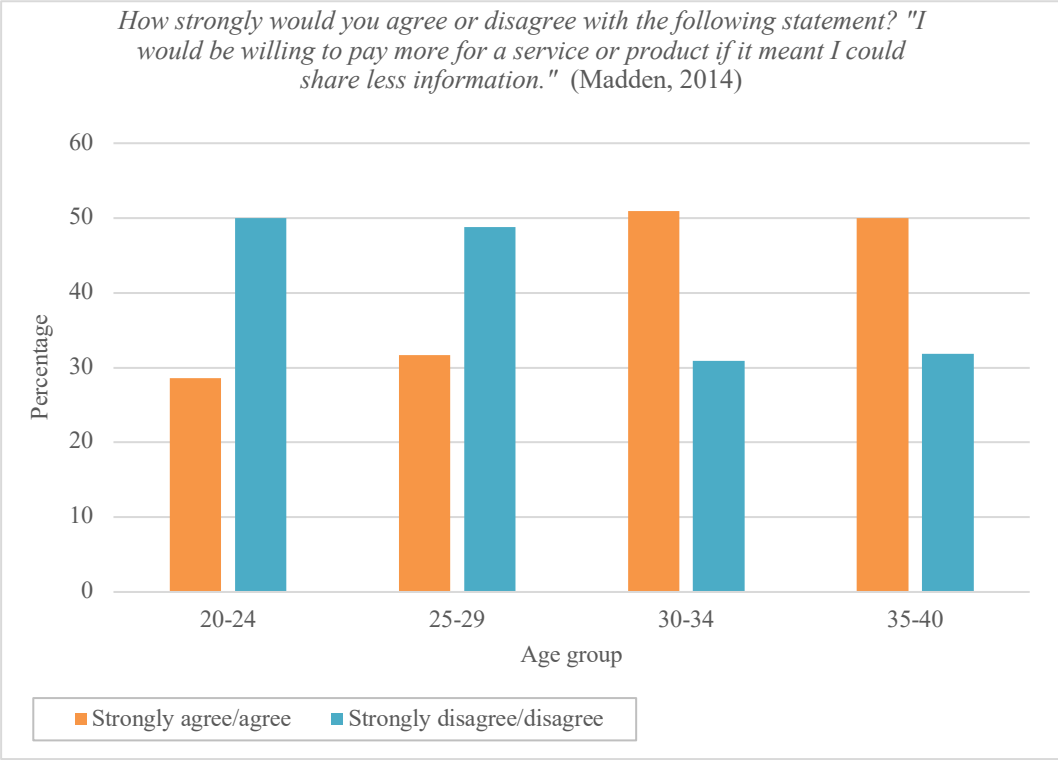
an absolute amount, or whether it should be relative to the price of the item being purchased. This suggests that at least some of the complexity in offering privacy for a price may be in the price itself. The price difference in the DVD experiments above (Preibusch, et al., 2013) was €1, therefore, this may be small enough that those already concerned about their privacy are willing to pay it, but if there was a greater price difference, they may have been less willing to pay. This links with the findings of Hann et al. (2007) who find that where companies offer a monetary reward for personal information (in the form of discounted prices or the chance to be entered into a prize draw), individuals are more likely to be motivated to share information. They suggest that if the reward is large enough, it will negate any concerns regarding privacy, although it needs to 'exceed a threshold of $10-20' (p.27).

There is some research which suggests that individuals are willing to pay a premium for privacy (Tsai et al., 2011), and this offers an explanation for the ambivalence expressed by my participants towards paying. The issue may be dependent upon the actual cost that people would be expected to pay to protect their privacy. It is possible that they would be willing to pay a minimal amount, but if companies ask them to pay over a certain amount, it would be deemed too high and they would need to reconsider whether to share the information or use the company at all. This would also explain why the responses to my survey question are clustered around 'Agree' and 'Disagree' options, rather than the stronger versions of these opinions. The willingness to pay to share less information is also likely to have a contextual element to it in that it will depend on the type of information being requested, so an individual may be more willing

to pay not to share their medical history (for example) than their favourite colour. The issue of context will be dealt with in the following chapter.

Previous studies regarding the impact of price upon charity donations are relevant here. Weyant and Smith (1987) consider whether suggesting large or small donation amounts makes a difference to the actual amount that people donate to charity. They find that when small donation amounts are suggested ($5, $10 or $25), more money is raised overall than when larger amounts are suggested ($50, $100 or $250). They put forth that this is because when a larger amount is suggested, it de-legitimises any smaller donation amounts, so that even though individuals are able to donate any amount that they choose, the suggestion of larger amounts leads to individuals feeling that a smaller donation would be inappropriate. This has interesting implications for my findings, as how willing an individual would be to pay for their privacy could depend on the price that is being requested, as well as the importance that the individual places upon that information. It may have therefore, been useful to offer survey participants the option of 'It depends' (and allowing them to expand on this), when responding to the question regarding whether they would be willing to pay more to reveal less information. Therefore, it is worth bearing in mind that there are multiple ways in which price can make a difference.

Opinions on the subject of paying for increased privacy become clearer when we separate respondents into their respective age groups:



(r-square: 0.009, p-values: 0.000-0.775)

Here there is a clear divide between those in their twenties and those in their thirties, with the older groups being much more willing to pay for privacy than younger groups. There are a number of possible explanations for this. One reason is that those who are older are simply more able to pay for increased privacy, they are more likely to be settled in a career and earning more money than their younger counterparts and so for them it may be a case of being able to pay to avoid the things that they find unacceptable. In fact, recent work by the Pew Research Centre (Madden, 2014) suggests that 67% of US millennials (broadly this term is used to describe those born between 1981 and 2000) do not believe that they currently earn enough to have the kind of life that they want. As such, if millennials are not earning the amount they would like, it suggests that they cannot afford everything they desire and privacy may be one of those unaffordable ideals.

This has been reinforced by studies that show that those in this generation are financially worse off than those in previous generations (O'Connor, 2018). It suggests that those in their late twenties are less likely to own their own homes than those in their early thirties. The issue of student debt has also had an impact on individuals' incomes, and it is worth noting that my survey was completed by a disproportionately high volume of those who had completed higher education (26.5% had completed undergraduate studies, while 35.9% had completed postgraduate education). Therefore, those who have recently graduated are likely to be dealing with student debt, which would, again reduce an individual's level of disposable income and thus their ability to pay for increased privacy.

Another potential explanation for this difference in opinion is that these age groups do essentially represent two distinct groups; those who are used to getting and sharing information for free (those in their twenties) (Twenge, 2017) and those who are not (those in their thirties). Therefore, those in their twenties are simply more used to making this tradeoff and so if it is a social norm for them, then it is entirely possible that they have never considered it being any other way. Those in their thirties, however, are far less used to it and so are potentially more suspicious of the suggestion of access to services or websites for free. Therefore, they consider this bargain more and would rather avoid sharing more of their data and are willing to pay to do so. Different age groups may also have different attitudes towards technology and social media; boyd (2014) suggests that teens differ from adults in that they are more accepting of social media in general. They are unconcerned about the changes brought about by technology and are far more interested in the benefits that it offers. Adults, on the other hand, are far more aware of how things were previously, (before the introduction of technology) and

as such recognise the changes that have occurred. This can lead to differences in attitudes and concerns, as boyd suggests, 'To teens, these technologies…are just an obvious part of life in a networked era, whereas for adults, these affordances reveal changes that are deeply disconcerting' (2014 p.14).

While this discussion around teenagers' attitudes may not appear to be relevant to my work, boyd's research was carried out between 2003 and 2012, and so these teenagers will now be adults, who may retain these attitudes towards technology and social media. This offers a potential explanation for the difference in views in the above graph, therefore, those who perceive social media as being a part of their lives, may be less concerned about their privacy, believing that this is simply the way things are. Older individuals, on the other hand, are likely to remember how things were before, and so may be more willing to pay to regain some of the privacy that they feel they have lost due to social media sites. Therefore, the choice of whether to pay for increased privacy, may not be a choice for everyone and so it may be necessary to share information in order to achieve discounts on products or free access to social media. For my younger participants, it may be that privacy is a luxury they are simply unable to afford.

Are acts of defiance possible?

This section will provide a response to the following question:
How do individuals attempt to regain some control in situations where they seemingly do not have any? Given the discussion in the previous chapter, and above, it may seem that it is impossible to have meaningful control when dealing with online companies and the only sensible way forward is to submit to the status

quo and share whatever information we are asked for. While it is true to say that there is an asymmetry of power, in favour of the social networking sites and other organisations, that is not to say that everyone who engages with social media has given up on having a level of privacy that they are comfortable with.

Therefore, in small, seemingly insignificant ways, people are drawing a line and refusing to move beyond it when they feel that companies are attempting to collect an unreasonable amount of information. As such, individuals have developed a number of 'tactics' (de Certeau 1988 p.185) that they employ in situations whereby they are not comfortable with sharing the information being requested. These tactics offer a way to resist the increasing demands for information that we are faced with.

Gillespie (2007; van Dijck, 2013; Cohen, 2017 and Bucher, 2018) suggests that technologies guide their users down the path of acceptable behaviour and often facilitates some user actions while restricting others. Although we would like to think that we are in control, we generally use the technology offered to us in the prescribed ways, rather than demanding that the technology changes to fit around how we would like to use it. As noted in the previous section, individuals will often forego some privacy or control in order to achieve greater convenience, which is what makes technology so persuasive, it allows us to 'get things done' more efficiently so that we can move onto something else, as illustrated by VR's comments:

> "Most of the time, right, even in life, anyone, most of the time you're in a rush, you're never just sat down doing something, you're in a rush to, I

> don't know, you're late for work, or, you know, as you know…and you're just doing it [HE: yeah], just err, and you're not even thinking about it, like, paying bills." (VR, female, 28)

VR's comment highlights how technology provides a means to an end, and as such we do not necessarily consider alternative ways to use it. It also means that as we come to rely on technology to carry out mundane, everyday tasks, we forget how we completed these tasks previously and become frustrated when there is an issue with the technology. At the beginning of December 2018, there was a data outage which meant that O2 customers were unable to access any services which relied on data to work (BBC News, 2018b), this led to customer complaints regarding the difficulty they had in carrying out simple tasks such as finding their way around in a new city. It appears that those complaining have become so reliant on using apps on their smartphones to navigate that they were (literally) lost without access to location services. This demonstrates a reliance on technology that causes issues for individuals when it fails them.

Gillespie (2007; van Dijck, 2013; Cohen, 2017 and Bucher, 2018) also notes that in any given situation, there are structural constraints which tend to be overt but there are also more implicit cultural rules. Often explicit reasons are given for the existence of certain rules or terms and conditions, such as requiring users to provide their real names, in order to protect them from potential identity theft. There are, however, also subtle means in place which encourage users to be more passive and simply move in the direction they are being steered.

How is disciplinary power exercised on social media?

This links with Foucault's work regarding disciplinary power (1977), which offers a useful explanation for our behaviour when sharing information, as per the discussion in my literature review. As a brief reminder, Foucault suggests that we are encouraged to behave in particular ways, as certain behaviour is rewarded; this is not necessarily something that is obvious and we only tend to notice this when we feel friction when attempting to behave in a way that is in opposition to what is expected. We thus 'become' through this covert discipline (1977), and as discussed throughout this thesis, it is in the best interests of social media sites to encourage users to share as much information as possible so that it can be packaged and sold to others. Foucault (1977) suggests that the environment thus becomes a tool for training those within it and this is what I argue has happened on social networking sites, in that users are 'trained' to connect with as many friends and acquaintances as possible, all the while, generating income for the platforms they are utilising. Therefore, disciplinary power is not only integrated, but almost completely hidden from users, who do not have this option. It is also important to note that while the actions and behaviour of users is revealed to the platform owners of the site they are using, it is not limited to that site, and through the amalgamation of data (as discussed in my literature review) come to be known by the owners of sites they have never used or visited. During the course of my interviews, only one interviewee mentions data from social networking sites being amalgamated and sold. While many speak with annoyance about their information being shared with advertisers, none appear to view this as being coercive, or anything to be concerned about, again, this is how disciplinary power operates, it is largely hidden from view, so as not to draw attention to what is happening.

Similarly, Foucault suggests that those who are disciplined are unable to see power, rather it is felt when their bodies feel restricted and unable to move in a particular way. As such, I suggest that this happens on these sites when an individual is directed to follow a particular order of actions, without deviation. Often, when completing a registration form, the information is requested in small chunks, so, for example, a person might be asked for their name and address details on one page, and on the next, their banking details and so on. In this way, they are being directed to share specific information in a particular order and are restricted, and often unable to move on until all fields on the current page have been completed. This is frustrating for my participants:

> "Erm, yeah, I find that irritating, you know a lot of the time they ask you for information that seems superfluous, obviously for marketing and you, they don't let you progress with buying something unless you actually fill in the details" (GM, female, 37)

> "Companies? Mm, God, I, I, I hate it, I find it unavoidable sometimes, you know for example, you've gotta sign, to get 10% off in a store or whatever, you've gotta like put your e-mail down" (TM, female, 25)

This again links back to the often-heard complaint from my participants that companies collect too much data from us, and as such, this is not necessarily something that participants are accepting of as part of the tradeoff bargain. Their frustration often leads them to consider ways in which they could access the

website or service that they wanted to without having to share data that they were uncomfortable sharing.

How can small wins increase control?

Therefore, while individuals are often required to share information with companies, that is not to say that they will always do so. Even in situations where it may appear that the only options available are to share the information or discontinue the transaction or registration process, that is not the case. My participants found ways around sharing this information:

> "Erm, again, I, I literally will give erm, I have a redundant e-mail address erm, which I will give them as my initial contact, erm, and I never give them the right mobile number, I change the last digit." (CB, male, 37)

> "…sometimes I just lie because I'm irritated erm, I almost always try to just not fill it in and I only then fill it in if they won't let me progress and then erm, and then yeah, I lie and then later on I get e-mails, so I put in everything, like, fake names, all this kind of stuff, and then I get lots and lots and lots of e-mails to these fake names so I know, I mean, I don't, I never remember which website that I've put that particular fake name to but I'm just like, 'Well, clearly they are selling my data', even if they say they aren't…" (GM, female, 37)

It is clear that individuals are not simply accepting that they must provide information to a company and when data is flagged as being mandatory, they resist in a subtle way, which allows them to gain access to the service or website

without having to provide their data. I term this behaviour 'small wins', as it offers a means of resistance, which is likely to go unnoticed by the company itself, and at a macro level, will change very little. However, for my participants, it gave them a feeling of power, of not being forced to submit to someone else's will. It allowed them to feel that they had 'got away' with bending the rules. In Foucauldian terms, it allows them to resist the disciplinary power and exercise a little control in a situation in which they appear to be powerless. Please note that when I am discussing control here, I mean in the sense of individuals being able to make the decision of whether to share information with a company and behave according to that decision. As discussed previously, there are often times when people are compelled to share information that they are not comfortable sharing, and so when I speak of control here, it refers to individuals having the ability to behave in ways that align with their beliefs. The work of de Certeau (1988) and Fiske (1989) is particularly relevant here, as both speak of the various tactics available to those who are disempowered versus the strategies of those who are powerful.

De Certeau argues that rather than being submissive, individuals may appear to have accepted the dominant message, but have instead subverted it in their own covert way. He speaks in terms of 'strategies' and 'tactics' (1988 p.185), to highlight the difference in power in these sorts of relationships. He defines strategies as practices coming from a position of power, offering the 'proper' way to behave. I argue that strategies are utilised by social networking sites when they direct users' behaviour and as examined above, are able to allow or deny access to their resource. As such, the terms and conditions set out by these sites offer the 'proper' way to behave. Tactics on the other hand, are for those deemed to be

'other': those who are on the margins who have no power. Tactics are not deemed to be proper, however, they are often employed in daily life. Therefore, de Certeau suggests that tactics are a tool for people trapped in a system that they are unable to escape from, in other words, they provide the means to subvert the dominant system and spaces. If we, again consider social networking sites, here, these could be described as being a dominant space, for the reasons outlined previously, in terms of the rules that those inhabiting those spaces are expected and required to follow.

Although the spaces in which consumers are able to utilise tactics is growing smaller, there is still room for subversion. When subversion occurs, it is not a case of the imposed rules being overtly rejected, instead they are used in a modified way, this is why, it may appear to others that the dominant message has been taken on by those in a submissive position, but this is not the case (Fiske, 1989). As such, it seems that they have accepted their position, but this is not so. This style of subversion is not planned, rather it happens 'in the moment', when an opportunity presents itself.

I would describe the actions of my participants as employing 'tactics' in order to maintain the level of privacy that they are comfortable with, while appearing to share the information that companies require. Participants describe the tactics they employ without a second thought; it is simply something that they do:

> "That's the thing, look at Facebook for example, I mean I write a post about once a month, I, I go on it all the time, but I don't ever actually do anything on it. So, because I'm not doing anything, I suppose in a sense,

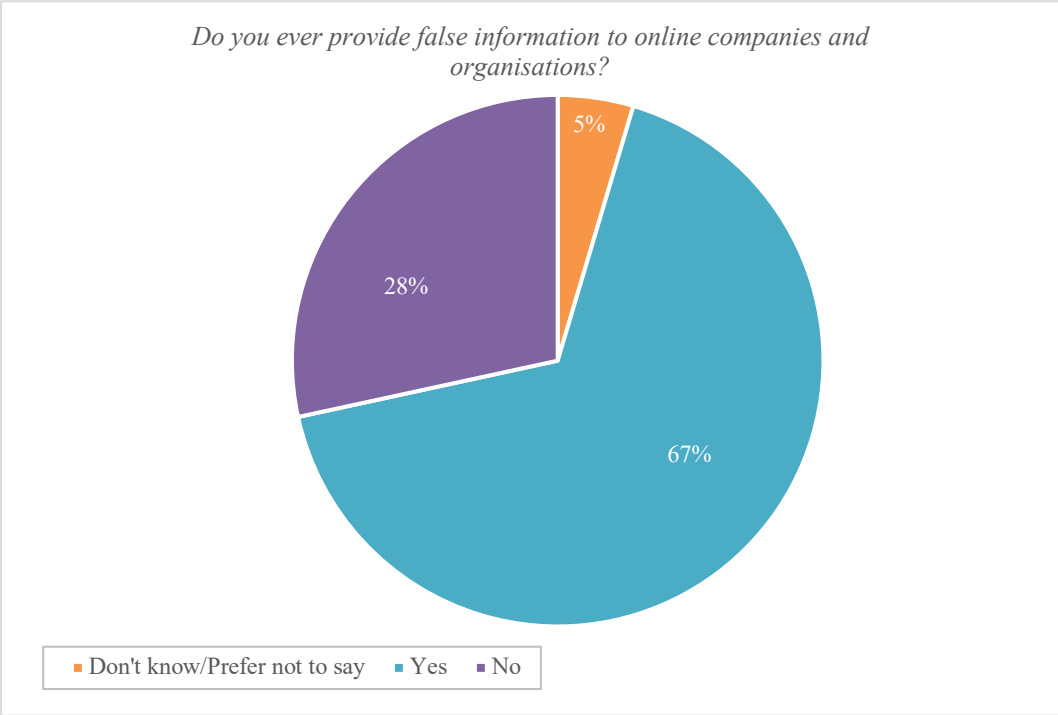
> I'm not really contributing in the way that they, businesses would want, or people would want. Erm, yeah, so I suppose in that sense it doesn't really work on me quite the same as it would others…" (LG, male, 24)

> "So, so, for example, I have a erm, I have a, I have a main e-mail address and then an e-mail address for junk…I have a kind of fake date of birth in, in, in, in my head…Erm, yeah so I will, I will, I will, purposefully deceive them in order to pass the form…err then I'm gonna give you what you want, but I'm not necessarily going to give you the true value of it."
>
> (PW, male, 37)

This suggests that these participants are 'making do' with the tools available to them. The company they are interacting with requires certain information from them, however, they are subverting this requirement by supplying false information so that they can access the website without compromising their privacy. In essence, they have fooled the company into believing that the data they have supplied is true. My participants understand that they are subverting the system in some way, as the quotes above illustrate, particularly the second quote, in which PW talks about how he will supply false information so that he can gain access to the website, but he will not give the company anything of value, in terms of true information. This type of behaviour is not limited to my participants, and has been described in other studies, in similar ways. Hargittai & Marwick (2016) describe how students struggle with navigating Facebook's privacy settings and so take matters into their own hands in order to achieve their desired level of privacy; this includes providing pseudonyms, rather than their real names.

Employing tactics as described above, can be a useful way for individuals to feel in control of what is happening to their information, and this can lead to them feeling less concerned about their privacy (Nowak & Phelps, 1992). It seems that simply being able to take action can reduce worries in this area, potentially because it moves control back into the hands of the individual, rather than the company (even if only in a small way). This links with the previous chapter and the importance that people place on feeling in control of their information and what happens to it, as such, supplying false information to companies can lead individuals to believe that they have more control. This can be particularly helpful in situations whereby individuals feel unable to trust those collecting their information and as such may mitigate the discomfort of sharing information with an organisation that a person does not trust.

Supplying false information I not a new tactic and when carrying out research previously, Metzger (2004) found that 20% of his participants admitted to providing false information. Although I did not ask my survey participants whether they had done this while completing my survey, I did ask them whether they ever provide false information:



This suggests that sharing false information with companies is widespread practice for my participants, as two-thirds of respondents admit to doing so. Although I did not ask them to specify the type of information, I suspect that often it is their e-mail address, as many of my interviewees had set up an email address specifically for 'spam' emails. In this sense, it is not strictly speaking, false information, as the e-mail address does exist, but it is more that it is not the person's main e-mail address, and so is not one that they check regularly. However, it is still a tactic that they are employing, as it is subverting the dominant power, by refusing to submit to the expectation of the company requesting information.

While supplying false information offers individuals the opportunity to appear to be participating in the social norm of sharing information (when they are, in fact subverting this), that is not to say that it is the only method employed in these situations. There is a more drastic alternative: refusing to share information

altogether. Although this is an obvious refusal to engage with the social norm and so may not appear to fall under the 'small wins' theory I put forth, this is not the case, particularly when we consider the work of Fiske (1989) in greater detail.

Fiske suggests two ways in which individuals can employ a counter-reading of the dominant culture, through 'resistance' or 'evasion', (1989 p.2) which I argue is broadly the two categories that my participants' responses fall under. It is important to note that it has been argued that any form of evasion or resistance that takes place on an individual level is occurring within the status quo and so cannot be considered true evasion or resistance. However, this ignores the micro level of everyday life and as such does not recognise the differences (as well as the links) between the various levels of resistance. It is also important to note that at an individual level, people may feel unable to make grand gestures which lead to large-scale changes, but by utilising evasion or resistance, on a day-to-day basis, they feel slightly more in control. In this way, individuals are drawn to resist the meanings being offered as a way of having autonomy over the meaning of their life, which they do not have ordinarily. Where individuals have no control over their lives, they cannot be empowered individuals, which means that they are unable to take social action. In situations when individuals are able to make gains in their daily lives, it means that they have been able to create space in which they can take action and create shifts in social power relations (albeit potentially small ones). It is also worth remembering that de Certeau (1988) also recognised that it is only possible to resist from within the dominant culture, not from outside of it.

It has been argued that if individuals are focused on merely improving conditions for themselves (rather than radically altering the system as a whole), then these tactics work to make the system itself stronger and delay the possibility of any real change. However, Fiske argues, that the resistance offered by popular culture has an impact at a micro level, and it offers a gradual erosion of the micro level, thus 'weakening the system from within' (p.11). I would suggest that this is what is happening when individuals share false information, because in doing so, they are supplying information that offers little (if any) value to those collecting the data. Therefore, when it is linked with other data, even if that information is correct, the inferences or predictions made will be based on partially incorrect information and so are less likely to be accurate. The impact of this may be limited, if only a few people take this action, as those collecting the information are unlikely to notice and may in fact only succeed in ensuring that the individuals themselves are presented with advertisements that are not relevant to them. However, if this action was taken on a larger scale, it would raise questions regarding the efficacy and efficiency of the commodification of individuals' information and could potentially render it pointless. It is important to note that this would require a large number of people to take this action and given that the actions of companies are broadly hidden when considering what happens to our data once we have shared it, this is unlikely to happen (although not impossible). It is also worth considering that generally, in their day-to-day lives, individuals are not necessarily aiming to make grand structural changes, rather they are often simply trying to make it through the day, with as little fuss as possible.

Fiske (1989) suggests the shopping mall as an example of a place where resistance can occur through acts of subversion. As such, although it is a place for

consumption, the shopping mall is freely accessible by individuals whether they intend to make a purchase or not. Therefore, when individuals visit the mall with no intention of consuming, they are subverting the purpose of that space. I suggest that this can be adapted to describe one form of subversion which occurs on social networking sites, in terms of those who join these sites but refuse to post regular status updates therefore resisting the dominant use of the space and refusing to use it for its intended purpose. This ensures that the owners of the site are able to collect very little information about them in order to sell it to advertisers. This is exemplified in the below quote:

> "That's the thing, look at Facebook for example, I mean I write a post about once a month, I, I go on it all the time, but I don't ever actually do anything on it. So, because I'm not doing anything, I suppose in a sense, I'm not really contributing in the way that they, businesses would want, or people would want. Erm, yeah, so I suppose in that sense it doesn't really work on me quite the same as it would others…" (LG, male, 24)

Fiske would argue that this individual is able to 'evade…control' (1989 p.33) and as such LG can freely use Facebook to contact friends and family in a convenient way, without having to pay for it with his privacy.

Fiske offers a further example which is useful here, when he discusses those who play video games in arcades and attempt to play on machines for as long as possible, having only paid a minimal amount of money to do so. This is seen as a battle against the arcade owners, whereby the video game players 'win their pleasures…by resistance rather than through cooperation.' (p.86). Therefore, it is

a way of taking control in a system which is set-up to encourage people to spend money quickly, therefore when a player is able to play for a long time with very little cost, it is seen as 'beating the system' (p.81).

In the same way as above, this could be used to describe the social media users who enter as little information as possible when creating an account with the site. The aim in this case would be to enter as little information as possible while still being able to maintain relationships with others through the site. The battle here is between the social media site, and the user, with the user managing to 'beat the system' (Fiske, 1989 p.81) if they are able to share minimal data, thus making them essentially worthless to the site as there is little to sell to advertisers. It is a way of refusing to provide surplus value, while still making use of the resources offered by the site, essentially for free. It is important to note here that (as discussed in my literature review), social media relies on more than simply the information we post (Bucher, 2018) and as such inferences are made based on who we are linked with and so this may not be quite as effective in terms of evading the collection of information as perceived. While this is not overtly recognised by my participants, it was mentioned during the discussion of sharing false information:

> "Erm, yeah so I will, I will, I will, purposefully deceive them in order to pass the form…err then I'm gonna give you what you want, but I'm not necessarily going to give you the true value of it." (PW, male, 37)

Therefore, this participant is quite open about providing false information that will have no value to the advertisers who will be sold his information (because it

is not truly his information). The sharing of false information is another method that can be used to beat the system, especially when the information being requested is mandatory. Therefore, by providing false information, the user is again able to access the site without paying with their information. While many do not necessarily speak in the same terms as this participant, there is a recognition that providing false information is a way of refusing to play by the rules of the social networking site.

When Fiske talks about evasion, he argues that 'evading this power or inverting it is an act of defiance' (1989 p.9), which is what I argue my participants are doing when they refuse to share information; they are evading the coercive power of the organisations collecting this information and in doing so are refusing to fully engage with it. In many ways, this offers a counter-argument to the neo-Marxist argument put forth in my literature review that while individuals may not consciously recognise that they are being exploited when using social media, they do feel a level of discomfort when asked to provide information they do not want to share. This was described by Foucault (1977) in terms of individuals being compelled to behave in particular ways by disciplinary power, but only noticing it when they feel restricted in some way. As such, when people want to behave in a particular way, but are unable to do so, they have limited options available and so employ methods of evasion or resistance, rather than simply submitting to the inevitable exploitation described by neo-Marxists.

As discussed previously, the two main ways in which individuals are able to defy expectations are through resistance (providing false information) or evasion

(refusing to provide information). Therefore, it will be useful to compare the proportion of individuals utilising these options:

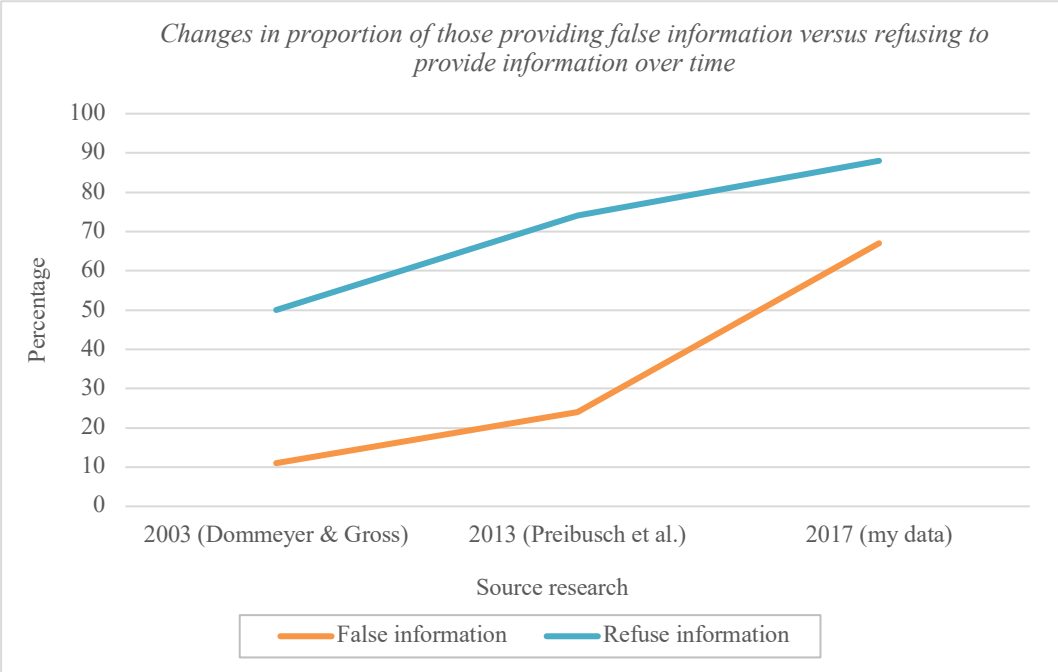
	% Provide false information *(n)*	% Refused to provide information *(n)*
Don't know/Prefer not to say	4.58 *(14)*	3.91 *(12)*
Yes	66.99 *(205)*	88.60 *(272)*
No	28.43 *(87)*	7.49 *(23)*
Total[12]	100.00 *(306)*	100.00 *(307)*

This demonstrates that while people admit to sharing false information (67.0%), they are much more likely to refuse to share information altogether (88.6%). This could be because they feel that refusing to share information feels more honest; they are taking action to demonstrate their reticence towards sharing that information. Some may be uncomfortable with purposely deceiving the company involved, and as such feel that refusing to share information is at least honest. It is also possible that in situations whereby individuals employ refusal of information, there is an alternative company or way of carrying out the task at hand, and so they do not lose that opportunity by refusing to share information. Alternatively, supplying false information may be utilised in situations whereby there is no alternative and refusal of information would present additional inconvenience to the individual. There is also the possibility that those participants had simply not considered providing false information as an option.

[12] Please note, this question was not compulsory and so participants were able to move on to the next question without providing a response.

This distinction between providing false information versus completely refusing to share information can be seen in other research in this area, whereby individuals are much more averse to supplying false information than to simply refusing to share it. In Preibusch, et al.'s (2013) study, participants are asked what they would do if a non-governmental website asked them for information that they did not want to share and offered various options. The majority of respondents say that they would cancel out of the transaction (74%), while others said that they would provide false information (24%). While the difference here is much starker than in my research, both demonstrate a preference towards refusal of information rather than providing false information.

Dommeyer and Gross (2003) reveal similar views in their research and find that generally people will refuse to share information (50%), rather than provide false information (11%) when asked to share a telephone number. This suggests that people are more reticent when faced with the option of sharing false information, Dommeyer and Gross suggest that this may be because '…it is viewed as dishonest and unethical' (p.48). It is interesting to note, that as time has progressed, the proportion of respondents who report being willing to share false information has increased.

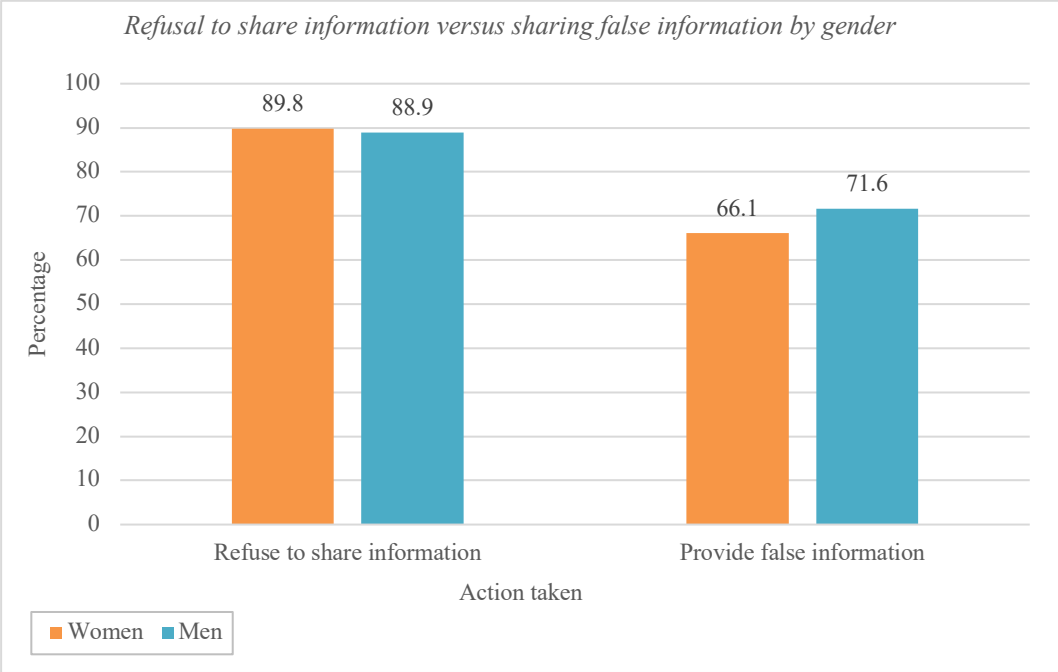


While it is interesting to compare these results it is important to remember that the questions in the three studies are phrased differently, and so the percentages are not necessarily directly comparable. However, it is worth considering why changes may have occurred. It could be due to a change in attitudes towards companies, in that they now feel much more faceless and abstract, and so individuals are less concerned about supplying false information to them. It is also possible that the amount of information we are being asked for has increased over this time period, as the way in which we interact with companies has changed and so we still want to be able to take part in this 'essential' part of daily life, without sharing more information than we are comfortable with.

Some interesting differences come to light when we consider the role gender might play in terms of which tactics are employed. When Sheehan (1999) asks participants how often they adopt particular behaviours when online, she finds that women are less likely to take action than men when concerned about their privacy. For both women and men, refusing to provide information is employed

much more frequently than providing false information. However, while women were more likely to refuse to share information than men, they were less likely to provide false information. The reason for this is deemed to be that men and women behave differently when it comes to protecting their privacy and men are more likely to take an active role and complain when companies collect (or attempt to collect) information that they do not want to share, while women are more passive and so will opt for action that is less confrontational.

Despite the age of this research, my survey responses are broadly in line with this:



While my responses are similar to those from Sheehan's study, there is little difference in the percentages employing each of the methods here, particularly in terms of refusing to share information. This could be due to a difference in attitude and behaviour of men and women, however, it could also be that attitudes have changed over time and it has become more commonplace for everyone to simply refuse to share information that they are unhappy sharing, particularly if there are other means of achieving the same goal.

It is important to note that whether an individual is employing resistance (sharing false information) or evasion (refusing to supply information at all), they are not attempting to change the overall system under which they live, these micro acts offer them a means to improve their daily experience (Fiske, 1989). This is what the 'small wins' I have examined here do; they give individuals a feeling of gaining a little control by being the one who decides what will happen to their information. In that transaction, at that moment, despite knowing deep down that we are relatively powerless to stop the collection of our information on a large scale, the individual is able to simply say 'No', and withhold the information being requested, whether that is through sharing false information or in refusing to share the information altogether. These 'small wins' offer a moment in which individuals take back a small piece of power and are able to feel that they have 'won' in a small way. It is important to remember that although I have suggested that when people refuse to share information or share false information, this is an act of resistance, there may be other explanations for this. During my interviews, participants expressed feelings of control regarding being able to decide whether to share information or not and being able to minimise the information they share, however, this may not be the case for everyone who behaves in this way, and as such other interpretations should not be discounted. Further, my focus here was in the conscious sharing of information, as this is something that participants were able to grasp and take diverging action (if they chose to). However, there are numerous other ways in which information is gathered by companies (Stoilova et al., 2019a), such as the items that individuals click on and the information or profiles they browse. Therefore, data generation is often something that occurs in the background and so is something that people have far less control over, unless

they choose to opt out of using the internet altogether, which as discussed previously, carries many disadvantages. As such, this is why I discuss the above actions as small acts of resistance as the overt sharing of information is not the only way in which social media sites are able to collect information from us. Therefore, even in situations whereby a person is registered with a social networking site under false details and only views the profiles of others, they will still generate a level of information, particularly as companies utilise those we are linked with to make inferences where information is lacking (Bucher, 2018).

Conclusion

The previous chapter considered issues of control, with particular focus on how much control individuals feel they have, whether they would like more and what barriers exist which reduce their ability to maintain the level of control they would like. I offered an examination of the concerns raised by my participants and suggested that continued sharing of information may not be an indication of acceptance, rather a resignation to do so. This chapter built upon this to consider the ways in which individuals can be said to be making tradeoff decisions. This offered a suggestion that rather than feeling apathetic, people are simply weighing up the potential costs and benefits and sharing data accordingly. Individuals are attempting to make logical, reasoned decisions in terms of trading their information for various benefits, (such as product discounts or targeted advertising). I argue that while this may appear to be a positive way for individuals to exercise their autonomy, the situation is more complicated than it initially appears, and due to the 'availability heuristic' (Tversky & Kahneman, 1982 p.20), the decisions we make may not be those that offer the greatest

benefits. This may also be compounded by our time-inconsistent nature (O'Donoghue & Rabin, 2000), in which our intentions towards greater privacy are defeated by the convenience offered in the moment. It is also important to consider the perceived benefits from sharing data such as greater convenience and being able to maintain relationships with friends and family through social networking sites. These incentives cannot be underestimated and the fear of suffering social isolation due to withdrawing from social media in particular may be too much for many to bear. Even when concerns are expressed, people are not necessarily sure what the best course of action is. As such, individuals feel a certain level of ambivalence, especially around whether they are willing to pay for additional privacy. There appears to be an age-related difference in attitudes when considering those aged between 30 and 40 (who are willing to pay) and those aged 20-29 (who are unwilling to pay). However, given the potentially precarious financial situation that many people in their twenties currently face, it may be more a case of being unable to afford to pay for increased privacy, rather than being unwilling to do so.

As discussed in the previous chapter, it can be difficult to exercise autonomy when being asked to share information and, in this chapter, I took this further to use the lens of Foucault's disciplinary power to consider how this is demonstrated through social media. By applying a Foucauldian approach, it is clear that despite not noticing it, we are often subject to disciplinary power in terms of the rules that we must abide by when utilising these sites. This kind of discipline is difficult to recognise, as it tends to rely on coercion to train users to behave 'correctly' and so encourages us to share much of our data, while making it appear that we are making a choice to do so. Although, it may seem that in these situations we are

unable to exercise any real autonomy, I suggest that we can behave as any disempowered group would and utilise the limited tools available to us to tactically subvert the rules (de Certeau, 1988 and Fiske, 1989). These small wins offer the ability to either resist or refuse the data collection we are subject to on a daily basis and take the form of supplying false information (resist) or refusing to provide certain information (refuse). Although they do not necessarily offer large-scale action at a macro level, at a micro level they allow people to maintain the level of privacy they desire, while appearing to have accepted the dominant message that sharing information is preferable. As such while these acts of defiance may not be noticed by those collecting the information, they offer a way for individuals to feel in control in their daily lives.

While the focus so far has been on how individuals feel about sharing their information with companies in a general sense, the next chapter will take a more nuanced approach to this and examine the role that context plays. This will consider how individuals feel not only about the type of information they are potentially being asked to share, but also who they are being asked to share it with.

Chapter Five: Context Matters

Introduction

In the previous two chapters, my focus has been on issues surrounding the sharing of information with companies, and concerns that my participants have around issues of control when being asked to share information. I have examined the ways in which individuals attempt to take control in seemingly small ways, as well as offering an explanation of the various barriers they encounter in their attempts to share only the information they want to. This chapter will take a more detailed view to consider the conditions under which individuals are more concerned about sharing their data.

Initially, I discuss the importance of context to individuals, in terms of the value of being able to keep different areas of one's life separate from each other (this is often a case of professional-life versus personal-life). This section examines the issue of 'context collapse' (Vitak, 2012 p.451), and the problems this can cause for individuals when different contexts overlap, causing a clash between expected social norms. It will also consider the importance of Nissenbaum's theory of 'contextual integrity' (2010 p.2), and how this can be said to offer an explanation for the discomfort we feel when contextual norms are broken.

Following this and utilising the work of Raynes-Goldie (2012), I propose that levels of concern around sharing information depend very much on the type of data being requested. As such, I will be applying Raynes-Goldie's distinction of 'institutional' and 'social privacy' (p.81) to examine how different types of data can evoke different levels of concern from individuals. In creating this

distinction, she suggests that institutional privacy relates to what organisations do with the information that we share with them, while social privacy is linked with information that impacts upon our reputation and who we are in the eyes of others.

While the distinction made by Raynes-Goldie is persuasive, I suggest that in addition to this, social privacy itself can be broken down further, into 'intrinsic' and 'issued' information categories which while not mutually exclusive, offer some potential insights into different levels of concern around different types of information. Within this section, I will also explore an alternative explanation for variations in concern around different types of information, in terms of how immediate and visible the threat is, utilising the 'availability heuristic' (Tversky & Kahneman, 1982 p.20).

The final section of this chapter will consider the impact of different audiences upon levels of concern for my participants. This will focus on my survey results to consider various combinations of audience and information type. While the levels of concern around many information/audience combinations are broadly as expected, there are a number of counter-intuitive findings which will be examined here with potential explanations offered.

It is important to remember that while audience-type offers a level of complication to the concerns individuals have around their information, it is one of numerous additional factors that could be considered. Other factors include (but are not limited to) the reason for the information being requested, and the content of the information itself. As such, some information will be shared with

little concern if the individual it relates to believes that the information itself is of little consequence. This will also be examined in the final section of this chapter. It is important to note that the more factors that are considered when examining privacy concerns, the more will be revealed in terms of the impact they have, and as such, my work here is exploratory in nature.

At this point it will be helpful to provide a brief reminder of what I mean when I discuss the terms 'internet privacy' and 'social media privacy'. Internet privacy is a term I use to encompass any information that we share with companies when online, broadly when accessing a service, whether that is online banking, purchasing an item online or using social media. Social media privacy, however, refers to privacy in relation to a smaller sub-section of sites which we use to connect with friends and family. Both of these terms refer to the collection of our data when we are online, and includes information we may be aware of sharing, as well as information that we are not aware of sharing.

What issues occur when contexts collapse?

Context plays a crucial role in our daily lives. Throughout the course of a day, we move between different contexts, often without giving it any thought. Generally speaking, we are not the same version of ourselves in each situation, rather, we put on what Goffman referred to as a 'performance' (1980 p.109) whenever we interact with others. For example, I might begin my day by working out at the gym, before getting the bus to work, where I spend most of my day working in an open-plan office, later on enjoying lunch with colleagues. At the end of the day I might get the bus home and then meet a friend at the cinema in the evening. Each

of these situations requires different behaviour (and a different performance) and has its own set of social norms, which often only become apparent in the event of them being broken (Nissenbaum, 2011).

To offer an illustration, if I were to sit next to a stranger on the bus and tell him or her about a situation in which my husband had recently upset me and ask for their advice, it would probably make them feel extremely uncomfortable, however, if I did the same while enjoying an evening out with my friend, it would not seem unusual. The social norms of these situations are broadly unspoken but are known to those within them and dictate the acceptable (and unacceptable) behaviour for each one. This highlights the relational nature of privacy, and how it is demonstrated through the interactions that we have with one another (Stoilova et al., 2019a). This conception of privacy builds on the work of Nissenbaum (2010), who suggests that social norms tell us what to expect in a given situation and how they are a product of the society in which they exist. This concept is also highlighted by Blank, et al. (2014) who describe these contexts as being 'circles' (p.25), that represent the different areas in our lives which are generally separate from each other. Therefore, they suggest that there is not a single overarching standard that sets out how we should behave in all situations, rather it depends on the social context in which we find ourselves. This reinforces the importance of the distinction between public and private areas as discussed previously and highlights the way in which we behave differently when we are in a space deemed to be private, versus one which is deemed to be public. In this way, (in a broader sense) we can see how social context exists on a macro level, when there is what many deem to be a binary distinction between public and private areas (although this is not necessarily the case). This highlights the way in

which social context plays a role in our behaviour, even when we fail to consider it.

Nissenbaum (2010) also suggests that contexts do not necessarily stand alone, and highlights the possibility for them to overlap, which leads to individuals having to manage numerous contexts simultaneously. She argues that this is not an issue in and of itself, rather problems arise when action permitted in one context is not permitted in a different, overlapping context (Sheehan, 2002). This causes issues for individuals as it can be difficult to identify what the acceptable behaviour is in such a situation. This is problematic because, as noted above, we behave differently in different situations and so when contexts overlap, we risk having to reveal a part of ourselves that had until that point remained hidden to those in a particular context. This can be troubling as it may mean that others gain a worse impression of us when they discover who we 'really' are (Goffman, 1968).

When this happens, it is often referred to as 'social convergence' (boyd, 2008 p.18) or 'context collapse' (Vitak 2012 p.451) and has become increasingly linked with our online lives, particularly in relation to social media. This is because sites, such as Facebook, have a tendency to blur previously distinct contexts and as such, once someone is added to your list of friends, they are potentially given access to all of your posts and so on, regardless of whether they are a close friend or an acquaintance[13] (Raynes-Goldie, 2012). This is problematic, as it is not how friendships operate in the offline world; here, we may choose to share things with

[13] There are two things to note here: firstly, when posting a status update on Facebook, users can decide to exclude particular friends from seeing that post and secondly, Facebook's use of algorithms means that being friends with someone does not automatically give them access to all of their posts. Dependent upon various factors, a user may only see a limited selection of a friend's status updates. Nevertheless, the potential exists for an acquaintance to have access to more of an individual's Facebook status updates than a close friend.

our close friends, that we would never divulge to work colleagues, for example. This causes issues of control for users especially because social networking sites limit the options available when responding to a friend request to either accept or reject. Whilst in reality, people manage this through only sharing certain posts with specific groups or excluding particular 'friends' from seeing posts, a starker choice is more consciously posed.

The issue with 'context collapse' (Vitak, 2012 p.451) is that 'Information that is well-known and freely available in one circle (say, a family) could be embarrassing or damaging if it were to become known in another setting (such as an employer)' (Blank, et al., 2014 p.26). Therefore, due to this loss of distinction between different contexts, everything is potentially known by everyone, which is problematic for the individual involved, particularly if it casts them in a poor light to their line manager (for example). This is an issue because individuals may post a status update to Facebook, believing that they are doing so in one context (personal context, for example), which has one set of norms 'only to find that others [such as their employer] have taken them to be operating in a different one' (Nissenbaum, 2010 p.225). The potential for a clash of personal and professional contexts is highlighted as a concern amongst a number of my interview participants:

> "Errrr, the only person or people I'd be intere- I'd be concerned about is my employer because… I don't want them to be looking at the things I post online and assuming things about me…I think my employer should have a more professional image of who I am and I don't think them looking at it [social media posts] will give them a good idea of who I am."
>
> (GD, male, 25)

> "Cos I feel like, you know, when I'm in my social life, my friends, it's such a, I'm in a very different world and headspace to when I'm at work." (PF, male, 39)

> "…but Facebook for me is, like I said, you know, I'm trying to keep that as private as I can, so erm, I'm try- I'm cutting out work colleagues as much as I can…I mean I do try to keep work and, and, and, and private separate" (TP, female, 40)

This demonstrates the concerns that my participants have in terms of the potential issue of their work and personal contexts becoming merged so that their employer or work colleagues have access to more information about them than they are comfortable with. It also hints at the way in which many of us attempt to portray ourselves as being professional at work but accept that this is not necessarily who we are when we are not at work.

Therefore, the nature of social networking sites means that we cannot know with any certainty who our audience is; when we post information to Twitter, for example, we have no idea which of our friends will read it and comment on it, or whether they will share it more widely. boyd (2014) argues that if we choose to engage with these sites, there is little we can do, except to accept that context collapses will occur (and attempt to resolve them when they do) or not to participate at all. As discussed previously, eschewing social media completely is problematic for many individuals in their daily lives. Engaging in this way has

become embedded in the everyday lives of many to such an extent that refusal to engage with social media is not perceived to be a realistic option.

Participants are aware of this issue, to varying degrees, and some attempt to fine-tune their privacy options in a bid to gain greater control over who can see their information:

> "I mean for one example, I haven't done this in my existing job, but a previous job where I was, I was friends on Facebook with my manager, I set it up so that he was the only person that couldn't see my posts, cos I just wanted to take that out of my mind that I can post stuff, I think that was mainly about political stuff that I just, I'm sure it probably would have been OK, but I erm just thought I'd rather like just not have to think about what's he gonna think about me saying this stuff?" (PF, male, 39)

> "…I've made dedicated groups sometimes with just the people that I went on that holiday with, you know, for sharing purposes…" (TM, female, 25)

This highlights not only an awareness of the varying contexts that my participants are moving between in their daily, online lives, but also demonstrates the attempts that some are making to gain a little more control, in order to maintain the boundaries between contexts. While they do not necessarily speak in these terms, it is clear that these participants feel it important enough to make efforts to differentiate which groups of people (or individuals) can see specific information about them, and which cannot. Given the additional knowledge and effort required to make these changes, I suggest that the issue of context collapse is important to my participants and is concerning enough for them that they are

taking action. It is also interesting to note here that participants are trying to obscure information, which is not necessarily embarrassing, but rather could cause an issue for them if it were to move between contexts.

While it may seem initially that the issue here is the movement of information between contexts, this can also be linked to my earlier discussion around control. These participants (and others) are making efforts to control who has access to their information and are attempting to maintain boundaries around it in terms of the various contexts in which it can be known. This highlights the importance of maintaining control over this information to ensure that it is only seen by those that they choose to allow to access it. Here, the context in which the information is being shared appears to be less important than controlling who has access to it. PF even says that although he restricted the information that his manager was able to see, he was sure that it would not have been an issue, therefore it could be said that what is actually important to PF is that he was able to take action to control what others are able to know about him, rather than what the information is itself.

This is an important point, as questions are often raised regarding how much the public actually cares about their privacy, given the amount of data that they share, particularly on social media. However, Nissenbaum (2010) argues that if we consider privacy as a right insofar as 'context-appropriate flows' (p.187) of information, it means that it is perfectly reasonable for individuals to say that they are concerned about privacy, while sharing information as long as their behaviour (in terms of what they share and what they withhold) is consistent with the contextual norms of the given situation. There are 'context-relative informational norms' (p.140), which set out the movement for specific types of information and

transmission rules which must be followed (such as the relationship between the transmitter and the receiver and how each party should behave). Transmission principles vary according to context and so, for example, there are differences between the friendship context and the healthcare professional context (although, there are also some similarities). While in both contexts sensitive and confidential information is shared, in the friendship context this will be reciprocal, but this would be completely inappropriate in the healthcare professional context. Therefore, different norms define different situations and what is acceptable within them.

Intrinsic and issued information

Through discussions with interview participants, it became clear that different types of information elicit different responses in terms of concerns regarding the information being shared. Although my initial focus (and indeed the focus of the next section) is on the combination of types of data and specific audiences with access to it, it is useful, when considering types of information, to begin from a broader perspective.

Raynes-Goldie (2012) suggests that an individual's privacy can be separated into one of two broad (but distinct) categories: 'social' and 'institutional' (p.81). While institutional privacy focuses on how institutions use and store our data, social privacy is more concerned with the 'management of identity, reputation and social contexts' (p.82). Raynes-Goldie's concept of social privacy links directly with the above discussion regarding context collapse and the issues that this can cause for individuals, particularly in terms of them being able to maintain control

over the impression that others have of them in different contexts. She also highlights how Facebook only allows users to control their social privacy (through the privacy settings on the site) however, there are no options available which allow users to make changes in terms of their institutional privacy. She argues that this distracts users, encouraging them to believe they have complete control over their privacy when in reality, they are only afforded (limited) control over their social privacy. This in turn, makes it more difficult for users to consider what Facebook itself is doing with their information 'behind-the-scenes' and as such, her participants are far more concerned with their social privacy than with their institutional privacy. This is problematic because if there is greater focus on one type of privacy (in this case, social), there is a possibility that the other type of privacy will be forgotten. Although Raynes-Goldie's focus is on Facebook, I suggest that this could lead to companies in general believing that they are able to do whatever they choose with individuals' information, with little concern or regard for those supplying the data.

Miller (2016) suggests that when companies collect large amounts of information, individuals cease to exist, becoming nothing more than data, which requires no ethical concern or responsibility. He refers to this as 'abstraction', which 'refers to the removal or withdrawal of something from its setting or context' (p.56), therefore, in this situation, individuals cease to be considered to be a 'real' person who should be treated with respect. As such, if institutional privacy is not considered by individuals, companies will continue to collect vast amounts of information, unchallenged, building up ever greater profiles and selling this information to data brokers. This practice is something that people are largely unaware of and so they share more information than they realise and only become

aware of this when a tailored advertisement appears on their Facebook page (for example). Many participants speak about how this makes them feel uncomfortable:

> "the idea of all the adverts that come up on my Facebook, they, they are tailored to either website searches or erm, if I've put my e-mail into something else…Erm it's weird that it comes up on things like my age and my marital status and if I'm in a relationship but not married, and I find sometimes that I get all these wedding, or engagement things pop up…so erm it's those type of things that I find bizarre" (MJ, female, 25)

> "I suppose', but then yeah, on the flip side of that, it's kind of you feel sometimes like you're talking maybe to a…group of close friends, when you're on Facebook or when you're googling you think you're at home, you know, on an evening, on your own just doing some stuff that you need to do, and you realise then when an ad pops up the next day that somebody's watching, or a machine is watching, something is watching and it does make you feel kind of a little bit err, violated, I guess."
>
> (ES, female, 36)

While this may not appear to be a serious issue, it is clear that individuals are not comfortable with the practice and when confronted with tailored advertising, are left feeling uneasy. This is particularly interesting as it appears to contradict the findings reported on page 184 whereby almost 70% of my participants agreed or strongly agreed that they accept online services are more personalised because companies are able to access their personal data. However, I would suggest that

this is not as strange as it may appear, given previous comments from interview participants (MJ in particular), whereby they accept that they do not think about their data privacy on a daily basis, however, when confronted with it in the form of a personalised Facebook ad, are suddenly reminded of how much is known about them, and this leads to feelings of unease. Therefore, potentially my survey respondents are aware of and accept that their data is sold to companies, on an intellectual level, (although they do not necessarily dwell on it) but may feel differently when a Facebook advertisement reminds them that companies know more about them than they had realised or consented to.

While Raynes-Goldie's distinction between institutional and social privacy is persuasive, and her explanation of social privacy is logical, it requires clarification, in terms of which information can be said to be 'social'. She focusses on social information as it relates to information shared on social media sites. This however raises questions regarding other types of information that does not fit neatly into the institutional or social category. As such, Raynes-Goldie's social categorisation appears to offer no clear space for the commercial information that I have been considering throughout this thesis. However, I would argue that as this is information that could impact upon how a person is perceived by others it can still be said to lend itself to the broad category of 'social'. Therefore, rather than limiting my consideration solely to Raynes-Goldie's narrow definition of social information, I instead, suggest that our commercial information can be included in the social category. This is particularly pertinent when we consider the aggregation of our data (as discussed in my literature review), in terms of the inferences that are often made based upon this information, especially as judgement can be made based upon this (as per

Raynes-Goldie's definition). For example, there have been instances whereby an individual's sexual orientation has been revealed to their families before they have had the opportunity to do so, causing issues for them (Fowler, 2012). Therefore, despite information not necessarily seeming to lend itself to the categorisation of 'social', given that it is often linked with more overtly social information, and due to the impact it may have on how others perceive us on its own, I broaden the category of social to include it. During my interviews, a number of my participants spontaneously made a distinction between different types of information:

> "So, I see private information as my location, maybe, and where I've been, but my personal private information, are probably thoughts and things that I would share with family members…So, I see that as slightly different, as that's more intimate to me…that's like numbers, and serial numbers, postcodes…that's all standard information, but I associate the information that was shared from the dating website: feelings, emotions and intimacy as different" (MJ, female, 25)

> "I think it's more emotional privacy, rather than things like my bank card details, or how much money I've got in my account…I personally feel this big divide between like, emotional and kind of, you know, normal information, so like my credit card details and stuff like that"
>
> (SM, female, 36)

> "I would find the dating website the most worrying, in all honesty because I think, you know, that's kind of qualitative information and data, whereas obviously, the rest of what we've spoken about, especially when it comes to the bank details etcetera. They are digital, they are something that can be changed, that can be manipulated etcetera, whereas obviously, the information about you…What makes them, as a person?"
>
> (TM, female, 25)

These participants suggest that there is an important difference between types of social information that individuals share. I have termed these different types of information as intrinsic and issued. As my participants suggest, what I term intrinsic data is related to our thoughts, beliefs, values and feelings, in other words anything that we would potentially consider to be a part of who we are. This type of information is termed as constitutive (or 'ontic') by Floridi (2005 p.198), in that it is a *part of us*, in the same way that a limb is a part of us, and as such cannot be easily separated from us. Issued information on the other hand, is information that is *about* us, and as such, is what Floridi deems to be 'arbitrary' (2005 p.197) data; it is bank account or credit card numbers, National Insurance numbers, mobile telephone numbers and so on. In other words, it is information that is issued to us by others (usually an institution), and as such, can easily be detached from us. It is not a part of who we are, and we have no emotional attachment to it, whereas we are emotionally attached to our intrinsic data, as it forms part of our identity. However, it is important to note that this suggested dichotomy between intrinsic and issued data may not be true for everyone, and as such this is at best considered to be an ideal model of information-type. Deciding where information should fall is potentially an interpretation to be made by each

individual in terms of the level of attachment they feel towards the information in question. There does seem to be a distinction to be made here, between different types of information, as it is something that my interviewees spoke about without prompting, and they had very definite ideas regarding when greater concern would be elicited. This highlights potentially broad categories of information that can be used to consider groups of information, rather than categories of single types of information.

This complication becomes clearer if we consider financial information. At first glance, it seems that financial data (such as account numbers) falls under the issued data category, in that it is not an integral part of our identity, rather, it is information that is ascribed to us by an institution. In Floridi's terms, it is 'attached to the bearer/user like a mere label…it is merely associated with someone's identity and can easily be detached from it without affecting the individual' (Floridi, 2015 p.247). When presented with the vignette regarding a situation in which financial details were hacked and leaked on the 'Dark Web', a number of participants share the view of Floridi regarding their attachment to this information:

> "…financial one, yeah, just again, cos I just think, actually the risk of that information getting taken is [pause]…I think although it's an inconvenience, the impact's actually quite small because if somebody was to, I don't know, clear out your bank account, and it was because of that, then in reality, you'd get it back anyway. So you wouldn't, d'you know what I mean? The actual inconvenience, yes, but actually lose out, no."
>
> (MB, male, 37)

> "I s'pose you know maybe I'm being a bit careless here about the financial stuff so but I, I dunno, I kind of assume that if like money was taken out of my account, although that'd be a big hassle, a) that's unlikely and b) if it did happen, they [the organisation that was hacked] would be liable for that, I assume and so therefore I could recoup it, so that doesn't worry me as much as err, as much as the headlines about these stories suggest that we should be worried…" (PF, male 39)

For these individuals the hacking of their financial data would be an inconvenience, but ultimately, they do not believe it would have a lasting, detrimental effect on them. Their perspective appears to be one of detachment from their issued data, they believe that any damage caused, in terms of money stolen, would be rectified and the money replaced. They do not believe that this would be particularly problematic, in the same way that the loss of another type of data might be. This is in line with Floridi's views regarding arbitrary and constitutive data discussed above. As such they appear to think of their bank details as being something separate from them (issued data); if their details were hacked, they would simply contact the bank and expect any losses to be dealt with and a new account number to be issued swiftly and with little fuss. It is also clear that they believe it is possible to restore any damage caused or losses incurred, as both MB and PF talk about how they would expect any money taken to be replaced, and so in their eyes, it would be almost as if their account had never been hacked, as their balance can be restored to its previous state. This is an interesting perspective to have as they do not appear to consider the prospect of longer-term issues which could be caused if an individual's financial information is hacked, such as incurring a poor credit rating, which could be much more

difficult to resolve. These participants make no mention of this, apparently believing that the extent of such an issue would be ensuring that the bank reimbursed them for the money that was taken and issuing them with a new account number. However, there were also a number of participants who were concerned about the longer-term issues relating to the hacking of their financial information and their perspectives will be considered later in this section.

Intrinsic information

Some participants felt that we are more vulnerable if intrinsic information is hacked and released to a wider audience (as was the case with the dating website vignette):

> "Erm, because of the personal nature of what it was they were sharing and sending. I think it's completely different to knowing where you are…compared what it is you're…saying to someone that is like pillow talk in a way, it's not the same, everything's evolved in the way that we communicate with people. Erm, you share private messages to people online the same way you would have written love letters, it's a completely different way of doing it…I think I'm most, I don't know, I, I feel like I'm most attached to the dating website information being leaked, erm I feel emotionally attached to it, because I think you know, I can see how relationships and lives were torn apart by the intimate sharing of information" (MJ, female, 25)

> "Ahm, it's a disaster, I think, for the, for the actual people, cos like you, you do, I think, you know, people are a little bit less like guarded whenever it's not like a face to face interaction anyway. So, I think in terms of chatting on like message boards and things like that ahm, it also you know ah, if they're trying to meet someone new, might be trying to explore like a different part of their identity that isn't, isn't I mean, public knowledge maybe or something that like they're also trying to sort of figure out, and, and then in terms of, of erm intimacy and romance, it's something which is very private, so you know it's like an extra ah, problem…" (SG, male, 31)

The comments here suggest a different kind of vulnerability when information which I have termed intrinsic is revealed to a wider audience. They highlight how individuals broadly consider these 'private' messages to be just that, and so often individuals reveal information that they would not share with others more widely or offer up a side of their personality that they usually conceal. This highlights the need for a private space in which we can be ourselves, and the need to be able to control who knows certain things about us. As discussed previously, when information of this nature is shared without consent, it is more than inconvenient, it leads to feelings of vulnerability which cannot be put right in the same way that financial information (for example) potentially can be. It is not possible to re-issue an identity to someone, and the repercussions can be far-reaching, in a way that the spread of financial information may not be. As discussed above, Floridi (2005) recognises this to a certain extent, when he discusses the constitutive nature of information. This is why the hacking of intrinsic data (as in the dating website vignette) is deemed by the participants above to be so devastating – the

information being shared is part of our identity, and as such, cannot be changed or restored.

For Floridi, this means that we need to re-think the law around issues of privacy, he suggests that, '…in the precise sense in which an agent *is* her or his information…it expresses a sense of *constitutive* or *intimate belonging* not of external and detachable *ownership*, a sense in which my body, my feelings and my information are part of me, but are not my (legal) possessions' (2005 p.112). As such, he argues that maintaining privacy over our information is incredibly important as, 'The right to be let alone is also the right to be allowed to experiment with one's own life, to start again, without having records that mummify one's personal identity forever, taking away from the individual the power to mould it' (2005 p 112).

I argue that this is what my participants are expressing above, particularly SG, who suggests that in the context of a dating website's messaging facility, an individual may be attempting to explore a part of their identity that they have not considered before, and so to have this exposed to others, when it is not something that they are sure about, could be incredibly damaging for them. The importance of being able to experiment with new or different identities was also highlighted by boyd (2014), who spoke to teenagers about their use of social media and found that impression management was very important to them. Although, her concern was context collapse (as discussed above), this is in a sense what happens in situations such as when intrinsic information is released to a wider audience, therefore, this is indicative of the issues for individuals, when this type of information is shared without their knowledge or consent. It can affect the

impression that others have of them, which, depending on the information itself, can be damaging to them. This highlights the importance of intrinsic data to individuals in a way that has not necessarily been considered previously, suggesting that there are concerns around information other than our bank details. It is also important to note that although my participants were asked specifically about different situations in which different types of information were hacked and shared, those who spoke about the difference between issued information and intrinsic information did so spontaneously, before the vignette part of the interviews.

Financial information – a complicating factor

While the above quotes suggest that individuals are more concerned when considering their intrinsic information as opposed to their issued information, this was not the case for everyone. This unexpected complexity becomes much more apparent when we consider responses to various vignettes that interviewees were presented with. Some participants appear to be more attached to their bank details (or at the very least, they foresee greater repercussions to having their account hacked):

> "…the financial one cos I think that's the one that can do the most damage and is the one that can hold most people to account." (DC, male, 36)

> "Well at the end of the day it's, it's to do with what so banking details? [HEF: Yeah] Well yeah, anything to do with banking details is highly problematic…I think anything financial is, I don't know why just cos it's obviously, it underlines everything in life, financial means…"
>
> (TJ, female, 23)

> "Erm, probably anything to do with, anything to do with my bank details, to be honest, cos that's what everyone worries about…but someone like me or you or you know who, who works, and that bit of money is all we've got, that's, that's what makes you worry…So, no, my bank being hacked, just makes me like even sweat, thinking about it." (VR, female, 28)

Some also express concerns in terms of the issues this could cause in the future:

> "And they [companies] should do everything within their control to make sure that no one can be damaged by that because the damage that will be done is you know, you're, it's always gonna be financial, and you don't know what people are gonna be damaged by that and the people who are using that data don't really care. So…you could be hitting a student who's worked hard and trying to get everywhere, and suddenly they can't go and buy a house because their credit rating's shocking cos someone somewhere has run up a load of debt in their name, err or created a passport in their name!" (DC, male, 36)

These comments potentially undermine the dichotomy of intrinsic and issued information set out earlier in this chapter, as financial information does not conform to the issued group that it would logically be assigned to. According to the categories previously identified, issued information, does not make up part of our identity, and as such should not elicit a particularly strong response, however, this is not what can be observed from the above comments. When discussing this scenario, the participants discussed earlier in this section seemed unconcerned

about their financial information being hacked, believing that the bank would reimburse them for any losses incurred. The participants here, however, do not share this optimism, with concerns being raised around having no money in their bank account or worries about the potential long-term issues such as the ability to obtain credit and live the kind of life they wish to. In contrast to the previous participants, these individuals make no mention of believing that the bank will be able to restore their account balance and resolve any issues. Of particular note is VR, who discusses having a physical reaction to the mere suggestion of an issue with her financial information, suggesting that she does not simply consider this to be an issued piece of information that means nothing to her. For these participants there is not the same detachment as for others, and so they are not able to shrug off a situation such as the hacking of their financial information in the same way. Therefore, although an initial evaluation may suggest that financial data is issued and as such, does not constitute part of our identity, given the importance that money plays in the lives of many, it does still elicit an emotional response when considering what could happen if we were to suddenly find ourselves without it. In addition, I would raise the point that while I have highlighted the complications which arise in categorising information in terms of financial information, that is not to say that this is the only type of information for which this is true. It should be borne in mind that there may be other types of information that elicit ambivalent feelings in the way that financial information does and as such further exploration of this matter is required.

Further to this, I would add that it is important to remember that financial information contains more than the account number that we are issued with upon opening an account, which in and of itself has no meaning to us. It is therefore

the information behind this issued information that is of a greater concern for many. The trepidation that some have around financial information is around someone gaining access to their accounts (and thus their money), or potentially people finding out what their salary is and making judgements based upon that. Therefore, the account number is only a concern insofar as it is the key to other, more detailed information that could cause an issue for the individual concerned. As such, those who are not concerned regarding their financial information may have no need to worry in terms of recouping their losses and/or what people might think of them, while those that it would cause an issue for have a greater need to worry.

Financial information can be deeply personal and is linked to social class and status in society, issues which I will not deal with in detail here, but it is important to acknowledge. Further, this information can also highlight tensions regarding the social and the economic, which links to my previous discussions around the commodification of data (Fuchs, 2013). In particular, if we consider that differential pricing may be offered to individuals on the basis of information they share, then those who have a customer loyalty card (for example) are able to access discounts that those without one cannot. While 69% of my survey respondents stated that they accepted trading their data for personalised services[14], responses to the question of paying for privacy were more ambivalent. This suggests that it is possible that people accept this tradeoff in situations whereby they are financially unstable and so need the discounts available for sharing their data. This potentially means that they share their information because they have

[14] Although my survey did not specifically ask participants whether they accepted the tradeoff of data for the discounts offered by loyalty cards, this personalisation question offers a hint at the level of acceptance

to, not because they are comfortable with this tradeoff. This further hints at the potential for exploitation whereby those who are more financially precarious may be coerced into sharing information in order to make items more affordable through the loyalty discounts offered. This also feeds into the discussion regarding those who are willing to pay to protect their privacy and the potential implications for such a system whereby only those able to afford it could be granted the level of privacy they would like.

This concern around financial information suggests that not all types of information will fit neatly into one of the suggested information types (intrinsic and issued). This highlights the importance of viewing these information types as being ideal, flexible, and potentially open to interpretation. They are not necessarily mutually exclusive but offer a useful framework for considering the ways in which we can think about different types of information and what it means to us. It will be useful here to briefly consider the work of Stoilova et al. (2019a and 2019b), previously referenced in my literature review. In their work regarding children's conceptions of privacy, they set out not only three contexts for privacy ('interpersonal', 'institutional' and 'commercial', 2019a, p.7), but also highlight how different types of information ('data given', 'data traces' and 'inferred data', 2019a, p.7) are prioritised in each of the privacy contexts. This offers an alternative view of the categorisation of our information and thus may account for the complications I have described above regarding intrinsic and issued information. Unfortunately, Stoilova et al.'s work was released in 2019 and so it was not possible for their findings to be fully examined in relation to my findings, but it is worth bearing in mind the different ways in which various theorists have conceived of types of information.

It is also important to be aware of other factors that play a role when we think about different types of information and how concerned individuals would be about others knowing that information. This will be considered in further detail in the next section; however, it is worth mentioning here that there are a number of additional factors which could impact upon the level of concern an individual feels about their financial information being hacked. This includes the level of regular income that individual has (if any) as well as how easily they could ameliorate the impact of having their money stolen, for example would they have easy access to money in a separate savings account? Further to this, it may also depend on how trusting they are of financial institutions in terms of how readily they would be able to correct any issue in terms of a person's financial information being hacked. As such, a person who believed their bank to be very trustworthy and capable of dealing with issues, may again demonstrate this in terms of less concern regarding their financial information.

Finally, it may be that while these categorisations are a useful way of separating types of information into different groups, the level of concern felt by people does not necessarily correlate with these categories in the way I have suggested. The above comments suggest that the level of concern itself is linked to the potential repercussions that may be experienced and so the impact of the information being revealed to others may be more instructive of the level of concern. As such someone who is not exploring a different side of their identity may have little concern for their messages being revealed to others in the same way that someone who is financially secure would have less concern about their financial information being revealed. This, in turn may link to issues of identity and

whether a person believes they are portraying their 'true self' to others, or that they are hiding a facet of their personality which they do not want to reveal. As noted throughout this thesis, my work is exploratory in nature and as such, further exploration is required before complete conclusions can be drawn. However, it is clear that distinctions are being made by individuals when considering different types of information.

How does the availability heuristic affect the decision-making process?

While a number of my participants discuss the importance they place upon intrinsic information, when interviewees were asked to rank the vignettes in terms of which would cause the greatest concern, financial information ranks the highest. This complicates my suggested model, acting as a reminder that information privacy is not something that can be easily fitted into rigid categories. Given the contextual nature of information privacy, it is extremely difficult to locate a model that encompasses all types of information in all contexts, however, as discussed previously, the model I offer here is one way of considering our data and the different levels of importance that we assign to it.

One compelling alternative model which is relevant is that of the previously discussed 'availability heuristic'; (Tversky & Kahneman, 1982 p.20) which suggests that those who can more easily recall an incident are more likely to overestimate the likelihood of it occurring. They also know how it feels to experience this situation which can make the possibility of it occurring again feel much more likely, or at the very least make the person involved much more averse to experiencing it again.

It is important to note that those who have not had direct experience of an issue with their data, may still employ the 'availability heuristic' (Tversky & Kahneman, 1982 p.20) if they see a number of media reports regarding hacking incidents and individuals losing money as this will increase the 'imaginability' (Tversky & Kahneman, 1974 p.1127) of an incident occurring. As such individuals often rely on the availability heuristic when potential threats are more immediate and visible.

This is certainly the case with social privacy issues in general, therefore individuals concern themselves with protecting this type of information (regardless of whether it is issued or intrinsic). This may be, in part due to concerns regarding what the consequences will be (as with the above example of financial information), and how keenly they would be felt. This is a view shared by Raynes-Goldie, who suggests that 'social privacy challenges can have immediate social consequences' (2012 p.184), and this, 'tends to distract from the potential, intangible institutional privacy threats, such as data collection, aggregation and mining' (2012 p.184). This was recognised by one of my participants when discussing two of the vignettes in particular: one involving communication information being collected on a large scale by the government, and another (which he refers to as telecommunications) which involves the customer records of a telecommunications company (including banking details) being hacked:

> "you'd think the government one would be worse, it is in some senses, but the, the telecommunications has a more direct effect on people [HEF: yeah], it makes someone have to change their credit card information, their

> bank information, reset all their passwords, it's a massive fuss. Whereas the government snooping on what you do it will very likely have little direct effect on you" (GD, male, 25)

However, he was not the only participant to recognise that concerns tend to increase, the closer the threat is to you:

> "…I suppose if something bad did happen and like my identity was stolen, or something like, then I would think more about maybe how much information I put online, I mean I keep my Facebook profile, you know, on the high security settings" (CY, female, 24)

> "…I guess when a story comes out in the media, you think, it makes me think about it and I might check my privacy settings, and kind of check my friend list again, on Facebook. Erm, but yeah, it's not something I think about day to day." (ES, female, 36)

As with Raynes-Goldie's work, the focus of the concerns discussed by these participants is their social privacy, CY talks about the potential for identity theft, but concludes that she has her Facebook profile on the highest security settings, and this seems to reduce her concerns. Similarly, ES highlights how the media may play a role in terms of bringing attention to potential issues, suggesting that visibility has an impact. This offers a potential explanation for why people may express greater concerns regarding the hacking of their financial data, as it is often the focus of media reports. As discussed throughout this chapter when individuals are subject to availability bias (Tversky & Kahneman, 1982), they tend to overestimate the likelihood of an event occurring, due to how easily they are able

to recall or imagine an example of it. Therefore, if a person can think of recent media reports regarding bank accounts being hacked, or they know a number of people who this has happened to, they will perceive it to be far more likely than it may actually be in reality. This offers an explanation for why the far more immediate repercussions of issues with social privacy warrant greater concern than those of any issue with institutional privacy.

As highlighted by the above quote from GD, the collection of information by large institutions, is likely to have very little (if any) direct impact upon individuals. The data is simply collected in the background, as we carry out our day-to-day activities, it requires no additional effort from us, and so it is easy for us to forget that it is happening. This is contrasted with the immediately-felt effects of having our identity stolen, for example, as this would require a certain level of effort on our part to ensure that we are issued with new account numbers, and that those who had stolen our details are prevented from taking money from our account(s) and affecting our credit score and so on. The link between the immediacy of the threat and our level of concern may also explain why some express greater concern regarding financial information being hacked rather than intrinsic information. As one of my participants suggests when discussing the dating website vignette:

> "…but I honestly if I was involved in that [online dating], I would not be that worried because I'd assume there's such a flood of information here, is anyone really gonna actually see this that I wouldn't want to see this? I would kind of assume that that's probably not gonna happen…"
>
> (PF, male, 39)

There appears to be greater concern around financial information being revealed as it is potentially believed to cause a greater issue to individuals than information which is intrinsic in nature. As noted by PF, when a large volume of intrinsic data is hacked and released, the likelihood of being singled out is low, unless you stand out in some way from the others. Therefore the consequences associated with financial information being hacked feel much more real and threatening to my participants than the various types of intrinsic information which they do not believe is particularly remarkable or problematic. This was not discussed by my participants in great detail, and when the issue was discussed, the consensus is that they are not harbouring any kind of potentially damaging secret and so even if information were to be exposed, it would not constitute a problem for them. This belief that we are merely a 'face in the crowd' will be discussed at greater length in the next section.

What contextual concerns exist?

As demonstrated in the previous section, the level of concern that individuals feel regarding information sharing relies on a number of factors, which includes the type of information as well as the extent of the consequences of sharing that data.

One potentially complicating factor to recognise from the outset is suggested by Huberman, et al., (2005) who argue that whether an individual believes him or herself to be 'typical or positively atypical compared to the target group' (p.22) makes a difference to how comfortable they feel in revealing information. When they asked participants how much they would need to be paid in order for them to divulge different pieces of information within a group, they find that perception

has an impact. In terms of weight, if an individual feels themselves to be below average or around the average weight for the group, they require little payment, while those who feel that they weigh more or much more than the average require a much higher payment. This suggests that we are less concerned about our privacy when we believe that we are merely a 'face in the crowd', as was highlighted by some of my interview participants:

> "My feeling is, I'm not doing anything illegal so why would it bother me? There's nothing for them to find out about me [HEF: Mmhm]. But possibly if I was involved in something that was a bit more, even if it's not really illegal, perhaps something a bit more secretive, or, perhaps I'd be more worried about it, but at the moment I feel like, 'well, what are they going to find out?'. It's not very interesting [HEF laughs]. So, people can look." (TS, female, 37)
>
> "I'm not particularly concerned because I don't [pause] think people are looking, I'm not particularly interesting person to look at" (CY, female, 24)

The above quotes highlight how my participants believe that as the data they are discussing is not particularly interesting or suggestive of illegal or illicit activity, it is likely to garner very little interest, and so in some respects, they are not worried about who sees it. As with the research of Huberman, et al., (2005), they believe that their information is fairly typical and so would not stand out or call for attention from those collecting the information. There is a suggested mundanity to their information and as such, they cannot foresee a situation whereby sharing it would cause them an issue in any way. This links with

comments in the previous section whereby PF in particular felt that he would not need to worry even if his dating website information were to be hacked, because so many records would be released that it is unlikely that he would stand out. What participants are essentially saying here is that they do not believe that their information would have a particular value to others, and as such, they do not believe that sharing it would cause them any issues now, or in the future. The lack of concern here is likely to be related to the type of information being considered.

What is the impact of type of information?

Huberman, et al., (2005), suggest that there are some types of information that are deemed to be much more sensitive to individuals than their weight. When the researchers rank pieces of information by the proportion of respondents who require payment of over $100 to reveal it, they find that financial information is deemed to be of greatest concern. Often when research has been carried out in this area previously, the main area of concern is around financial information or information that could identify an individual, such as their name or address (Ackerman, et al., 1999 and Acquisti & Grossklags, 2005), this is also highlighted as a concern for my participants, when asked: *Are you concerned about sharing some types of information more than others?*

> "Erm, I mean, I'm concerned about [pauses], I mean in the sense, the obvious sense I guess of like I'd be more concerned about sharing my bank details than my erm, just pictures of a night out or something…"
>
> (AQ, male, 26)

> "I wouldn't like to share my address, necessarily…you know I wouldn't like other people to know particularly where I lived if it wasn't for you know receiving goods. Erm, same with phone number, I wouldn't want nuisance calls or anything…Yeah, I s'pose, yeah, yeah, the ones that you could physically be, someone could turn up at your house or something like that, I don't want that, or someone to speak to you personally, I s'pose, yeah." (CY, female, 24)

> "Yes, err and also, I'm not too worried about my address as much but yeah [HF: Mmhm] cr- anything related to credit card or anything basically that can lead to them other kind of fraud being, erm [HEF: Uh-huh] err committed with that information, yes, I, that's definitely something I, I would think more about than, yeah, than a picture" (JZ, female, 25)

This can also be noted when considering the free text responses to the survey question: *What information would you <u>never</u> share online?*

	Frequency	Percent
Address/location info/holiday dates	161	**28.90**
Financial info	84	**15.08**
Contact details (including phone number/e-mail address)	46	**8.26**
Family info (including photos)	41	**7.36**
Date of birth/ birthday	39	**7.00**
Personal details/issues	28	**5.03**
Miscellaneous	25	**4.49**
Info relating to intimate relationships/feelings/sexuality	21	**3.77**
Employment details (place/name of employer)	20	**3.59**
Passwords/PINS/login details/answers to security questions	20	**3.59**
National Insurance/government issued ID	14	**2.51**
Photos (Inc. nudes, at parties, personal)	12	**2.15**
Health/medical info	10	**1.80**
Full name/signature	9	**1.62**
Car details (including number plate/driver's license details)	8	**1.44**
Information about others (friends/colleagues etc.)	8	**1.44**
Political/religious views	6	**1.08**
Citizenship data/passport	5	**0.90**
Total responses [15]	557	**100.00**

[15] Please note, the total here is high as many responses contained items which were applicable to multiple categories.

It is clear to see that address or financial information is of the most concern to individuals, who are potentially concerned about identity theft or being burgled while on holiday, and the issues this would cause them. However, if we consider the responses to the subsequent question: *Why would you not share the above information?* a different picture emerges:[16]

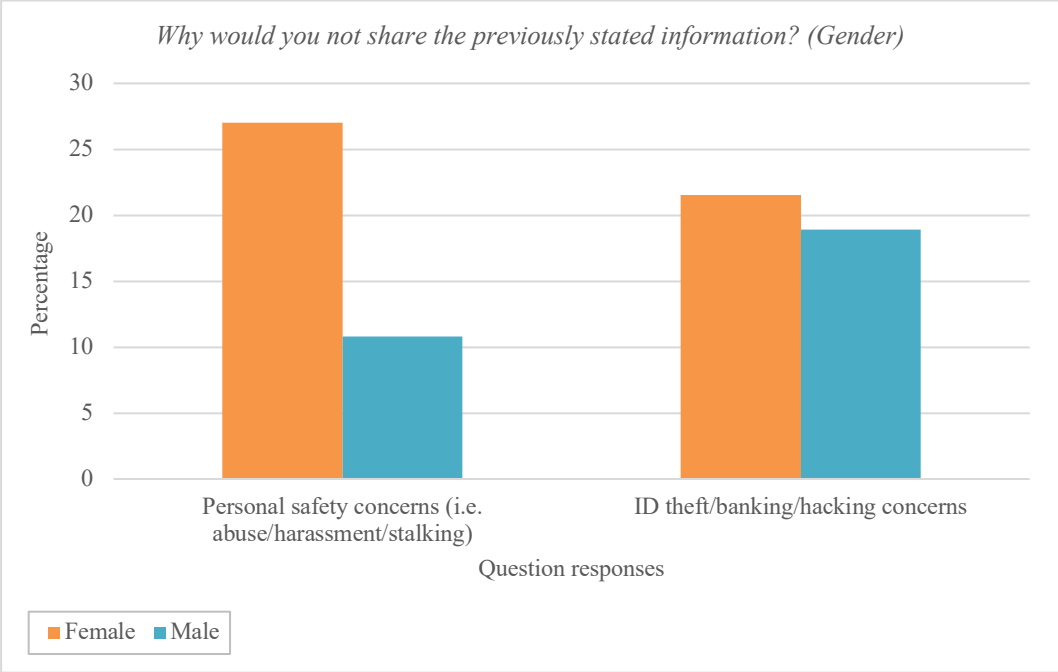
	Frequency	**Percent**
Personal safety concerns (i.e. abuse/harassment /stalking)	84	**23.86**
ID theft/banking/hacking concerns	79	**22.44**
Info is private/personal	76	**21.59**
Concerns re: potential repercussions	27	**7.67**
Physical security concerns (burglaries etc.)	26	**7.39**
Concerns re: protecting others (Not my info to share)	23	**6.53**
Miscellaneous	18	**5.11**
Concerns re: spam/info being sold/shared with unknown others	16	**4.55**
Info is stored forever	3	**0.85**
Total[17]	352	**100.00**

Therefore, it is not simply a case of people being concerned about identity theft, as the highest concern is actually around issues of personal safety, rather than identity theft, this could also hint at concerns regarding the consequences of issues

[16] The table shows the categories that free-text responses were assigned to.
[17] Please note, the total includes responses that contained items which were applicable to multiple categories.

occurring. As noted in the previous section, many of my participants believe that issues around identity theft can be remedied, in that bank account details can be changed and re-issued, however, if an individual is a victim of harassment or stalking, the consequences of this will be felt much more keenly and cannot be remedied in the same way that other information can. Again, as examined in the previous section, this may be indicative of media reporting around the issue of harassment and stalking, suggesting that this is particularly prevalent, and something that people 'should' be concerned about. It may offer another example of availability bias (Tversky & Kahneman, 1982), in that we may know of others who have suffered this, or remember media stories, which highlight this as a potential threat to us.

If we focus on the two biggest concerns overall, 'Personal safety' and 'Identity theft' and factor in gender, it is clear to see a difference in concerns:



(r-square: 0.053, p-value: 0.00)

Concerns around personal safety are driven by women, which suggests that there may be a gendered dimension to concerns regarding what information individuals are willing to share online. Quotes such as those below are typical of the free-text responses from female survey participants:

> "I am always very conscious of who knows where I am, just in case anything were to happen such as being stalked or anything worse, especially as a woman." (female, 20-25)

> "Concerned about possibility for physical stalking" (female, 20-24)

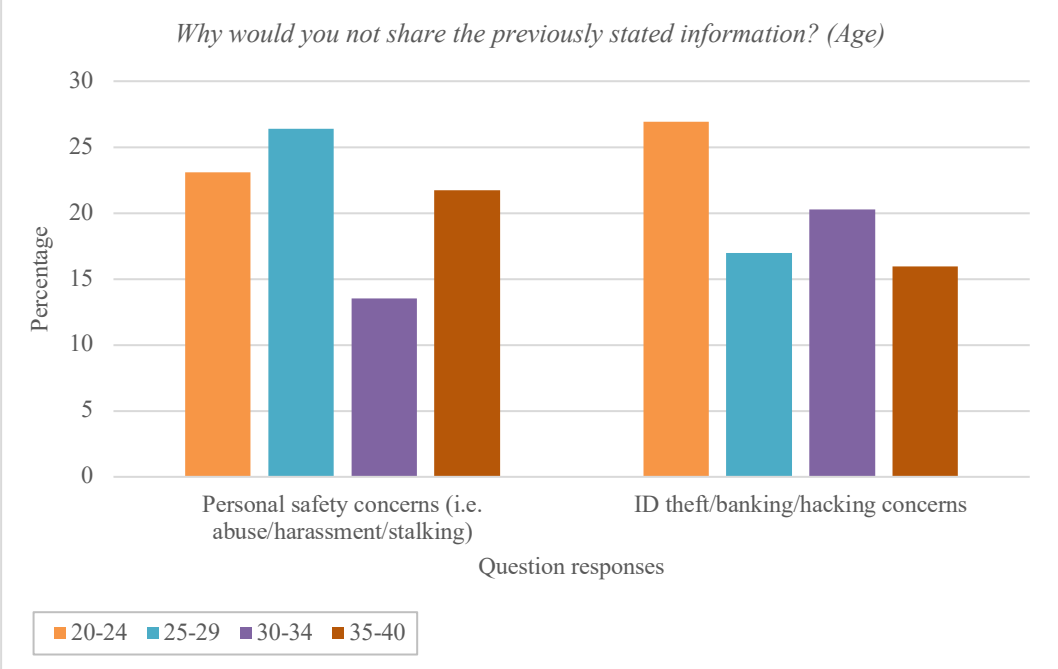
> "Fear of being stalked" (female, 25-29)

These sorts of comments occurred far less often for men, who appear to have more diverse concerns; when categorising all responses given for this question, those given by men are spread across all of the categories. Women's responses, however, are concentrated on the above categories, suggesting that women's concerns may be more specific than men's in terms of information sharing.

This difference in concerns between men and women has been found in previous research, with Thelwall (2011) suggesting that women are concerned about their physical security to a greater extent than men. He suggests that media scares 'may create an atmosphere in which women may worry about the potential for strangers to contact or physically locate them' (2011 p.253). He argues that women are more concerned about their personal safety in an online context particularly in terms of being harassed offline, due to information they have

posted online. As such, strangers will represent risk and danger to women in particular. This is perhaps unsurprising given that statistics suggest that women are five times as likely as men to have been sexually assaulted (Office for National Statistics, 2018) and given that concerns around crime tend to be gendered (Ferrarro, 1995). The most recent statistics from the Crime Survey for England and Wales (Office for National Statistics, 2018) show that over a period of twelve years (2006-2018) women aged 16-59 have been the victim of stalking to a greater extent than men, with the most recent figures (2018) showing this percentage for women to be more than double that of men (women 5.4%, men 2.6%). It is important to note, however that the prevalence of stalking is relatively low, and it is possible that concerns regarding stalking far outweigh the actual incidence of it. This is not the only area in which this occurs, and Dedkova (2015) suggests that this situation can be problematic in her observation of the discrepancies between high levels of concern regarding children being groomed online by strangers and the low levels of occurrence. She suggests that this could be due to media coverage, which presents the issue as much more prevalent than it is, leading people to have a disproportionate perception of its likelihood. This is particularly problematic as it can lead to policy and resources being focused on a relatively low-level threat, while a higher-level threat is ignored. In terms of the concern highlighted here regarding the potential for being stalked, this could lead to women focusing on the threat of being stalked by a stranger who discovers details about them online, rather than the potential for intimate partner violence, which may be much more common. Again, this links to the 'availability heuristic' (Tversky & Kahneman, 1982 p.20) in that if the media is reporting on cases of stalking and so on, it is likely to be at the forefront of women's minds when considering their concerns regarding sharing information online.

Another interesting point to note regarding this question is that the concerns regarding these categories was higher amongst the younger participants, as per the below graph:



(r-square: 0.005, p-value: 0.261)

It is particularly striking to note that for each category, those in their twenties appear to be more concerned about these issues than those in their thirties. There are a number of possible explanations available for this, in particular, the concerns around identity theft may be due to the more precarious financial situation that those in their twenties currently find themselves in. As per the discussion in the previous chapter, in general, millennials are worse-off financially than previous generations (O'Connor, 2018), and this may affect concerns regarding the impact of identity theft.

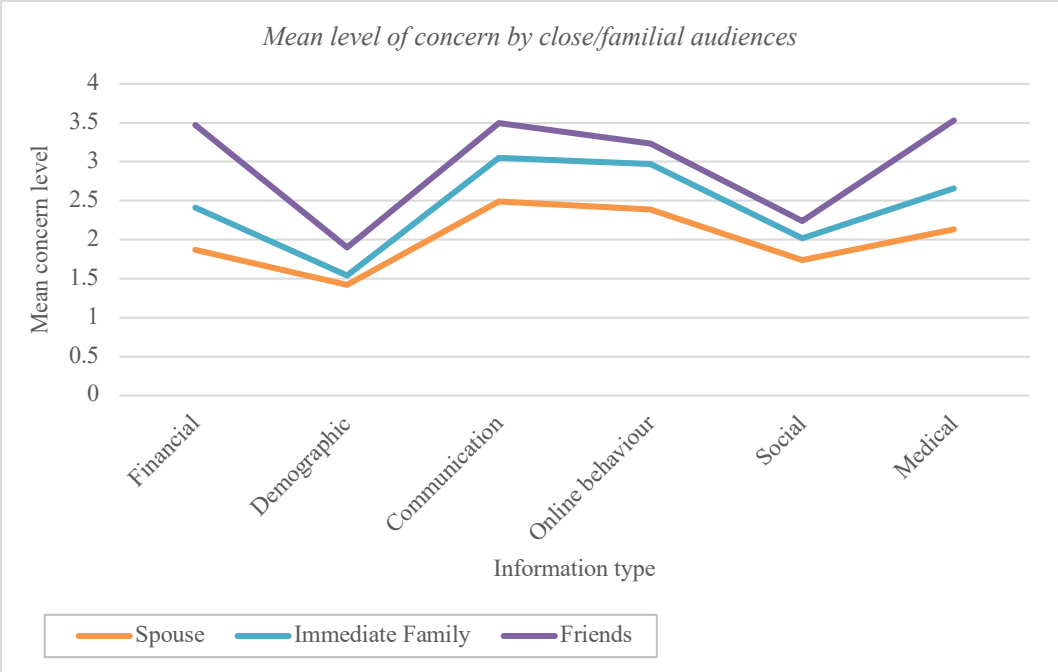
Information and audience combinations

The above discussion highlights how concerns around privacy can depend very much on the type of information being requested. However, this is only part of the issue, we will now examine concerns around data-sharing in terms of who it is being shared with. This issue has been studied previously, in particular Olson, et al. (2004) carried out research which asks participants to rank how comfortable they are in terms of sharing various pieces of information with different types of audiences. They find that participants did not want to share most items with the public, but neither did they want to share everything with their spouse. They found broad areas of agreement, but also areas where participants shared little common ground, particularly in terms of sharing personal statistics with co-workers.

My research was similar in that participants were given a piece of information to consider and asked to rank how concerned they would be for various audiences to have access to that information. They were asked to rank each audience from 1 (not at all concerned) to 5 (extremely concerned). The audiences range from those who would be expected to raise few concerns (the participant's spouse, immediate family or friends), those who would generally be deemed acquaintances (neighbours and work colleagues/employer) to those who would be expected to cause a greater level of concern (stranger, third-parties or the government/police). I will deal with each of these audience categories in turn.

Close/familial category

Audiences in this group (spouse, immediate family or friends) cause varying levels of concern for participants, with spouse consistently having the lowest level of concern, regardless of the type of information. The graph below offers a comparison between the three audiences:

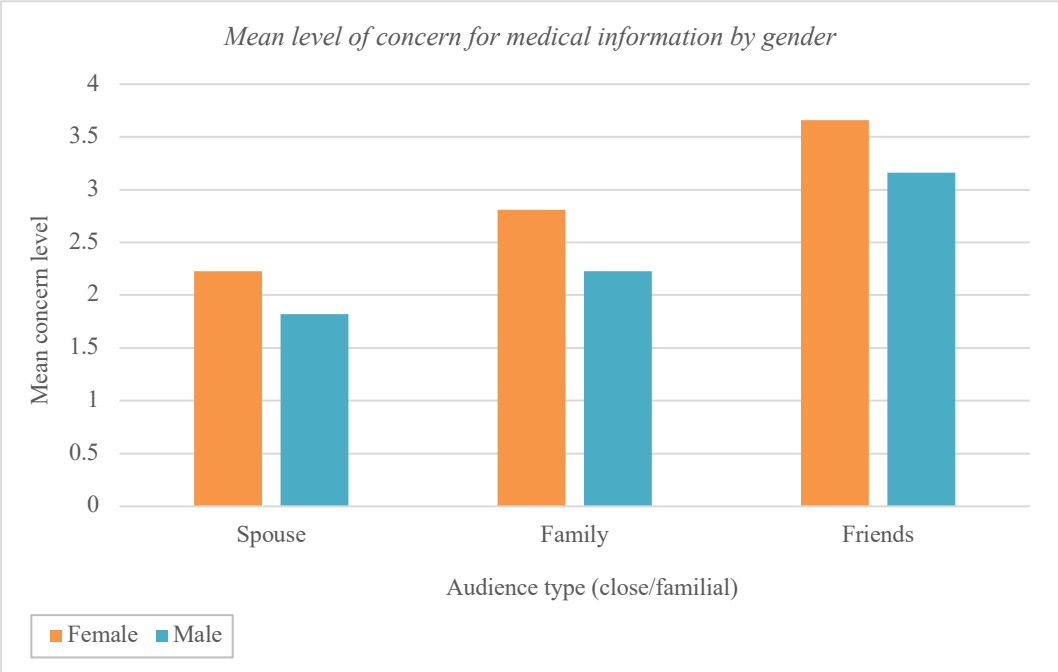


(Paired samples tests p-values range: 0.00-0.002)

It is perhaps not surprising that although the levels of concern themselves are different, the pattern that they follow for these audiences is very similar, suggesting wide agreement amongst participants. This suggests that Nissenbaum's theory of 'contextual integrity' (2010 p.2) could be representative of how we live our daily lives, given the broad agreement for these types of information and audiences. It suggests that there is some common context in which we exist, which means that we have greater concern when considering sharing our financial information with our friends than with our spouse (for example).

However, that is not to say that there was no variation within this group of audiences, and it should be noted that this is one of only two groupings where men had a higher average concern than women for some information/audience combinations. In fact, men are more concerned than women about their spouse and immediate family having access to their financial, demographic and online behaviour information, as well as being more concerned about their social behaviour information being known by their spouse. Although women were more concerned than men for a greater number of audience/information combinations, it is striking that it is the above combinations which elicit greater concern from men than women. It is also worthwhile to consider that the instances where men are more concerned is around sharing information with their spouse, or immediate family, this is not the case when friends are the audience. It is difficult to know why this might be the case, without drawing unsubstantiated generalisations and is something that would be worth investigating further in the future.

When considering these audiences, it is particularly noteworthy that concerns around medical information show the largest difference between women and men (with women being much more concerned):

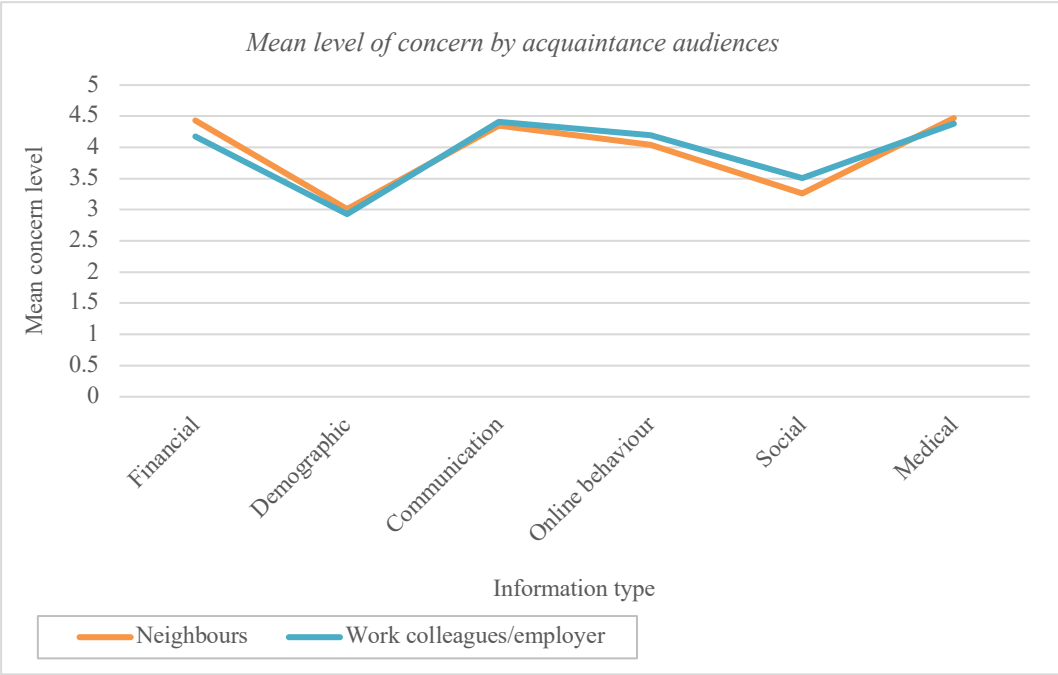


(p-values: Spouse: 0.038, Family: 0.006, Friends: 0.013)

This could be due to women (aged 16-60) attending the doctors more regularly than men (Wang et al., 2013), and therefore having more of a medical history and thus more information to consider. As such, if men visit the doctors less than women, there is less information and so less to worry about, which could explain the lower concern level expressed here. The study carried out by Wang et al. (2013) finds that the difference in incidences of visiting the doctor between women and men is partly due to reproductive issues and again, this could offer an explanation for women's concern over their medical information, as contraception (for example) can be a contentious and deeply personal issue. As such, it is perhaps not surprising to find that women are less concerned with their spouse knowing this information (especially as it is likely to involve them), but more concerned about their family having access to this information.

Acquaintance category

This category encompasses audiences which individuals generally would not know very well (if at all) and consists of their neighbours and work colleagues/employer. Within this category there is greater concern than for the previous one, which is to be expected, as these audiences tend not to have intimate knowledge of an individual. The closeness of the lines on the graph below highlight how difficult it is to separate concerns regarding these two audiences:



(Paired samples tests p-values range: 0.00-0.222)

This graph suggests that there has been wide agreement amongst participants, but it is interesting to note that the audience causing the greatest concern is not consistent, so for financial, demographic and medical information, neighbours would be of the greatest concern, while for communication, online behaviour and social information, it is an individual's employer (or work colleague) who causes the greatest concern. This could simply be because people recognise that their behaviour in these categories, may be deemed unprofessional (as discussed by my

interviewees previously), and so this is why they would be a little more concerned if this were to become known in the work context. Again, this hints at the potential issue of 'context collapse' (Vitak, 2012 p.451), as discussed at the beginning of this chapter, whereby it could cause an individual an issue in terms of their personal or social life context becoming merged into their professional life context. Where the employer has received a lower concern score, such as with medical information, this could be due to these participants having no medical issues that they would worry about their employer knowing. Therefore, if they had a medical issue that they would not be comfortable for their employer to know, they may have a higher concern level around this combination of information and audience. This is highlighted by one of my interview participants:

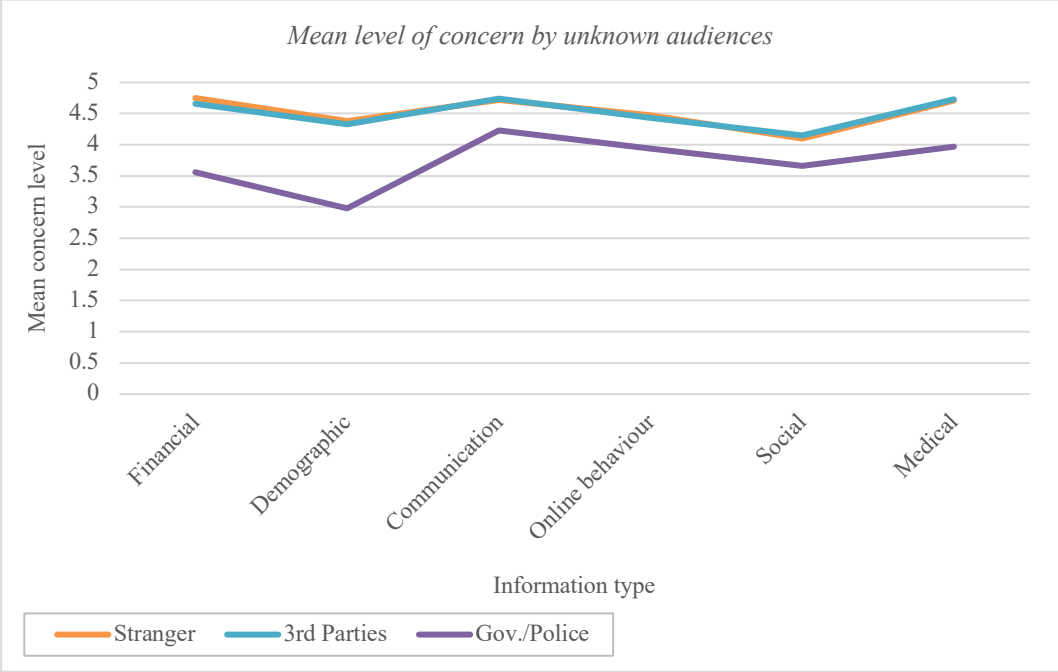
> "I'm very aware of sharing erm, my health issues…Erm, so it's something that I haven't actually disclosed at work, erm only to certain people…So, in terms of the health status that's quite, yeah. Because again, this is about potential employers, you know, if they figure out that I'm, I'm a person with a lot of health issues, then how likely are they going to employ me, so that's, that side of it, the health aspect is more, I think that's the most important one." (TP, female, 40)

This participant conveys her concern around her employer (in particular any future employer) learning of the health issues she has, and potentially not employing her because of it, therefore she would be more likely to have a higher level of concern around sharing her medical information with her employer than someone who has no medical issues.

When considering gender, there is little variation for these information/audience combinations, and it is also important to note that for **all** combinations in this category, women express higher levels of concern than men. It is unclear why this would be, it is possible that in a work context, women may feel that they have to work especially hard to be seen professionally and so would be concerned if their social or communication information became more widely known amongst those that they work with. This concern has a basis in previously carried out research by Gorman and Kmec (2007), who find that women are subject to 'stricter performance standards' (p.828) than men, 'even when women and men hold the same jobs' (p.828). Although this research was carried out some time ago, if this is still the case, it provides a potential explanation for why women feel especially concerned when considering their social or communication information being accessed by those they work with or their employer. If women are held to higher standards, it means that seemingly innocuous social media posts could cause them greater damage professionally than men posting similar updates, and if this were the case it would make sense for them to be more concerned about such information being seen by an employer. However, it is important to note that this view is not expressed by my participants. Another potential reason for this is the nature of the information posted online by women and men. Thelwall (2011) suggests that despite being more concerned about online privacy, women still tend to share a greater level of personal information than men, therefore the concern level here could be due to women sharing more information. As with the discussion around medical information above, if men are sharing less information online, they have less information to be concerned about, regardless of who will see it.

Unknowns category

This final category contains three audiences, which are likely to be unknown to the individual concerned, and so would potentially be the most problematic. The audiences are: a stranger, any third-party that the individual has not chosen to share data with and the government/police.



(Paired samples tests p-values range: 0.00-0.503)

This chart shows a little more variation than for other audience categories which is interesting, given that it is around audiences who are unknown to the individual concerned. While the level of concern for both stranger and third-parties is virtually the same across all categories, there is less concern around the same information when considering the government/police. There are a number of potential explanations for this. In the case of information such as demographic or medical, there may be an expectation that the government has access to it anyway

through the National Health Service and census (for example), and so there is little need to be concerned.

> "…Err, then, then I'm probably going down to the government one, err as, as the fourth one, so, going, you know, err, I would, kind of expect the government the government is going to do that [collecting information]."
>
> (PW, male, 37)

> "… the government, cos government do it anyway [collect information], so, there's no point worrying about it." (VR, female, 28)

Although the above quotes do not mention specific types of information, they demonstrate the expectation (shared by a number of my participants) that the government is collecting our information and there is little to be gained from worrying about it. This offers a potential explanation for the lower levels of concern regarding government collection of information expressed in my survey. This may also hint at a level of cynicism in terms of the expectation that the government collects information about everyone, and so could lead to some resignation in terms of the collection occurring whether we agree to it or not. There is also the perception that there is something suspicious about those who are unwilling to share their information with the government, as expressed by this interviewee:

> "Yeah…if you…do everything you're meant to do and you tell them all the information, you've got nothing to worry about, you know, again, it goes like with the website, where people, with their data being exploited, if you're doing something that you shouldn't be doing, then yeah you are gonna have a concern, because you're trying to get away with something, that you shouldn't be doing in the first place." (CB, male, 37)

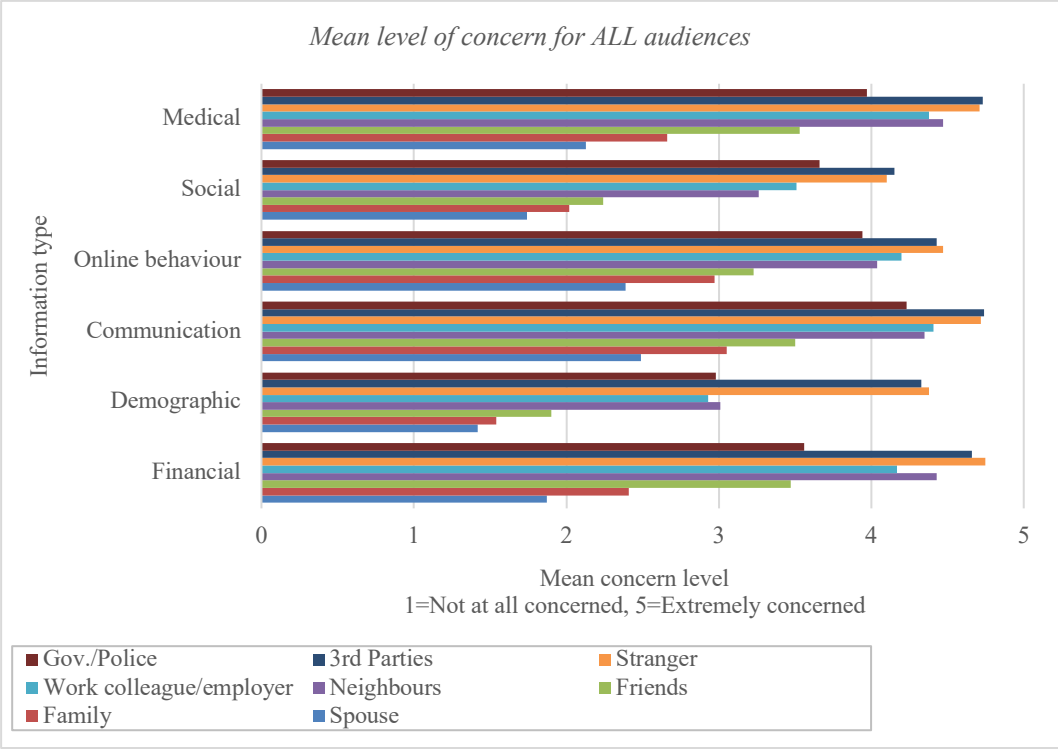
This participant believes that it is only those people who are attempting to behave in an immoral or illegal way who would be concerned about the government/police having access to various pieces of information. The presumption here is that an individual does not need to worry about the collection of their data, as long as they are behaving in a legal or moral way. This participant had little concern around government/police collection of data as he believes that they have nothing to hide and so concern is unnecessary. This may also be the reason that survey participants appear less concerned about the government/police than other audiences in this category having access to their information.

While it has been informative to separate the audience groups into different categories to examine them in detail, further patterns emerge when we consider all of the information/audience combinations together. This allows us to make comparisons between different types of audience, in a way that was not possible when different types of information are dealt with separately.

All categories

This section will examine the patterns that emerge when all information/audience combinations are considered in tandem, as this offers a way of gaining an overall picture of where concerns lie for my participants. As noted previously, there are a number of similarities in terms of the level of concern expressed by participants, and this supports Nissenbaum's (2010) claims regarding the importance of 'context-relative informational norms' (p.129). This offers an explanation for the broad agreement demonstrated, particularly as her approach recognises the importance of the relationship between those involved in a particular situation. This tends to be the person sharing the information and who they are sharing it with. Therefore, her suggestion of appropriate flows of information is applicable here, as it suggests that as long as information flows in the expected manner, there should not be an issue. The previous graphs suggest that there is broad agreement amongst my participants in terms of what appropriate flows of information look like, as represented by the level of concern. I argue that in situations where the level of concern is high, this is where the flow of information is deemed to be inappropriate by individuals, with the opposite being true where the level of concern is lower. Therefore, higher levels of concern, can be seen as an indication that the information flow is deviating from the accepted norms, which causes higher levels of concern. Given that my research is exploring the intersection of information and audience type as it relates to individuals' concerns, it is difficult to say whether one of these items is driving the level of concern more than the other, or whether it is the combination itself.

The below graph shows the mean levels of concern for each information/audience combination:



(Paired samples tests p-values range: 0.00-0.579)

It is clear from this graph that different information/audience combinations evoke different levels of concern from individuals, suggesting that there are a range of attitudes towards privacy and who should or should not have access to specific information. There are, however, clear patterns, in terms of different types of information, for example, demographic information is of a lower concern than financial information regardless of the audience.

What is particularly striking, is that while most audiences follow a similar pattern in terms of concern level across the different types of information, the government/police audience does not. In fact, despite this audience-type being categorised as 'unknowns' (as we are unlikely to personally know those in this group), it is of less concern for most types of information than the audiences that I have categorised as 'acquaintances'. This is surprising as the two other audience-

types from the 'unknowns' group (stranger and third-parties) score very similarly and are of the greatest concern for all types of information. This is potentially due to the nature of third-parties and strangers; they are unknown to us, and so we cannot know what they are likely to do with any information that they obtain about us, this is generally a cause for concern. However, despite the government/police also being unknown to us, it could be that there is a belief (as discussed previously), that we need only be concerned about this collection if we are involved in some type of illegal or illicit behaviour[18]. As illustrated by the below quotes there is a belief that the government/police are collecting information for our own good (to combat crime or terrorism). This view is shared by several participants:

> "We, I always have this argument if you've got nothing to hide, then you don't have anything to worry about…I think it's the same scenario, if you're not doing things you shouldn't be doing, then you shouldn't have to worry about it. I want, I'd rather be safe [HE: Mmhm] than dead"
>
> (AL, female, 36)

> "I'm not particularly concerned because I don't [pause] think people are looking, I'm not particularly interesting person to look at like maybe if I was on some sort of watch-list maybe, but I don't think I'm particularly interesting to look at. So, I'm not particularly worried, well I'm not searching for anything I would be worried that if anyone saw…"
>
> (CY, female, 24)

[18] It is also important to note that while the level of concern regarding the government/police audience is lower than other audiences in the 'unknowns' category, it is still of high concern as the concern level only falls below 3 for demographic information, for all other types of information, it remains above 3.5.

> "Again, the flipside of that is that actually protecting things like national security's quite key, and unfortunately there are people that will use messaging and things like that, that obviously put other people at risk. And we need to use all the tools that we've got at our disposal as a society, I think to, to try and combat that the best way we can."
>
> (MB, male, 37)

This suggests that despite the government or police being unknown to individuals, there is a level of trust, which would not be possible with the other audiences in the 'unknowns' category. Trust is facilitated when we trust the information we are provided with by others (often experts), in that we accept that they know more than we do in a given situation and so we trust the information that they supply us with (O'Neill, 2002). In this case, these participants believe the information that the government shares regarding the necessity of collecting information in order to keep citizens safe. It is impossible for checks to be made into the claims of the government, but these participants are expressing their trust in the information provided, and as such have fewer concerns regarding this collection.

However, this may also hint at the cynicism discussed earlier in this chapter; potentially individuals feel that there is little they can do in terms of choosing whether to share information with the government/police, and so there is little point in being concerned about it. This is highlighted in work from Twenge (2014), who suggests that since generation X (which the older participants would be categorised as), people believe that collective action does not have an impact on the world around them. Therefore, if this is a belief shared by my participants,

they may believe that there is little point objecting to the government or police collection of information. For strangers and third-parties on the other hand, we are able to take steps to ameliorate this, if we choose to. As such, we can avoid sharing information with third-parties, in terms of refusing to share information or providing false information (as several my participants admitted to doing in the previous chapter). Therefore, concern here could be around whether participants feel they are doing enough, or whether they know enough to be able to avoid sharing this data, as examined in Chapter Three.

While the high level of concern around the third-party audience suggests that people are concerned about their institutional privacy and what happens to their information when it is passed on, I would suggest that concerns expressed here are more around issues such as spam and junk emails. This is the main concern when this audience was discussed with my interviewees and offers a potential explanation regarding why the government/police is of lesser (although still significant) concern to individuals than other unknown audiences. We experience very few consequences from the government/police collecting our information when compared to the potential consequences from third-parties and strangers, this can make government/police information collection seem less harmful to individuals in comparison (as suggested previously by GD). Government collection of information has no noticeable impact on our day to day lives in the same way as the other data collection. In fact, only one interviewee spontaneously mentioned data aggregation or other aspects which could be considered to be institutional in nature. This suggests that this is not an issue that immediately comes to mind for many individuals, and therefore is unlikely to be

what my survey participants are thinking about (however, it is important to note that I cannot say this with complete certainty).

It is perhaps surprising to find that concerns here centre around seemingly inconsequential items such as spam and junk mail, which many would deem to be harmless, if a little annoying. However, my participants spoke of this with annoyance, potentially because it is something that occurs quite often and so, employing the 'availability heuristic' (Tversky & Kahneman, 1982 p.20) is something that comes to mind quite easily for them, when they are considering this issue. While receiving junk mail is not an occurrence that causes harm to the recipient (above a general feeling of annoyance), it is something that offers a visible reminder of how little control an individual really has over their information once they have shared it with an organisation. Receiving spam messages is a reminder that whether they have agreed to it or not, their information has been shared with a third-party, which serves as a reminder that there is little they can do to stop this from happening. This may suggest to the person that despite their best efforts, they have not been successful in maintaining the boundaries that they would like.

One final point, which becomes more apparent when all of the information/audience combinations are viewed together, is the lack of variation in concern levels between the different types of information for the stranger and third-party audiences. It is clear from the graph that there is very little diversity between the mean concern levels reported for these audiences, whereas for all other audiences, the difference between the highest and lowest concern levels is at least 1 point, and in some cases, it is much higher than that. This suggests that

there are real differences between how concerned individuals are about different types of information being accessed by different types of audience when they personally know the audience involved. However, when they do not know the audience at all, there is much less variation in terms of concern level, it is almost as if all types of information become equally concerning when we cannot see or know who has access to our data.

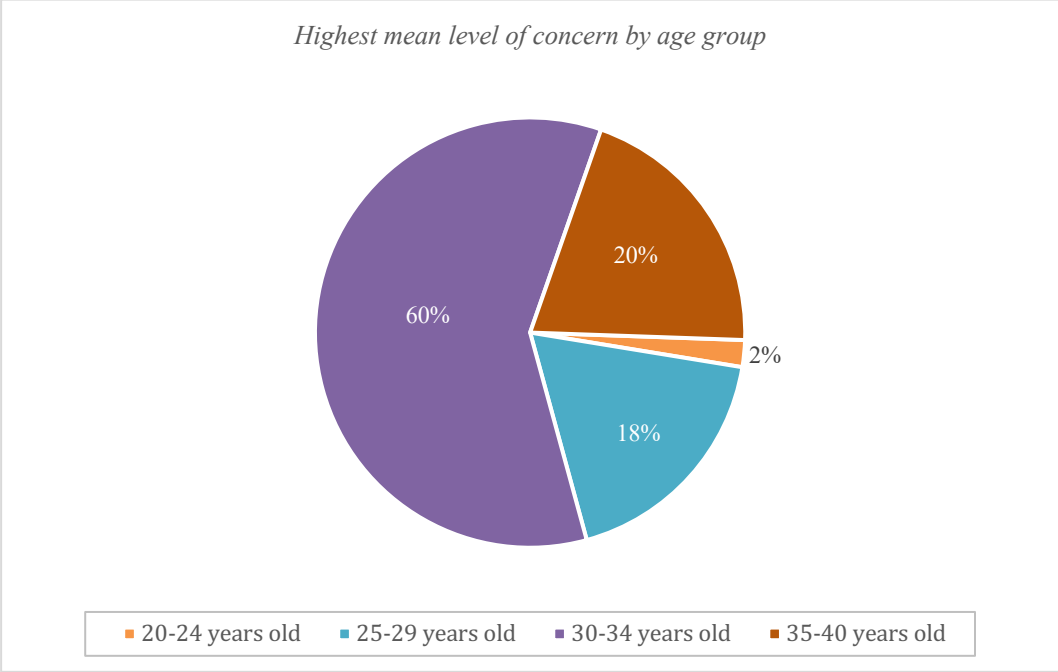
As a final point, on this subject, it is worth noting that the overall context plays a role here, therefore, given that my participants are likely to be UK-based, and have self-selected to take part in a survey about privacy, it is possible that these responses highlight the self-selection bias discussed in my methods chapter, and therefore a more representative sample may have lower levels of concern, given that they would not necessarily have a pre-existing interest in privacy. It is also possible that had the focus of my survey not been commercial surveillance, and/or the types of information had been different, again this would have elicited different levels of concern.

While it is useful to gain an overall picture of where concerns lie for my participants, it is often unsurprising, however, when we examine the results in terms of demographic groups, there are some important counter-intuitive findings. Therefore, we will now turn to the different concerns of the various age groups that took part in my research.

Age-group differences

As discussed previously, when discussing concerns around privacy, there is generally a belief that younger individuals are less concerned about their privacy than older individuals (boyd, 2014). While my research is only concerned with a specific age range (those aged 20-40 years old), there are still a number of interesting insights to be gained here.

The age group that appears to be the most concerned are those aged 30-34 years old. This group expresses the highest level of concern for 59% of information/audience combinations, while those in the oldest age group (those aged 35-40 years old) account for the greatest mean level of concern for only 20% of the information/audience combinations. [19]



[19] In total, there were 49 information/audience combinations, therefore when discussing levels of concern in this section, I am talking about the proportion of these 49 combinations for which each age group had the highest mean.

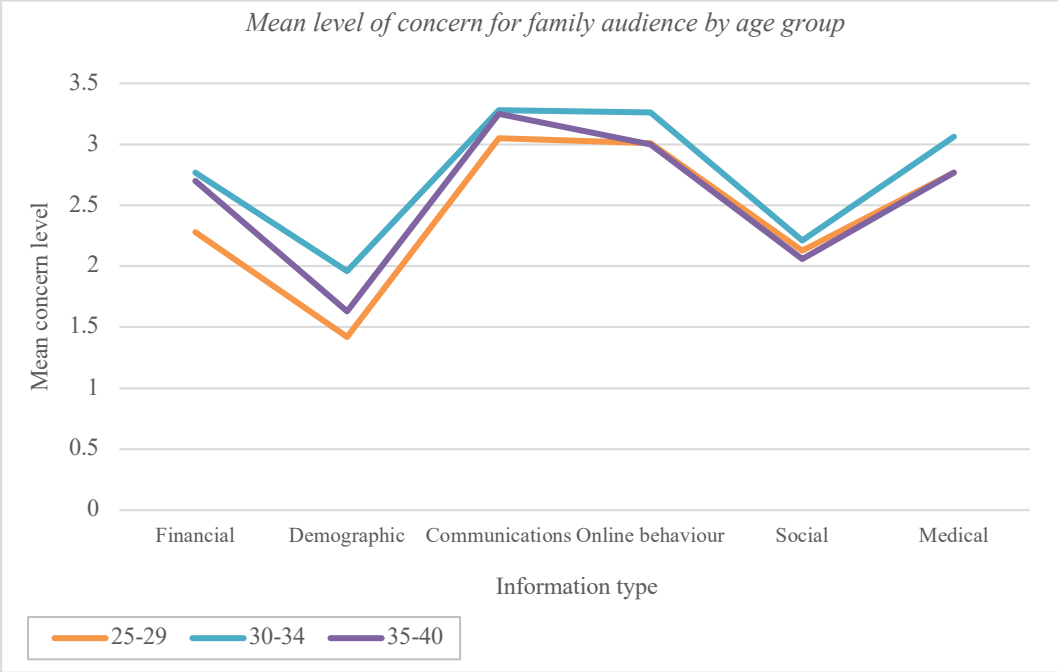
While it is true to say that those in their thirties have the highest mean level of concern, for the majority of combinations (80%), those in their twenties still expressed the highest level of concern for 20% of the information/audience combinations, suggesting that there are specific areas which are problematic for them. It is also interesting to note that of those in their twenties expressing concern, those aged 25-29 express the highest level of concern for 18% of the information/audience combinations, suggesting that this group is especially worried.

The above figures suggest that there is not a straightforward divide between those who grew up with the internet (those in their twenties) and those who did not (those in their thirties), as was my expectation at the outset. We can learn more if we examine where concerns lie in greater detail, focusing on which information/audience combinations cause the greatest concerns for each age group. As the youngest age group (those aged 20-24) expressed the highest concern level for only one information/audience combination (2%), they will not be included in the subsequent discussion.

As noted above, the age group expressing the highest average concern for the largest proportion of information/audience combinations, is those aged 30-34 years old. This group has the highest mean level of concern for at least one type of audience for each type of information. The focus of their concerns seems to be around demographic information, for which they have the highest mean level of concern for **all** audiences. However, they are also concerned about their online behaviour information as well as their communications data, which cause concerns for six and five audience types respectively (out of a total of six

audience types). One of the reasons for this level of concern could be that as individuals start families of their own, and feel more responsible, they could feel that they have more to lose, should something untoward occur. Individuals have a more permanent, long-term job, and so they are no longer working in precarious part-time work (Arnett, 2015), which on the surface appears to offer greater stability to an individual, however, it could cause increased levels of anxiety in terms of the level of responsibility which is now on their shoulders. Therefore, it may have the opposite effect, and induce greater levels of anxiety due to the stakes being higher, and there being so much more to lose should the worst happen.

When considering the various age groups, those aged 30-34 are consistently the most concerned about their family having access to various pieces of information about them, as demonstrated on the below graph:



(Paired samples tests p-values range: 0.001-0.226)

This demonstrates that there are particular types of information that concern those aged 30-34 more than other age groups when accessed by their family, in particular, demographic, online behaviour and medical information. This concern around family was highlighted by my interviewees:

> "there's more people that could hurt you in, in, in like your circle if you will, rather than the wider circle that you've chosen to be part of anyway." (TM, female, 25)

> "But of course, you know, for other family members, they have, they have other friends and they have other friends, and it's and it's then allowing your circle to become wider, which actually isn't even really your choice, and I think that's quite tricky." (SM, female, 36)

This suggests an awareness that despite concerns which are often raised regarding those that we do not know having information about us, people in our lives could also cause us harm if they know certain things about us. The second quote also highlights how there is the potential for unintended issues to occur due to the wider circle of acquaintances or friends that family members have. This was also borne out in my interviews when discussing the dating website vignette, whereby a number of participants spoke about how they would be much more concerned if information from that site became known by those they know, rather than someone they do not know. This age group (30-34) could therefore be particularly concerned in part because they are likely to be in a long-term relationship, with a child (or children) and as with SM's comment above, may be concerned that their relatives may inadvertently reveal information to a wider

audience. This is not necessarily carried out with any malice, but potentially because the relative is unaware of how far they are sharing information or the level of sharing that their relative is comfortable with.

Potentially the reason that those in their early thirties are the most concerned is because they are only just beginning to become established as a parent, partner or in their career while those who are older may be less concerned because they are more established in these areas and so have a safety net in place. On the other hand, those in their late twenties may still be in more casual relationships, working in part-time, or zero-hours roles and so have yet to begin to become established as those in their early thirties are. Those in their twenties have been termed to be in a specific phase of development, known as 'emerging adulthood' (Arnett, 2015 p.2). As such these individuals are seen as being on the cusp of adulthood, when life becomes more serious, as the 30-34-year-olds in my survey are discovering.

The 30-34 age group is particularly interesting because when we consider which audiences cause them the most concern, it is somewhat counter-intuitive when compared to overall concerns. As discussed above, the family audience causes the most concern for this age group, (in comparison to other age groups) for every type of information, however, the friends and government/police audience groups are of a concern for five out of six information-types. This is specific to this group, because when considering those aged 35-40 years old, the audience that is the most concerning for them is strangers (for three types of information) and for those aged 25-29 years old, it is evenly distributed between neighbours, strangers and work colleagues/employers (with each of these audiences being of particular

concern for two types of information). Therefore, those aged 30-34 years old appear to be more concerned about those in their lives having access to information about them than those unknown to them. There is the potential that this is due to those concerned facing relationship or career issues that they have not experienced before, particularly as relationships become more serious and jobs become careers (Arnett, 2015). Therefore, there may be an expectation that the individual should be able to deal with these issues without making mistakes, and they may feel that if those in their lives knew more about these issues (and their response to them), they may judge them harshly. There may also be a level of anxiety around an individual feeling that they are behind others in terms of progressing into adulthood, maybe they have not reached the milestones that they believe they should have for someone of their age. This could again, lead to anxiety around others finding out about this, particularly those who are family members who may be disappointed in them.

It is important to note here that how an individual defines their family changes over time, particularly across the age groups that I am examining here. As more students leave university with debt, many are left with little choice but to return to living with their parents, often into their mid- to late-twenties (Hooker, 2019). Therefore, family for those in their twenties is potentially very different to that defined by those in their thirties. By the time they reach thirty, most individuals have different responsibilities, such as a long-term partner, potentially a child and are no longer answerable to their parents. As such, their family and responsibilities will differ from those who are living at home with their parent(s); this could offer an explanation for different levels of concern regarding information being known by an individual's family.

Conclusion

In this chapter, I have acknowledged the importance of context in terms of individuals and the opportunities afforded to them by being able to compartmentalise different areas of their lives. However, with the growth of social media, it is becoming increasingly difficult for boundaries to be maintained between different contexts. As such, there are times when 'context collapse' (Vitak, 2012 p.451) occurs, which can cause issues for people, particularly when they are forced to reveal a part of their identity previously unknown in one of the contexts. Nissenbaum's work on 'contextual integrity' (2010 p.2) is especially useful here, as it highlights how we are often unaware of the different contexts that we move between until we face an issue. This also served to highlight how different situations tend to have different contextual norms, which set out how information should flow within that context and offers an explanation for the discomfort we sometimes feel when asked to share information.

By considering the broad categories of privacy, as set out by Raynes-Goldie (2012), in terms of 'institutional' and 'social privacy' (p.81), I was able to set out the two categories that I believe information encapsulated in the 'social privacy' realm can be broken down into: intrinsic and issued information, once we have broadened social privacy to include commercial information. To do this, I utilise Floridi's (2005) conception of 'arbitrary' or 'ontic' (p.197/8) information as a foundation. The distinction between types of information was brought to me by a number of my interviewees and offers a way of considering our emotional attachment (or lack thereof) to different pieces of information. By examining two of the vignettes from my interviews (one regarding issued information being

hacked and the other intrinsic information), to demonstrate that the situation is not quite as clear as it initially appears. While issued information is not necessarily part of our identity, many appear to have an emotional attachment to it, particularly when we consider financial information. I suggest that this may be due to the availability bias (Tversky & Kahneman, 1982), which suggests that we feel more threatened by issues which we can more easily imagine occurring.

Finally, this chapter focused on various combinations of information and audience, which allowed me to draw some particularly interesting and at times, counter-intuitive findings, especially when considering different demographic groups. Of particular note was the finding that women have greater concerns around information being revealed which could lead to a physical safety threat such as stalking. This again may be due to availability bias (Tversky & Kahneman, 1982), but also speaks to the gendered nature of fear around certain types of crime.

In terms of the audience/information combinations, many of my findings appear to be as expected. However, the government/police audience causes a lower level of concern when compared to other unknown audiences. I posit that this could be due to the belief, expressed by a number of participants, that only those who are involved in illicit or illegal behaviour need to be concerned, as well as a general trust in the government's claim that collecting our information is necessary to counter terrorism and other threats we face.

The issues at stake here are much more complex than they seem initially, and while my work has taken a particular interest in the intersection between type of

information and audience, there are other combinations that could have been included, although to do so may have proved to be impossible, given the potentially infinite number of combinations. In this work, I have attempted to explore how different audiences and types of information can impact the level of concern individuals feel, which has rarely been attempted previously.

The focus on contextual matters in this chapter suggests that it is too simplistic to assume that people who share their information (either with companies or on social networking sites) do not care about privacy. This is clearly not the case, and I have demonstrated the varying degrees of concern regarding two factors – the type of information and the audience that will have access to that information, thus highlighting the nuanced nature of privacy. The context in which we are being asked to share information plays a vital role in whether we feel comfortable sharing it, and as discussed, issues can be caused when contexts collapse, and information is revealed in an unintended context. This is more than simply a case of an individual being caused minor inconvenience or embarrassment; in cases where a person is experimenting with their identity, the revelation of one facet of their identity in an unexpected context can have serious implications, and thus where opposing contexts collapse we lose the ability to create our own identity (Floridi, 2005) and who we are becomes fixed. This is problematic because we are then potentially unable to express ourselves fully or modify who we are, improve ourselves and start again in the future.

Conclusion

Introduction

This thesis offers an initial exploration of how individuals negotiate the boundaries of internet privacy. By exploring the key themes of control, defiance and context, I add some much-needed nuance to the debate around privacy, highlighting the importance of context in particular. My focus on those who engage with social media means that I am able to demonstrate that the axiom that those who utilise social media have few concerns regarding their privacy, is an oversimplification which obfuscates the contextual nature of privacy. As stated previously, while we do not necessarily want everyone to know everything about us, neither do we want to hide everything from everyone. When we care about our privacy depends on the situation we are presented with, as well as factors such as the specific information we are being asked to share and who we are being asked to share it with. Decisions regarding whether to share information or not are deeply personal and as such cannot be considered in terms of a privacy dichotomy, whereby privacy is either on or off. Ultimately, this thesis does not offer a definitive answer regarding the value of privacy, as it is dependent on the individual concerned and the particular situation, however, I have utilised a qualitative approach to answer the following research questions:

- How much control do individuals feel they have over the information they share in their daily lives?
- How do individuals feel about the amount of information they share with companies and online?
- How do individuals negotiate the boundaries of internet privacy?
- In what contexts is privacy important to individuals?

My responses to these questions were designed to explore privacy, especially from the perspective of those who share information on social media, however, it was also important to ensure that I did not focus solely on information shared in this way. Given the ubiquitous nature of Big Data and the aggregation and commodification of the information we share with numerous companies (not all of which are social media organisations), I felt it necessary to include this information-sharing in my study. As such, I explored how people feel about sharing information with companies *in addition* to on social media, especially as it is a situation in which individuals may feel under more pressure to share information. This view is held by a number of my participants:

> "you know everyone's gotta have a phone bill really haven't they? And you need to give your details for that to work, it's not really quite such an optional thing" (AQ, male, 26)

This demonstrates how difficult it can be for people to exercise control in situations whereby they are required to share information, and highlights in a small way how situations differ in terms of what people feel they need to share (and whether they have the option to withhold information). This was an important area of study, as social media sharing is broadly deemed to offer greater control.

In answering the above research questions, I have been able to examine issues around trust, control, context and decisions regarding whether to share information; I now offer responses to these questions.

Research questions

How much control do individuals feel they have over the information they share in their daily lives?

This is a key issue when considering privacy and is closely linked with issues of trust, as people attempt to control the information they share and who they share it with. There is often a sense of mistrust, particularly in terms of the third-parties that companies sell data to without the knowledge or consent of those who have shared their information. This is demonstrated in the following exchange between myself and an interviewee:

> "So, what is it that you don't like about the third-party..." (HEF)
> "Who the hell are they? You know, erm, you don't, you've got no idea who they are" (CB, male, 37)

The issue with third-parties is that people are often unaware of who they are and what they will do with information once they have it. There is an awareness of the practice of information being sold between companies, but participants feel unable to have control in a meaningful way, especially when we consider the difficulty in understanding exactly what we are agreeing to when presented with lengthy terms and conditions. In fact, these documents are deemed to be so confusing that many do not attempt to read them, believing this to be a strategy by companies to encourage individuals to accept the terms and conditions without examining them in detail. This can lead to minor acts of defiance which take the form of either supplying false information or refusing to share information if there is an option to do so. This offers a way for individuals to feel a small sense of

control in terms of maintaining the level of privacy they desire while accessing the site or service they require.

It is also important to note here that despite the perception of a lack of control, that is not to say that people are resigned to having little control and do not desire more, rather they employ tactics and take opportunities when they present themselves to gain additional control, as described above. When dealing with social networking sites, however, there is often a feeling or perception of having greater control over information, particularly in terms of deciding what to post online, such as status updates or tweets. Here too, though, there is the potential for a loss of control in terms of when friends and family post items and tag an individual or when something posted on social media is shared more widely than the individual posting it intended. This necessitates greater consideration prior to posting and often those who cannot be trusted to maintain privacy boundaries are excluded from accessing specific posts (generally without their knowledge). In this sense, it can be argued that individuals are able to employ greater control over their information and how widely it is shared amongst their friends and/or family circle and it can even be argued that this is a tool employed by social media companies to distract us from the reduced control we have when considering what the site itself does with the information that users share on the platform (Raynes-Goldie, 2012).

The issue of control is one that can be contentious and while people may want more control, this is likely to come at a cost particularly in terms of convenience. As such, the desire for additional control is potentially tempered not only by considerations of how achievable the desired level of privacy is, but also whether

achieving that level of privacy is worth the costs that may be incurred. This is an issue that is more serious than it may seem at first glance, especially as many depend on the use of social networks to maintain relationships with friends and family who live in other countries, for example. It is also important in terms of the convenience it offers to people when organising social events, or simply learning about the events occurring in their friends' lives, and thus to consider eschewing these sites in order to regain some privacy, could result in a level of social isolation for that individual.

How do individuals feel about the amount of information they share with companies and online?

This is linked with the above issue of control, in that the absolute amount of information that an individual shares is immaterial, what matters is the level of control they have over how much they share. For example, there may be two individuals who share the same objective amount of information but if one feels that they are required to share more than they are comfortable with (and thus feels less in control), they will be unhappy with the amount of information they share. Ultimately, the amount of information that participants are comfortable with sharing is a subjective decision which often relates to issues of trust.

In situations where participants feel they can trust those that they are sharing their information with, they are broadly happy with the amount of information being requested. However, issues arise when we are asked for information that does not appear to be relevant to the activity we are engaged in. This raises suspicions that the company requesting the information is doing so in order to sell it on to a third-party. Here the issue is that the company is not being honest with the person

involved when requesting the information, in a sense pretending that they need the information for their own records, when this may not be the case. Here, the amount of information being requested raises questions regarding what it is needed for and what will happen to it once shared.

It is also important to recognise that when participants share information it does not necessarily signal tacit acceptance, neither does it mean that they are happy or comfortable in doing so. This is demonstrated in discussions of the privacy paradox, in that an individual may talk about their dissatisfaction with the level of information they are required to share, while continuing to share information. As discussed previously, there are several reasons why people behave in this way, not least because they feel unable to control how much they share.

Therefore, there is a general feeling of discontent regarding the amount of information that individuals share, although it must be noted that where people feel they have control over their data, they are unconcerned about the amount they share, as per the below comment:

> "I feel that the amount I share with companies, is perfectly legitimate. I think the amount they share with other companies is not!" (DC, male, 36)

This demonstrates how many participants feel that they control what they share with companies, while recognising that this is as far as their control can reach, and what happens to it after that is beyond what they are able to control. Therefore, it is possible for people to feel happy with the amount of information they share with companies, while at the same time, being unhappy with what happens to

their information at a subsequently. This highlights how difficult it can be to maintain privacy boundaries and recognises the limited control we can be said to have when engaging with companies.

How do individuals negotiate the boundaries of internet privacy?

There are numerous ways in which participants negotiate the boundaries of internet privacy, and the ability to do so has become much more pressing when we consider issues of context collapse and the potential negative consequences of this. Despite the difficulty involved in maintaining the level of control that individuals would like, they are deemed to be responsible for sustaining the level of privacy that they are comfortable with.

Despite the issues with control I have examined above, there is often a feeling amongst participants that they are making logical tradeoff decisions whereby they consider the benefits they will receive from sharing information and weigh that against the potential loss of privacy and the potential consequences of that. This belief in the ability to make logical decisions is overlaid with feelings (or at least the illusion) of being in control and only sharing information that they want to. There is a sense that whatever methods an individual is employing, if they have not suffered an issue thus far, they are making the right decisions:

> "That's it, it's yeah, it's saying, ' Oh, that's never gonna happen to me, I've been fine for 23 years so far, why's it ever gonna happen now? I'm not gonna do anything different, I'm not gonna change my behaviour, so I'm not at risk.'" (TJ, female, 23)

The above quote demonstrates that participants perceive the lack of an issue as being indicative that they are protecting their privacy in an efficient manner, and thus require no additional work or effort; they can continue as they have been protected thus far. This is part of the issue with a topic such as that of internet privacy, in that it has become a part of our daily lives to such an extent that we barely consider it, until or unless there is an issue. It is such an abstract notion that is it difficult to generate strong feelings about it and this is perhaps why it often appears that there is a lack of concern regarding privacy. However, that is not to say that efforts are not being made, and as discussed previously, participants do attempt to reinforce boundaries through acts of defiance, such as refusing to provide information or by providing false information, which allows them to access the service or website they want to without sharing more information than they are comfortable with. Interestingly, as this action is often taken in a bid to reduce spam emails, it is often not perceived to be a specific strategy in relation to one's privacy, it is more a part of people's daily lives, a habit that they have developed, that does not take any additional thought or effort. However, I argue that it is much more than that, representing a rejection of the incessant collection and aggregation of data that has now become a part of our everyday lives.

The negotiation of the boundaries of internet privacy is necessarily part of a daily practice for individuals whether they recognise it as such or not, and by making these efforts to reinforce their boundaries, participants are attempting to exercise control over their data. However, it is important to note that boundaries in this area are not fixed and as such will change depending upon contextual factors.

In what contexts is privacy important to individuals?

Context is of utmost importance when considering internet privacy because the type of information that participants are willing to share and who they are willing to share it with makes a difference to how comfortable they feel when being asked to share that information. Privacy itself is not 'on' or 'off', instead numerous factors impact upon levels of comfort when we are asked to share information and as such whether we are more or less willing to share. Previously, it was easier to keep different areas of our lives separate from each other; in particular our work and home-life. However, this is becoming increasingly difficult as contexts seep into each other online, especially on social networking sites, where our friends list often includes close friends, relatives and work colleagues, thus requiring additional thought and effort if we are posting something that may be contentious to someone on that list. Concerns regarding this caused one of my participants to change his privacy settings on Facebook:

> "I haven't done this in my existing job, but a previous job where I was, I was friends on Facebook with my manager, I set it up so that he was the only that couldn't see my posts, cos I just wanted to take that out of my mind that I can post stuff, I think that was mainly about political stuff that I just, I'm sure it probably would have been OK, but I erm just thought I'd rather like just not have to think about what's he gonna think about me saying this stuff?" (PF, male, 39)

This demonstrates the importance of context and the concerns that may be felt at the prospect of different contexts in our lives converging. As PF states, he was not posting anything that was particularly controversial, but it gave him a sense of

peace to know that he did not have to put additional effort into considering what he was about to post or who would see it. Therefore, context is important enough that many feel it necessary to take action to reduce the likelihood of different contexts collapsing in on each other, and often this is done through making amendments to privacy settings on social media. This also links with the issue of control discussed above and is one of the areas in which control can be said to be possible.

As discussed previously, although we can categorise social information into intrinsic and issued information, there are complications in doing so, as participants have differing opinions regarding the type of information that would cause them the greatest level of concern. This highlights the complex nature of information type and how context varies according to what is important to the individual concerned. Another complicating factor here is if we consider the role that previous experience can play when considering levels of concern then it is possible that those who have not experienced a negative consequence previously are not as concerned as those who have had an issue. In particular this may make it seem that experiencing an issue is more likely, as they are able to recall the previous situation, as per the 'availability heuristic' (Tversky & Kahneman, 1982 p.20). This suggests that the context in which participants believe there will be immediate negative consequences for them are of greater concern than in contexts where there will be few (if any) issues and/or they will be experienced far into the future.

Moving away from the type of information, the audience that will have access to the information also has an impact on levels of concern. Although concern levels

tend to be as expected in that participants are less concerned about audiences who are closely related or are close friends; other groups, however, offer a slightly more surprising reading of context. As such, there is less concern when participants are asked to share information with the government/police, when compared with strangers or third-parties (that they have not already agreed to share information with). This highlights the potential for less concern when we believe that there will be no negative consequences related to sharing data (although it is important to highlight that the concern scores for the government/police remain above 3 for most types of information). I have attributed the slightly lower levels of concern here to participants' belief that they are not doing anything wrong or illegal and so believe they do not need to be as concerned about those in authority having access to information about them. Strangers and third-parties, however, are of slightly more concern, potentially because it is not always clear who they are and what their intentions are with regard to our data.

Context offers an interesting and complicating lens through which to consider our privacy, and which contexts cause greater concern is dependent upon many factors, while I have considered two important factors, there are others which require further investigation.

Research findings

Through the interviews and surveys that I carried out, new light has been cast upon how people negotiate the boundaries of internet privacy, particularly in terms of the contextual nature of privacy. However, it is important to note that

prior work has considered the role of context; Nissenbaum's (2010) work has been particularly instructive and offered a foundation upon which to consider context. Her discussions around contextual integrity and appropriate data flows were particularly inciteful, suggesting that information sharing varies from situation to situation. In some situations people are happy to share data and in others they are not. Therefore, my work sought to examine this further in an attempt to discover whether there was universal agreement on which particular situations cause high levels of concern and which do not. I believe that my findings have gone some way towards validating the work of Nissenbaum and demonstrating the importance of context to individuals, while considering specific situations. By focusing on social media users, I have also studied a group that is often assumed to have little or no interest in their privacy, and so this adds weight to the argument that this is not the case.

I have also considered the social privacy in terms of commercial surveillance, which has rarely been done previously. To do so, (and as set out previously), I have broadened Raynes-Goldie's (2012) definition of social privacy to include commercial information, which upon initial consideration may not appear to be social in nature. However, given the aggregation of data which links numerous pieces of information about an individual and the way in which this can affect how others view them, I argue that commercial information fits into the category of social information. In doing so, I have been able to complicate matters by considering types of information which would not necessarily have been considered to be social previously, (such as financial), thus drawing out issues that have been taken for granted.

While at times, my findings have generated additional questions, particularly, which situations generate greater levels of concern in terms of sharing information, there can be no doubt that people do care about their privacy and what happens to their information. However, they do not necessarily consider it in the course of their daily lives and it often only becomes worthy of more than a momentary thought when our attention is drawn to the potential for things to go wrong, such as with Edward Snowden's 2013 revelations regarding government surveillance (Greenwald, et al., 2013) or the more recent Cambridge Analytica Scandal (Cadwalladr & Graham-Harrison, 2018). Here, we have been reminded of the potential for negative consequences when sharing our data, bringing into sharp focus how little we know about what happens to our data once we have shared it. Despite the potential issues, we continue to share our information, and there are various reasons for this, such as the benefits we receive from doing so as well as potentially feeling that there is little we can do to halt this collection.

While participants feel that too much information is requested and lack trust in those collecting it (suspecting that it will be shared with others), we do have (limited) ways in which we attempt to regain some control and can exercise defiance in the face of continued data collection. This can be in the form of a complete refusal to share information or by sharing false information to gain access without foregoing privacy. Regardless of which method is used, participants feel empowered by such actions and believe that they have been able to take action in their own way and draw a line in terms of how much information they are willing to share.

These tactics are not employed all the time, indeed, to do so may render them less effective, however, these methods are employed when individuals deem it necessary and are related to the context in which information is being requested. Therefore, it is imperative that we consider context when thinking about privacy, for this will inform how comfortable a person is with sharing specific information with particular audiences. There is no formula for this, and it depends very much on the individual in question, although Nissenbaum's (2010) work regarding appropriate information flows offers a foundation for considering this. When I attempted to define broad categories that different types of social information could be separated into (intrinsic and issued information), as a way of refining how concerned individuals would be in different contexts, there were issues, in that some information did not neatly fit into the expected category (financial information was particularly problematic). However, as discussed previously, this may be due in part to the category of financial information being too broad as it encompasses account numbers, as well as salary information and the balance of our current accounts and so on, which may explain the ambivalence towards this type of information. Therefore, while my study of types of information and audience has been informative when considering the issue of context, it does not offer a definitive scale regarding which types of information or audience will be more or less worrisome than others, except to say that context is vital to considerations and negotiations around internet privacy. However, by suggested additional categories of information, and a rationale behind them, I have been able to consider types of information that may have been taken for granted previously and offer another way to consider privacy and when it does or does not matter to us.

Original contribution

By considering the categorisation of information types, I have built upon the foundations offered by Raynes-Goldie (2012) and Floridi (2005) in an attempt to develop a useful categorisation of social information, which I term intrinsic and issued information. While this has offered one way of considering different types of data in terms of how important the privacy of certain pieces of information is, this has not been wholly successful, as there are data for which categorisation is not as clear as expected. The example I offer here is that of financial information such as a person's bank account number, which initially appears to be issued information, in that it is issued by a financial institution and not a part of that person's identity in the same way that intrinsic information is. Therefore, it should carry no emotional weight for them and as such if it were to be known by an unscrupulous hacker, the individual could simply inform the bank and be re-issued with a new account number. In theory, this would be nothing more than a minor inconvenience; this view was shared by a number of participants, who felt little concern for this type of information, believing that the bank would take responsibility and deal with any losses incurred. However, this view was not shared by everyone and for others, there was a much greater emotional attachment and as such this led to far greater concerns regarding a situation whereby bank details were hacked. However, this is due, in part to the fact that an individual's account number is the key to accessing their money and so while the account number in and of itself is not meaningful, it allows access to items that are much more important to us, and so elicit an emotional response. Further, as discussed previously, financial information is not devoid of emotional attachment or

response for many individuals, and so this reminds us that other factors may affect our response to issues involving particular pieces of data.

This example demonstrates that while some types of information initially appear to be straightforward to categorise, (for example, private messages would be categorised as intrinsic information), this is not necessarily the case. Therefore, what could be described as a failure in terms of my attempt to offer a new categorisation for social information, merely serves to reinforce the contextual nature of privacy. As such, if privacy were not nuanced or contextual, the process of categorising information would be much clearer, however, the differing views of my participants here highlights that this is not an issue that is amenable to categorisation, bringing forth it's the complex nature.

My consideration of context and its importance when people are attempting to negotiate the boundaries of internet privacy is where most of my original contribution lies. Although this concept has been considered previously, particularly in the work of Nissenbaum (2010), in terms of how individuals reflect upon their privacy and when they are and are not willing to share specific information. This is fundamental to the everyday decisions that people make; they are not blindly sharing their information with whoever requests it, rather the context in which information is being requested is fundamental to how participants feel about sharing that information. The importance of context is a significant finding, especially given the existence of the privacy paradox and the subsequent suggestion that while people may express reticence at sharing information, they continue to do so. If we consider the role of context, it is clear that the sharing of data is nuanced and simply because a person shares

information in some situations, with some audiences, that does not mean they will share the same information with a different audience. Therefore, people are often much more aware of concerns regarding their privacy and make different decisions regarding whether to share information, dependent upon contextual factors.

While some of my results in this area appear axiomatic, in terms of the levels of concern raised in relation to particular audiences that we are broadly close to, I offer an initial exploration of the impact of context which has rarely been seen previously. Future research could go in any number of directions, following my work, given that there is so much still to unpack in terms of context. It is possible that if I were to carry out my research in exactly the same way now, it would elicit different responses, given how reliant many have become on online platforms since the beginning of the Coronavirus pandemic of 2020. Given that my research offers a snapshot of how individuals negotiate the boundaries of their internet privacy at a particular point in time, it could be fruitful to consider a longitudinal study of people, over a longer period of time, which could examine how concerns regarding privacy change over a person's lifetime, given the different priorities they have over a longer period. This may answer some of the questions which were raised when I considered differences in responses of participants of different ages (and potentially different life-stages).

Where do we go from here?

As discussed throughout this thesis, this study is exploratory in nature and so offers a suggestion of avenues which would benefit from further examination.

Given the importance of context, and the paucity of previous research in this area, there is still much to uncover, particularly in terms of which contextual factors have a greater impact, or whether they are of equal importance. This research has not only demonstrated that those who use social media do care about their data privacy, but also that they are not willing to sit by and allow their data to be collected and sold without taking some sort of action, as demonstrated in their (small) acts of resistance. I have also shown the importance of context, which adds to the existing research and offers more detailed information regarding what is or is not important to individuals. As such, my work demonstrates that type of information and the potential audience for that information affects the levels of concern expressed. As discussed previously, this is in line with Nissenbaum's work regarding contextual integrity (2010) but offers an added level of detail by considering particular types of information and specific audiences, which can be built upon in future research. In particular, the work of Stoilova et al. (2019a and 2019b), could be especially illuminating, as many of their findings regarding children can be said to apply to adults also. Their work regarding the various types of contexts and data types in particular offers an area which would only benefit from further examination and exploration. This is especially important because as discussed throughout my thesis, much of the data collection that takes place when we are online is hidden and as such many adults are unaware that it is happening. This is particularly pertinent, as there is often the expectation that parents and teachers will educate children and young people in terms of internet usage and how to look after their data online, however, this is difficult (if not impossible) if the adults themselves lack the knowledge required to be able to do this.

Given the introduction of the GDPR 2018 and DPA 2018 and in the wake of the Cambridge Analytica scandal, it is important to recognise attempts by the government and law to provide support for individuals to help them to navigate the complicated landscape of internet privacy. Indeed, it could be argued that legally, we are now in a better position in terms of what companies are legally sanctioned to do with data we have shared, however, there are questions regarding whether the situation has improved in a practical sense. For example, the introduction of the GDPR 2018 was cast as an opportunity for individuals to review what they had agreed to regarding companies they had shared information with previously, however, as discussed throughout, the sheer volume of GDPR notices that people received prior to the legislation coming into force became a hindrance to many who were confused by this (Kelion, 2018). Therefore, we cannot assume that new legislation will automatically improve things for individuals, regardless of the intention. Another issue with legislation is that it tends to move much more slowly than technology advances and as such may be ill-equipped to deal with issues by the time it is introduced. While it is too early to say whether this has been the case when considering the GDPR 2018 and DPA 2018, it is important to note the wide array of changes and issues that have occurred in the time I have been carrying out this project. For example, the Investigatory Powers Act 2016 has been passed, faced a successful legal challenge and been superseded by the Data Retention and Acquisition Regulations 2018; in the past year, Facebook has faced numerous legal challenges and fines in the aftermath of the Cambridge Analytica scandal.

At the same time, technology continues to advance and the introduction of facial recognition technology has become part of many individuals' daily lives, as it

allows them to unlock their mobile devices (for example), this is despite the technology itself facing much criticism (Kelion, 2019). Concerns regarding electronic assistants, such as Amazon's Alexa have also been raised regarding the potential for conversations to be recorded and stored (Greenberg, 2017). Any of these issues are worthy of further exploration and have the potential to affect how we consider and negotiate the boundaries of our internet privacy and so we must continue to investigate and question what these changes mean, rather than simply accepting them because they make our lives more convenient.

If I were to make recommendations for the future, based on my findings, I would strongly urge individuals to take a more pro-active approach to their data privacy, although I appreciate that it appears overwhelming to begin with and as such, this would also require work on the part of companies who collect and sell our data. Terms and conditions documents need to be much clearer for individuals to read and understand, so that we are all able to take a more active role in securing our own privacy and ensure that we only share our data when we are comfortable in doing so. I appreciate that companies are unlikely to volunteer to do this, particularly as there is the belief that if individuals are given more control over what they share, they will choose to share less. While this may be true in some cases, in others, it may not, and people may feel more empowered and trusting of organisations and thus more willing to share their information as the believe that it will be dealt with respectfully. As such, this is likely to require legal intervention to take the choice out of the hands of companies and force them to do this and so governments and/or regulators would need to work on this. However, this is only a small piece of the puzzle and if companies did not make so much money from aggregating and selling user data, they simply would not do it and so I believe

there is also work to be done there in terms of encouraging companies to consider users to be customers, rather than the product. This will be particularly challenging, given the ambivalent feelings that my participants had towards the potential to pay for increased privacy, as such there are no straightforward or easy answers here, but I do believe that control should be put back into the hands of individuals, so that they can make meaningful decisions regarding the sharing of their information. The GDPR 2018 and DPA 2018 are steps towards this, however, already, in the wake of the Coronavirus pandemic, the principles of these laws are potentially being ignored (Cellan-Jones, 2020), in the name of public health. Therefore, if we take no other action, it is important that we consider the implications in terms of our privacy whenever we are asked to provide information, for whatever reason, and where possible ask questions, rather than simply providing the information and asking questions later.

> "The constellation of inconvenient choices may be all that stands between us and a life of total, efficient conformity."
>
> (Wu, 2016)

Bibliography

Ackerman, M. S., Cranor, L. F. & Reagle, J., 1999. *Privacy in e-commerce: examining user scenarios and privacy preferences.* s.l., Proceedings of the 1st ACM conference on Electronic commerce.

Acquisti, A., 2004. *Privacy in electronic commerce and the economics of immediate gratification.* s.l., Proceedings of the 5th ACM conference on Electronic commerce.

Acquisti, A. & Grossklags, J., 2005. Privacy and rationality in individual decision making. *IEEE security & privacy,* 3(1), pp. 26-33.

Acquisti, A. & Grossklags, S. J., 2003. *Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior.* s.l., 2nd Annual Workshop on Economics and Information Security-WEIS.

Acquisti, A. & Gross, R., 2006. *Imagined communities: awareness, information sharing and privacy on the Facebook.* Berlin, Springer, pp. 36-58.

Amazon, 2019. *Product page for Amazon Echo Dot.* [Online]
Available at: https://www.amazon.co.uk/gp/product/B07PJV3JPR/ref=fs_aucc
[Accessed 1 October 2019].

Andrejevic, M., 2013. Estranged free labor [sic]. In: T. Sholz, ed. *Digital Labor [sic]: The Internet as Playground and Factory.* Oxon: Routledge.

Andrejevic, M. & Gates, K., 2014. Editorial: Big data surveillance: Introduction. *Surveillance and Society,* 12(2), pp. 185-196.

Anthony, D. & Stark, L., 2018. *Don't quit Facebook, but don't trust it, either.* [Online]
Available at: https://theconversation.com/dont-quit-facebook-but-dont-trust-it-either-93776 [Accessed 10 April 2018].

Arendt, H., 1958. *The Human Condition.* London: University of Chicago.

Ariés, P., 1996 [1962]. *Centuries of Childhood.* London: Random House.

Arnett, J. J., 2015. *Emerging Adulthood: The Winding Road from the Late Teens Through the Twenties.* New York: Oxford University Press.

Babbie, E. A., 1973. *Survey research methods.* California: Wadsworth.

Barter, E. & Renold, C., 1999. The use of vignettes in qualitative research. *Social Research Update,* 25(9), pp. 1-7.

BBC News, 2015a. *Ashley Madison infidelity site's customer data 'leaked'.* [Online] Available at: http://www.bbc.co.uk/news/business-33984017 [Accessed 26 November 2015].

BBC News, 2015b. *TalkTalk attack: 'Urgent action needed' on cyber-crime.* [Online] Available at: http://www.bbc.co.uk/news/uk-34622754 [Accessed 5 November 2015].

BBC News, 2018a. *Facebook fined £500,000 for Cambridge Analytica scandal.* [Online] Available at: https://www.bbc.co.uk/news/technology-45976300 [Accessed 21 July 2019].

BBC News, 2018b. *O2 4G data network restored after day-long outage.* [Online] Available at: https://www.bbc.co.uk/news/business-46464730 [Accessed 11 December 2018].

BBC News, 2019. *Facebook agrees to pay Cambridge Analytica fine to UK.* [Online] Available at: https://www.bbc.co.uk/news/technology-50234141 [Accessed 1 November 2019].

Bennett, C., 2012. *Not on Facebook? What kind of sad sicko are you?.* [Online] Available at: https://www.theguardian.com/commentisfree/2012/aug/12/catherine-bennett-facebook-psycopaths [Accessed 22 July 2016].

Benson, V., Saridakis, G. & 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.

Berger, P., Berger, B. & Kellner, H., 1977. *The Homeless Mind.* Middlesex: Penguin Books Limited.

Blanchette, J. F. & Johnson, D., 2002. Data retention and the panoptic society: The social benefits of forgetfulness. *The Information Society,* 18(1), pp. 33-45.

Blank, G., Bolsover, G. & Duboois, E., 2014. *A new privacy paradox.* San Francisco, CA, Annual Meeting of the American Sociological Association.

Booth, R., 2014. *Facebook reveals news feed experiment to control emotions.* [Online] Available at: https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds [Accessed 30 July 2019].

Bourdieu, P., 1984. *Distinction. A social critique of the judgement of taste.* London: Routledge.

boyd, d., 2008. Facebook's privacy trainwreck: Exposure, invasion and social convergence. *Convergence,* 14(1), pp. 13-20.

boyd, d., 2014. *It's Complicated: The Social Lives of Networked Teens.* New Haven and London: Yale University Press.

boyd, d. & Crawford, K., 2012. Critical questions for big data: Provocations for a cultural, technological and scholarly phenomenon. *Information, Communication and Society,* 15(5), pp. 662-679.

Bradbury-Jones, C., Taylor, J. & Herber, O. R., 2012. Vignette development and administration: A framework for protecting research participants. *International Journal of Social Research Methodology,* 12(53), pp. 427-440.

Braun, M. T., 2013. Obstacles to social networking website use among older adults. *Computers in Human Behaviour,* 29(3), pp. 673-680.

Bryman, A., 2012. *Social research methods.* Oxford: Oxford University Press.

Bucher, T., 2018. *If...then: Algorithmic power and politics.* Oxford: Oxford University Press.

Buchi, M., Just, N. & Latzer, M., 2017. Caring is not enough: the importance of internet skills for online privacy protection. *Information, Communication & Society,* 20(8), pp. 1261-1278.

Cadwalladr, C., 2019. *Cambridge Analytica a year on: 'a lesson in institutional failure'.* [Online] Available at: https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie [Accessed 19 September 2019].

Cadwalladr, C. & Graham-Harrison, E., 2018. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* [Online] Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [Accessed 19 September 2019].

Campbell, D. & Fiske, D. W., 1959. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychology,* Volume 54, pp. 297-312.

Carvell, T., Gurewitch, D. & Oliver, J., 2015. *Government Surveillance.* s.l.:HBO.

Cellan-Jones, R., 2020. *Coronavirus: England's test and trace programme 'breaks GDPR data law'.* [Online] Available at: https://www.bbc.co.uk/news/technology-53466471 [Accessed 21 July 2020].

Chellappa, R. K. & Sin, R. G., 2005. Personalization versus privacy: an empirical examination of the online consumer's dilemma. *Information Technology and Management,* 6(2-3), pp. 181-202.

CitizenFour. 2014. [Film] Directed by Laura Poitras. s.l.: Radius-TWC.

Clark, T., 2010. On 'being researched': why do people engage with qualitative research?. *Qualitative Research,* 10(4), pp. 399-419.

Cobain, I., 2018. *UK has six months to rewrite snooper's charter, high court rules.* [Online] Available at: https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules [Accessed 10 October 2019].

Cohen, J. E., 2012. Configuring the networked citizen. In: A. Sarat, L. Douglas & M. M. Umphrey, eds. *Imagining new legalities: privacy and its possibilities in the 21st century.* California: Stanford University Press.

Cohen, J. E., 2017. Sureillance vs. privacy: effects and implications. In: D. Gray & S. E. Henderson, eds. *Cambridge Handbook of surveillance law.* New York: Cambridge University Press.

Cohen, J. E., 2019. The emergent limbic media system. In: M. Hildebrandt & K. O'Hara, eds. *Life and the law in the era of data-driven agency.* Northampton: Edward Elgar Publishing Ltd.

Cohen, N. S., 2008. The Valorization of Surveillance: Towards a Political Economy of Facebook. *Democratic Communiqué,* 22(1), pp. 5-22.

Coll, S., 2014. Power, knowledge and the subjects of privacy: Understanding privacy as the ally of surveillance. *Information, Communication and Society,* 17(10), pp. 1250-1263.

Comor, E., 2010. Digital Prosumption and Alienation. *Ephemera,* 10(3), pp. 439-454.

Consolvo, S. et al., 2005. *Location disclosure to social relations: why, when, & what people want to share.* s.l., Proceedings of the SIGCHI conference on Human factors in computing systems.

Costa, E., 2018. Affordances-in-practice: An ethnographic critique of social media logic and context collapse. *New Media & Sociey,* 20(10), pp. 3641-3656.

Couldry, N. & Mejias, U. A., 2019a. *The costs of connection: How data is colonizing human life and appropriating it for capitalism.* Stanford: Stanford University Press.

Couldry, N. & Mejias, U. A., 2019b. Data colonialism: Rethinking Big Data's relation to th contemporary subject. *Television and New Media,* 20(4), pp. 336-349.

Cresswell, J. W., 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* London: Sage.

Culnan, M. J., 1993. "How did they get my name?" An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quartery,* pp. 341-363.

de Certeau, M., 1988. *The practice of everyday life.* London: University of California Press.

Dedkova, L., 2015. Stranger is not always danger: the myth and reality of meetings with online strangers. In: M. F. Wright, ed. *Living in the Digital Age: Self-Presentation, Networking, Playing and Participating in Politics.* Brno: Muni Press.

Dommeyer, C. J. & Gross, B. L., 2003. What consumers know and what they do: An investigation of consumer knowledge, awareness and use of privacy protection strategies. *Journal of Interactive Marketing,* 17(2), pp. 34-51.

Douglas, M. & Wildavsky, A., 1983. *Risk and Culture.* London: University of California Press.

Dyer-Witheford, N., 2015. *Cyber-Proletariat: Global Labour in the Digital Vortex.* London: Pluto Press.

Eleuze, I. & Quan-Haase, A., 2018. Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. *American Behavioural Scientist,* 62(10), pp. 1372-1391.

Elias, N., 2000 [1994]. *The civilising process: Sociogenetic and psychogenetic investigations.* Oxford: Blackwell Publishers.

Elias, N., 2008 [1939]. Essay 4 - L'espace privé: Private space or private room?. In: R. Kilminster & S. Mennell, eds. *Essays II: On Civilising Process, State Formation and National Identity. The Collected Works of Norbert Elias Volume 15.* Dublin: University College Dublin Press.

EMC Corporation, 2014. *Consumer perceptions on security: Do they still care?,* s.l.: EMC Corporation.

Facebook, 2019. *Privacy Settings and Tools.* [Online] Available at: https://www.facebook.com/settings?tab=privacy [Accessed 10 October 2019].

Ferrarro, K., 1995. *Fear of Crime: Interpreting Victimization [sic] Risk.* New York: State University of New York.

First Insight, 2019. *The Rise of the Male Power Shopper,* s.l.: Berns Communications.

Fiske, J., 1989. *Reading The Popular.* London: Unwin Hyman.

Floridi, L., 2005. The ontological interpretation of informational privacy. *Ethics and Information Technology,* 7(4), pp. 185-200.

Floridi, L., 2015. Free online services: enabling, disenfranchising and disempowering. *Philosophy and Technology,* 28(2), pp. 163-166.

Fogel, J. & Mehmad, E., 2009. Internet social network communities: Risk taking, trust and privacy concerns. *Computers in Human Behavior [sic],* 25(1), pp. 153-160.

Foucault, M., 1977. *Discipline and Punish.* London: Penguin Books.

Foucault, M., 1980. *Power/Knowledge: Selected interviews and other writings 1972-1977.* Harlow: The Harvester Press Limited.

Fowler, G. A., 2012. *When the most personal secrets get outed on Facebook.* [Online] Available at: https://www.wsj.com/articles/SB10000872396390444165804578008740578200224 [Accessed 15 November 2014].

Fuchs, C., 2010. Labor in Informational Capitalism on the Internet. *The Information Society,* 26(3), pp. 179-196.

Fuchs, C., 2012. The political economy of Facebook. *Television and Media,* 13(2), pp. 139-159.

Fuchs, C., 2013. Class and exploitation on the internet. In: T. Scholz, ed. *Digital Labor [sic]: The Internet as Playground and Factory.* Oxon: Routledge.

Fuchs, C., 2014. *Social Media: A Critical Introduction.* London: Sage.

Gadzheva, M., 2008. Privacy in the age of transparency: The new vulnerability of the individual. *Social Science Computer Review,* 26(1), pp. 60-74.

Garfinkel, S., 2001. *Database Nation: The Death of Privacy in the Twenty-First Century.* California: O'Reilly Media.

Giddens, A., 1991. *Modernity and Self-Identity.* Cambridge: Polity Press.

Giddens, A., 2012 [1991]. *The Consequences of Modernity.* Cambridge: Polity.

Gillespie, T., 2007. *Wired shut: Copyright and the shape of digital culture.* London: The MIT Press.

Glance, D., 2018. *It's impossible for Facebook users to protect themselves from data exploitation.* [Online] Available at: http://theconversation.com/its-impossible-for-facebook-users-to-protect-themselves-from-data-exploitation-93800 [Accessed 10 April 2018].

Glaser, B. G. & Strauss, A. L., 1967. *The discovery of grounded theory: Strategies for qualitative research.* London: Weidenfield and Nicholson.

Goffman, E., 1968. *Behavior in Public Places: Notes on the Social Organisational of Gatherings.* New York: The Free Press.

Goffman, E., 1990 [1969]. *The Presentation of Self in Everyday Life.* Middlesex: Penguin Books Limited.

Gong, X., Liu, Z. & Wu, T., 2018. Gender differences in the anticedents of trust in mobile social networking services. *The Services Industry Journal,* pp. 1-27.

Gordon, S., 2003. *Privacy: A study of attitudes and behaviours in US, UK and EU information security professionals.* [Online]
Available at:
https://www.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf
[Accessed 02 February 2016].

Gorman, E. & Kmec, J. A., 2007. We (have to) try harder: gender and required work effort in Britain and the United States. *Gender and Society,* 21(6), pp. 828-856.

Greenberg, A., 2017. *A Hacker Turned an Amazon Echo Into a 'Wiretap'.* [Online] Available at: https://www.wired.com/story/amazon-echo-wiretap-hack/ [Accessed 6 March 2018].

Greene, J. C., Kreider, H. & Mayer, E., 2012. Combining Qualitative and Quantitative Methods in Social Inquiry. In: B. Somekh & C. Lewin, eds. *Theory and Methods in Social Research.* London: Sage.

Greenwald, G., 2013. *NSA collecting phone records of millions of Verizon customers.* [Online] Available at:
https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [Accessed 22 April 2015].

Greenwald, G., MacAskill, E. & Poitras, L., 2013. *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* [Online] Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [Accessed 10 July 2016].

Groopman, J. & Etlinger, S., 2015. *Consumer perceptions of privacy in the Internet of Things.* [Online] Available at: http://www.altimetergroup.com/pdf/reports/Consumer-Perceptions-Privacy-IoT-Altimeter-Group.pdf [Accessed 25 November 2015].

Guest, G., Bunce, A. & Johnson, L., 2006. How many interviews are enough? A experiment with data saturation and variability. *Field Methods,* 18(1), pp. 59-82.

Habermas, J., 1989. *The Structured Transformation of the Public Sphere.* Cambridge: Polity Press.

Hann, I. H., Hui, K. L., Lee, S. Y. & Png, I. P., 2007. Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems,* 24(2), pp. 13-42.

Hargittai, E. & Marwick, A., 2016. "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication,* Volume 10, pp. 3737-3757.

Hernández, B., Jiménez, J. & Martin, M. J., 2011. Age, gender and income: do they really moderate online shopping behaviour?. *Online Information Review,* 35(1), pp. 113-133.

Hern, A., 2017. *'Anonymous' browsing data can be easily exposed, researchers reveal.* [Online] Available at: https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers [Accessed 8 September 2017].

Hesmondhalgh, D., 2010. User-Generated Content, Free Labour and the Cultural Industries. *Ephemera,* 10(3), pp. 267-284.

Hochschild, A. R., 2003. *The managed heart: commercialization of human feeling.* London: University of California.

Hogarth, R. M. & Reder, M. W., 1986. Introduction: perspectives from economics and psychology. In: R. M. Hogarth & M. W. Reder, eds. *Rational choice: The contrast between Economics and Psychology.* London: University of Chicago.

Hoofnagle, C. J. & Urban, J. M., 2014. Alan Westin's privacy homo economicus. *Wake Forest Law Review,* Volume 49, pp. 261-318.

Hooker, L., 2019. *'Costs soar at hotel of mum and dad'.* [Online] Available at: https://www.bbc.co.uk/news/business-49508854 [Accessed 30 August 2019].

Huberman, B. A., Adar, E. & Fine, L. R., 2005. Valuating privacy. *IEEE security & privacy,* 3(5), pp. 22-25.

Hughes, R. & Huby, M., 2004. The construction and interpretation of vignettes in social research. *Social Work and Social Sciences Review,* 11(1), pp. 36-51.

Hunter, A. & Brewer, J., 2003. Multimethod research in Sociology. In: A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and behavioral research.* London: Sage.

Information Commissioner's Office, 2019. *Guide to the General Data Protection Regulation (GDPR).* [Online] Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf [Accessed 15 September 2019].

Jackson, M., Harrison, P., Swinburn, B. & Lawrence, M., 2015. Using a qualitative vignette to explore a complex public health issue. *Qualitative Health Research,* 25(10), pp. 1395-1409.

Jarvenpaa, S. L., Tractinsky, N. & Saarinen, L., 1999. Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication,* 5(2), p. JCMC526.

Jenkins, N. et al., 2010. Putting it in context: The use of vignettes in qualitative interviewing. *Qualitative Research,* 10(2), pp. 175-198.

Jensen, C. & Potts, C., 2004. *Privacy policies as decision-making tools: an evaluation of online privacy notices.* s.l., Proceedings of SIGCHI Conference on human factors in computing systems.

John, L. K., Acquisti, A. & Lowenstein, G., 2011. Strangers on a plane: Context dependent willingness to divulge sensitive information. *Journal of Consumer Research,* 37(5), pp. 858-873.

Johnson, B. & Turner, L. A., 2003. Data collection strategies in mixed methods research. In: A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and behavioral research.* London: Sage.

Kelion, L., 2017. *Gmail to end ad-targeting email scans.* [Online] Available at: https://www.bbc.co.uk/news/technology-40404923 [Accessed 8 March 2018].

Kelion, L., 2018. *How to handle the flood of GDPR privacy updates.* [Online] Available at: https://www.bbc.co.uk/news/technology-43907689 [Accessed 10 May 2018].

Kelion, L., 2019. *Amazon heads off facial recognition rebellion.* [Online] Available at: https://www.bbc.co.uk/news/technology-48339142 [Accessed 19 June 2019].

Kleinman, Z., 2018. *Cambridge Analytica: The story so far.* [Online] Available at: https://www.bbc.co.uk/news/technology-43465968 [Accessed 9 August 2018].

Kolsaker, A. & Payne, C., 2002. Engendering trust in e-commerce: A study of gender-based concerns. *Marketing Intelligence and Planning,* 20(4), pp. 206-214.

Kosinski, M., Stillwell, D. & Graepel, T., 2013. Private traits and attributes are predictable from digital records of human behaviour. *Proceedings of the National Academy of Sciences (PNAS),* 110(4), pp. 5802-5805.

Kramer, A. D., Guillory, J. E. & Hancock, J. T., 2014. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS,* 111(24), pp. 8788-8790.

Kumar, K., 1997. Home: The promise and predicament of private life at the end of the twentieth century. In: J. Weintraub & K. Kumar, eds. *Public and Private in Thought and Practice.* Chicago: University of Chicago Press.

Kvale, S., 2009 [2007]. *Doing interviews.* London: Sage.

Lasch, C., 1995. *Haven in a Heartless World.* London: Norton.

Laufer, R. S. & Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues,* 33(3), pp. 22-42.

Lawler, S., 2002. Narrative in social research. In: T. May, ed. *Qualitative research in action.* London: Sage.

Layder, D., 1998. *Sociological practice: Linking theory and social research.* London: Sage Publications.

Lee, R., 1993. *Doing research on sensitive topics.* London: Sage.

Lin, Y., 2018. *#DeleteFacebook is still feeding the beast – but there are ways to overcome surveillance capitalism.* [Online] Available at: https://theconversation.com/deletefacebook-is-still-feeding-the-beast-but-there-are-ways-to-overcome-surveillance-capitalism-93874 [Accessed 10 April 2018].

Lyon, D., 1994 [1988]. *The Information Society: Issues and Illusions.* Cambridge: Polity Press.

Lyon, D., 2000 [1994]. *The Electronic Eye: The Rise of Surveillance Society.* Cambridge: Polity Press.

Lyon, D., 2005 [2001]. *Surveillance Society: Monitoring Everyday Life.* Buckingham: Open University Press.

Madden, M., 2014. *Public perceptions of privacy and security in the post-Snowden era,* s.l.: Pew Research Center [sic].

Madden, M. & Rainie, L., 2015. *Americans' Attitudes About Privacy, Security and Surveillance,* s.l.: Pew Research Center [sic].

Martin, K. D., Borah, A. & Palmatier, R. W., 2018. A strong privacy policy can save your company millions. *Harvard Business Review.*

Marwick, A. E. & boyd, d., 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society,* 16(7), pp. 1051-1067.

Mason, J., 2002. *Qualitative researching.* London: Sage.

Mason, M., 2010. Sample size and saturation in PhD studies using qualitative interviews. *Forum: qualitative social research,* 11(3).

Maus, G., 2015. *How corporate data brokers sell your life and why you should be concerned.* [Online] Available at: https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/ [Accessed 30 September 2015].

McDonald, A. M. & Cranor, L. F., 2008. The cost of reading privacy policies. *IS A Journal of Law & Policy for the Information Society,* pp. 540-568.

McGrath, J. E., 2004. *Loving Big Brother: Performance, Privacy and Surveillance Space.* London: Routledge.

Meek, A., 2015. *Data could be the real draw of the Internet of Things - but for whom?.* [Online] Available at: http://www.theguardian.com/technology/2015/sep/14/data-generation-insights-internet-of-things [Accessed 20 January 2016].

Metzger, M. J., 2004. Privacy, trust and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication,* 9(4), p. n.p..

Miller, V., 2011. *Understanding Digital Culture.* London: Sage.

Miller, V., 2016. *The Crisis of Presence in Contemporary Culture.* London: Sage.

Milne, G. R. & Culnan, M. J., 2004. Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing,* 18(3), pp. 15-29.

Mitchell, V., Stephen, A. & Kamleitner, B., 2018. *Your online privacy depends as much on your friends' data habits as your own.* [Online] Available at: https://theconversation.com/your-online-privacy-depends-as-much-on-your-friends-data-habits-as-your-own-93860 [Accessed 10 April 2018].

Morse, J. M., 2003. Principles of mixed methods and mulitmethod research design. In: A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and behavioral research.* London: Sage.

Nippert-Eng, C. E., 2010. *Islands of Privacy.* Chicago: University of Chicago Press.

Nissenbaum, H., 2010. *Privacy in Context: Technology, Policy and the Integrity of Social Life.* California: Stanford University Press.

Nissenbaum, H., 2011. A contextual approach to privacy online. *Daedalus,* 140(4), pp. 32-48.

Norberg, P., Horne, D. R. & Horne, D. A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviours. *Journal of Consumer Affairs,* 41(1), pp. 100-126.

Nowak, G. J. & Phelps, J., 1992. Understanding privacy concerns: an assessment of consumers' information related knowledge and beliefs. *Journal of Direct Marketing,* 6(4), pp. 28-39.

Nurse, J., 2019. *Amazon, Facebook and Google don't need to spy on your conversations to know what you're talking about.* [Online] Available at: https://theconversation.com/amazon-facebook-and-google-dont-need-to-spy-on-your-conversations-to-know-what-youre-talking-about-108792 [Accessed 8 March 2019].

Obar, J. A., 2015. Big data and the phantom public: Walter Lippmann and the fallacy of data self-management. *Big Data & Society,* pp. 1-16.

Obar, J. A. & Oeldorf-Hirsch, A., 2018. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society,* pp. 1-20.

O'Connor, S., 2018. *Millennials poorer than previous generations, data show.* [Online] Available at: https://www.ft.com/content/81343d9e-187b-11e8-9e9c-25c814761640 [Accessed 10 March 2019].

O'Donoghue, T. & Rabin, M., 2000. The economics of immediate gratification. *Journal of Behavioral [sic] Decision Making,* 13(2), pp. 233-250.

Office for National Statistics, 2018. *Crime Survey England and Wales estimates of sexual assault and domestic abuse experienced by adults aged 16 to 59.* [Online] Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/adhocs/

008805crimesurveyenglandandwalesestimatesofsexualassaultanddomesticabuseexperiencedbyadultsaged16to59 [Accessed 30 June 2019].

Olson, J. S., Grudin, J. & Horvitz, E., 2004. *Towards understanding preferences for sharing and privacy,* s.l.: Microsoft Research..

O'Neill, O., 2002. *A question of trust: the BBC Reith lectures 2002.* Cambridge: Cambridge University Press.

Onwuegbuzie, A. J. & Collins, K. M., 2007. A typology of mixed methods sampling designs in social science research. *The Qualitative Report,* 12(2), pp. 281-316.

Paine, C., Reips, U. D., Stieger, S. & Joinson, A., 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies,* 65(6), pp. 526-536.

Pangrazio, L. & Selwyn, N., 2017. *'My data, my bad...' Young people's personal data understandings and (counter) practices.* Toronto, Ontario, Canada, Proceedings of the 8th International Conference on Social Media & Society. ACM Digital Library.

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

Pierson, J., 2012. Online privacy in social media: A conceptual exploration of empowerment and vulnerability. *Communications & Strategies,* 88(4), pp. 99-120.

Preibusch, S., Kübler, D. & Beresford, A. R., 2013. Price versus privacy: An experiment into the competitive advantage of collecting less personal information. *Electronic Commerce Research,* 13(4), pp. 423-455.

Proferes, N., 2017. Information flow solipsism in an explanatory study of beliefs about Twitter. *Social Media+ Society,* 3(1), pp. 1-17.

Rainie, L. & Duggan, M., 2016. *Privacy and Information Sharing,* s.l.: Pew Research Center [sic].

Raynes-Goldie, K. S., 2012. *Privacy in the age of Facebook: Discourse, architecture, consequences.* Doctoral dissertation: Curtin University.

Rodgers, S. & Harris, M. A., 2003. Gender and e-commerce: An exploratory study. *Journal of Advertising Research,* 43(3), pp. 322-329.

Ronson, J., 2015. *So You've Been Publicly Shamed.* London: Picador.

Scholz, T., 2013. Introduction: Why does digital labor matter now?. In: T. Scholz, ed. *Digital Labor: The Internet as Playground and Factory.* Oxon: Routledge.

Sebastianelli, R., Tamimi, N. & Rajan, M., 2008. Perceived quality of online shopping: Does gender make a difference?. *Journal of Internet Commerce,* 7(4), pp. 445-469.

Seneviratne, S., Seneviratne, A., Mohapatra, P. & Mahanti, A., 2014. Your installed apps reveal your gender and more!. *Mobile Computing and Communications Review,* 18(3), pp. 55-61.

Sheehan, K. B., 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviours. *Journal of Interactive Marketing,* 13(4), pp. 24-38.

Sheehan, K. B., 2002. Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society,* 18(1), pp. 21-32.

Shelton, M., Rainie, L. & Madden, M., 2015. *American's privacy strategies post-Snowden,* s.l.: Pew Research Center [sic].

Smythe, D. W., 2012 [1981]. On the Audience Commodity and its Work. In: M. G. Durham & D. M. Kellner, eds. *Media and cultural studies: Keyworks.* Malden: Wiley-Blackwell.

Solove, D., 2007. "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review,* 289(44), pp. 745-772.

Solove, D., 2009. *Understanding Privacy.* London: Harvard University Press.

Solove, D., 2013. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review,* Volume 126, pp. 1880-1903.

Spicer, N., 2016. Combining qualitative and quantitative methods. In: C. Seale, ed. *Researching society and culture.* London: Sage.

Spiekermann, S., Grossklags, J. & Berendt, B., 2001. *E-privacy in second generation E-commerce: privacy preferences versus actual behaviour.* s.l., ACM, pp. 38-47.

Spinello, R. A., 2017 [2003]. *Cyberethics: Morality and Law in Cyberspace.* Massachusetts: Jones and Bartlett Learning.

Starr, C., 1969. Social benefit versus technological risk. *Science,* Volume 165, pp. 1232-1238.

Statista, 2019. *Distribution of Facebook users worldwide as of October 2019, by age and gender.* [Online] Available at: https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/ [Accessed 10 December 2019].

Stoilova, M., Livingstone, S. & Nandagiri, R., 2019a. Children's data and privacy online: growing up in a digital age: research findings. *London School of Economics and Political Science.*

Stoilova, M., Nandagiri, R. & Livingstone, S., 2019b. Children's understanding of personal data and privacy online - a systematic evidence mapping. *Information, Communication and Society,* pp. 1-19.

Stutzman, F., Gross, R. & Acquisti, A., 2012. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy & Confidentiality,* 4(2), pp. 7-41.

Sujon, Z. & Johnston, L., 2017. *Public friends and private sharing: Understanding shifting privacies in sharing culture.* Toronto, ON Canada, SM Society '17.

Swaminathan, V., Lepowska-White, E. & Rao, B. P., 1999. Browsers or buyers in cyberspace? An investigation of factors influencing electronic exchange. *Journal of Computer-Mediated Communication,* 5(2), p. JCMC523.

Tashakkori, A. & Teddlie, C., 2003. The past and future of mixed methods research: from data triangulation to mixed model designs. In: A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and behavioral research.* London: Sage.

Teddlie, C. & Tashakkori, A., 2003. Major issues and controversies in the use of mixed methods in the social and behavioral sciences. In: A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and behavioral research.* London: Sage.

Thaler, R. H. & Sustein, C. R., 2009. *Nudge: Improving Decisions about Health, Wealth and Happiness.* London: Penguin.

The Independent Online, 2018. *Facebook loses a million European users in three months.* [Online] Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/facebook-users-europe-drop-mark-zuckerberg-cambridge-analytica-a8609716.html [Accessed 28 July 2019].

Thelwall, M., 2011. Privacy and gender in the social web. In: S. Trepte & L. Reinecke, eds. *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* Berlin: Springer.

Toffler, A., 1981. *The Third Wave.* London: Pan Books.

Travis, A., 2015. *Investigatory powers bill: the key points.* [Online] Available at: https://www.theguardian.com/world/2015/nov/04/investigatory-powers-bill-the-key-points [Accessed 10 October 2019].

Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A., 2011. The effect of online privacy information on purchasing behavior [sic]: An experimental study. *Information Systems Research,* 22(2), pp. 254-268.

Tufecki, Z., 2008. Can you see me now? Audience disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society,* 28(1), pp. 20-36.

Tufekci, Z., 2015. *Mark Zuckerberg, Let Me Pay for Facebook.* [Online] Available at: https://www.nytimes.com/2015/06/04/opinion/zeynep-tufekci-mark-zuckerberg-let-me-pay-for-facebook.html [Accessed 20 October 2016].

Turow, J., 2003. *Americans and online privacy: The system is broken.* Pennsylvania: Annenberg Public Policy Center of the University of Pennsylvania.

Turow, J., Hennessy, M. & Draper, N., 2015. *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation,* Pennsylvania: Annenberg School for Communications, University of Pennsylvania.

Tversky, A. & Kahneman, D., 1974. Judgement under uncertainty: Heuristics and bias. *Science,* 185(4157), pp. 1124-1131.

Tversky, A. & Kahneman, D., 1982. Judgement under uncertainty: Heuristics and biases. In: D. Kahneman, P. Slovic & A. Tversky, eds. *Judgement under uncertainty: Heuristics and biases.* Cambridge: Cambridge University Press.

Twenge, J., 2014. *Generation me: why today's young Americans are more confident, assertive, entitled - and more miserable than ever before.* New York: Atria Books.

Twenge, J. M., 2017. *iGen: why today's super-connected kids are growing up less rebellious, more tolerant, less happy and completely unprepared for adulthood.* New York: Atria books.

Utz, S. & Krämer, N., 2009. The privacy paradox on social network sites revisited: the role of individual characteristics and group norm. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 3(2).

Van Dijck, J., 2013. *The culture of connectivity: A critical historyof social media.* Oxford: Oxford University Press.

Van Dijck, J., Poell, T. & De Waaal, M., 2018. *The platform society: public values in a connective world.* Oxford: Oxford University Press.

Van Slyke, C., Comunale, C. L. & Belanger, F., 2002. Gender differences in perceptions of web-based shopping. *Association for Computing Machinery. Communications of the ACM,* 45(8), pp. 82-86.

Vertesi, J., 2014. *My Experiment Opting Out of Big Data Made Me Look Like a Criminal.* [Online] Available at: https://time.com/83200/privacy-internet-big-data-opt-out/ [Accessed 6 June 2018].

Vertesi, J., 2015. How Evasion Matters: Implications from Surfacing Data Tracking Online. Interface, 1(1), p.13.. *Interface,* 1(1), pp. 1-14.

Vincent, D., 2016. *Privacy: A Short History.* Cambridge: Polity Press.

Vitak, J., 2012. The impact of context collapse and privacy on social networking site disclosures. *Broadcasting & Electronic Media,* 56(4), pp. 451-470.

Wacks, R., 2016. *Privacy: A Very Short Introduction.* Oxford: Oxford University Press.

Wang, Y. et al., 2013. Do men consult less than women? An analysis of routinely collected UK general practice data. *BMJ Open,* 3(8).

Ward, M., 2017. *It is easy to expose users' secret web habits, say researchers.* [Online] Available at: https://www.bbc.co.uk/news/technology-40770393 [Accessed 8 September 2017].

Weintraub, J., 1997. The theory and politics of the public/private distinction. In: J. Weintraub & K. Kumar, eds. *Public and Private in Thought and Practice.* Chicago: University of Chicago Press.

Westin, A. F., 1970. *Privacy and Freedom.* London: The Bodley Head.

Weyant, J. M. & Smith, S. L., 1987. Getting more by asking for less: The effects of request size on donations of charity. *Journal of Applied Psychology,* 17(4), pp. 392-400.

Wolfe, A., 1997. Public and private in theory and practice: Some implications of an uncertain boundary. In: J. Weintraub & K. Kumar, eds. *Public and Private in Thought and Practice.* Chicago: University of Chicago Press.

Wu, T., 2018. *The Tyranny of Convenience.* [Online] Available at: https://www.nytimes.com/2018/02/16/opinion/sunday/tyranny-convenience.html?action=click&module=RelatedLinks&pgtype=Article [Accessed October 2018].

Young, A. L. & Quan-Haase, A., 2013. Privacy protection strategies on Facebook. *Information, Communication and Society,* 16(4), pp. 479-500.

Zuboff, S., 2015. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology,* Volume 30, pp. 75-89.

Zuboff, S., 2019. *The age of surveillance capitalism: The fight for the future at the new frontier of power.* London: Profile Books.

Appendix A: Participant Information Sheet

Participant information sheet

Thank you for provisionally agreeing to take part in my research. My name is Hayley Evans from the University of Kent. I am carrying out this research as part of my PhD in Sociology, which is looking at how individuals think about privacy when it comes to information about them.

This research has been awarded ethical approval by the SSPSSR Research Ethics Committee at the University of Kent.

Your participation in this research is entirely voluntary, you are under no obligation to take part and can withdraw your participation at any time.

If you agree to take part in this research, you will be asked to attend a one-to-one interview with myself at a location convenient to you. The interview will be audio-recorded and will take approximately an hour to complete.

Your responses will be kept confidential – there will be no one else involved in the transcription of these interviews, which will be stored securely and no one else will have access to the audio recordings (unless required to by law). This research will be published as a thesis at the end of my PhD (in 2018) and I will also present my research findings at various conferences. I also hope to have my research findings published in various academic journals.

If at any point you are uncomfortable with answering a particular question, or discussing a particular topic, please let me know and we can move on to the next section or question. Also, if at any point, you would prefer me to switch off the audio-recording device, I will do so. Equally if you decide that you no longer wish to participate during the interview (or even afterwards), you are completely free to withdraw your participation and do not have to provide me with a reason for this. If you withdraw your consent, I will delete all data you have provided me with.

You will be offered the opportunity to receive a copy of your transcript via e-mail. If you would like to receive this, please provide me with your e-mail address or (at a later date), please e-mail me on the below e-mail address.

To thank you for taking part in my research, once all interviews have been completed, your name will be entered into a prize draw for a £25 iTunes gift card (or equivalent). Please let me know if you do not want to be entered into this draw.

If you have any questions or concerns, please contact me on the below details: Hayley Evans, Cornwallis East, SSPSSR, University of Kent, Canterbury, Kent, CT2 7NF. E-mail address: he91@kent.ac.uk.

Appendix B: Participant Consent Form

Participant consent form

Thank you for agreeing to take part in my research. Please initial next to each statement to indicate that you have read, understood and agree to each statement. Finally, sign and print your name at the bottom of this form to indicate that you consent to participate in this research.

	Initials
I understand that my participation is voluntary	_____
I understand that I can withdraw my participation at any time without having to provide an explanation	_____
I understand that the interview will be audio-recorded and transcribed at a later date	_____
I understand that I will be given a pseudonym for reporting purposes	_____
I have been given a copy of the participant information sheet and have read and understood the information it contains	_____
I understand that I will be entered into a prize draw for a £25 iTunes gift card (or equivalent), I understand that if I do not win, I will be offered no other incentive for my participation	_____
I understand that the results of this research will be reported in a PhD thesis, at various conferences and in academic journals	_____
I understand that responses I have given during the interview may be quoted in a PhD thesis, at various conferences and in academic journals	_____
I have been given the opportunity to ask any questions and these have been answered to my satisfaction	_____

I have been given an adequate amount of time to consider my decision to participate and agree to participate in this research:

Signature:

_____

Name of participant:

_____

(please print)

Date:

_____

Please provide your e-mail address if you would like to be sent a copy of your transcript:

E-mail:

_____

☐ Please tick this box (and provide me with details) if you know someone who may be interested in participating in this research

Appendix C: Interview Schedule

Interview schedule

General info to note:

- **Gender**
- **Age**
- **Social media used?**
- **Own a smartphone?**

1. Are you generally concerned about who has access to or knowledge of your activity on the internet and social media?

2. Do you have any experience around issues of data privacy?
    - If so, what was the issue?

3. Do you consider yourself to be a person who values their privacy?

4. Can you think of an example of when you had to stop and think about your privacy?

5. Do you feel you are in control of your information and who you share it with?

6. Do you think more should be done to protect the privacy of your information?

7. What, if anything, might encourage you to do more to protect your privacy? (i.e. time constraints, technical knowledge).

8. Do you employ any strategies or avoid certain things to retain privacy?

9. Are you concerned about sharing some types of information more than others?

10. How do you feel about the amount of information that you share with companies?

Vignettes
I am now going to talk to you about a number of different scenarios involving various pieces of information that you may share in your day-to-day life. Although the situations I describe may not be something you have personally experienced, I would like you to imagine how you would feel in these scenarios. There are no 'right' answers, I am simply trying to find out how people feel about the privacy of different pieces of information.

Control of image
Claire & Gemma are good friends who used to work together. Claire is a member of a popular social networking site, but Gemma is not. Gemma hosts a small party to which she invites some of her friends (including Claire). After the party, Claire uploads a number of pictures from it to the social networking site. When friends who weren't invited, see the pictures, they are upset with Gemma, who asks Claire not to post pictures of her to the social networking site in future.

1. What is your reaction to this story?
2. In your opinion was Gemma's privacy invaded?

Location information
A well-known technology company is launching a new smartphone app which is said to make users' lives more convenient. The product works like a personal assistant, reminding the user of various important events (such as items to buy, bills to pay, friends'/families' birthdays), as well as integrating various 3rd party apps to help the user be more organised. It uses the individual's location to suggest nearby events and attractions, offer public transport timetables, weather information and directions for onward travel.
The company says that users are able to customise what the app reminds them about, highlighting its convenience.

1. What are your thoughts about a product like this?

Personal information breach
A large dating website has been hacked and customer details published online. The leaked information includes individuals' answers to the website's personality questionnaire as well as private messages and conversations people have had on the site.

1. What is your reaction to this story?

Financial information breach
During the summer of 2015 a large telecoms company's customer database was hacked and various pieces of customer information stolen. Initially the hackers said that they wouldn't release the information if the company paid a large ransom. However, as the company said they couldn't confirm or deny what (if anything) had been stolen, it did not pay the ransom. As a result, the customers' details were released onto the 'Dark-Web'.
Customers were advised to speak to their bank/credit card provider if they noticed any suspicious activity on their account.

1. What is your reaction to this story?

Communication information

A man who previously worked as a contractor for the National Security Agency in the United States has made claims that the UK government has been collecting huge amounts of communications information about all UK citizens. This information includes the content of messages individuals have sent in the form of text messages and/or e-mails. This has been carried out in secret, without anyone being aware of this happening.

The government claims that the collection of information was necessary in order to keep ordinary citizens safe from terrorist threats. The government has argued that those who are not involved in illegal activity have nothing to worry about.

1. What is your reaction to this story?

i. Please rank the scenarios we have discussed from most to least concerning.

ii. Can you think of any further scenarios which you would find particularly concerning?

Appendix D: Survey Questions

General Questions

I would like to start with some questions about the privacy of your data. By this, I mean your ability to maintain control over the information you share with others, either with online companies and organisations or via social networking sites, such as Facebook or Twitter.

How often do you think about your online privacy?

- ○ Whenever I am online
- ○ When an issue arises
- ○ When the media reports on a related issue
- ○ Whenever I am asked for information by an online company or organisation
- ○ Don't know
- ○ Prefer not to say

Have you ever had any of the following issues around the privacy of your information? (Please select all that apply)

- ☐ An email account of mine was hacked
- ☐ A financial account of mine was hacked
- ☐ A social media account of mine was hacked
- ☐ A picture of me was shared online without my knowledge or consent
- ☐ I received unwanted/spam emails
- ☐ I was stalked online
- ☐ Other (please specify)

- [ ] No
- [ ] Don't know
- [ ] Prefer not to say

Sharing data online

In this section, I want you to think about the information that you share online. By this, I mean the information you might share on social networking sites, just as Facebook or Twitter. I want to know about the kinds of things you think about before posting information online.

Do you share personal information on social media? Personal information refers to any details about you as a person which could be used to identify you or express who you are. For example, your place of work or date of birth/birthday.

- ( ) Share on all social media
- ( ) Share on some social media
- ( ) Share where I trust the site
- ( ) Never share
- ( ) Don't know
- ( ) Prefer not to say

Thinking about the social networking site that you use most often, how much personal information do you share? Personal information refers to any details about you as a person which could be used to identify you or express who you are. For example, your place of work or date of birth/birthday.

- ( ) Everything I am asked to share
- ( ) A limited amount of information

- ○ I never share personal information
- ○ Don't know
- ○ Prefer not to say

How much thought do you give to what information you share online before you post something?

- ○ A lot
- ○ Some
- ○ Not very much
- ○ None at all
- ○ Don't know
- ○ Prefer not to say

Do you think about who can see what you share online before posting?

- ○ Yes
- ○ No
- ○ Don't know
- ○ Prefer not to say

Do you take measures to limit who can see what you post online?

- ○ Yes
- ○ No
- ○ Don't know
- ○ Prefer not to say

Which of the following measures (if any) have you employed when using social media in the past to protect your privacy? (Please select all that apply)

- ☐ Read terms and conditions before signing up
- ☐ Supplied false details, such as a fake date of birth or birthday
- ☐ Amended privacy settings to reduce the audience for your posts
- ☐ Refused to save credit card details on the site
- ☐ Periodically went through my list of 'friends' or followers and removed those I no longer want to connect with
- ☐ Set-up audience groups to differentiate between who can see my posts
- ☐ Refused to give consent for data to be shared with linked sites/apps
- ☐ Opted not to check into locations
- ☐ Other (please specify)
- ☐ I haven't taken any action
- ☐ Don't know
- ☐ Prefer not to say

How confident are you that only your intended audience can see your posts?

- ○ Very confident
- ○ Quite confident
- ○ Not very confident
- ○ Not at all confident
- ○ Don't know
- ○ Prefer not to say

What information would you never share online?

Why would you not share the above information?

Collection of data

In this section, I'd like you to think about the information that you are asked to share with online companies and organisations in your daily life. This doesn't need to be a particular online company or organisation, I am interested in how you generally feel about the information that is requested: for example when you are completing a form to open an account.

Overall, how do you feel about the amount of information online companies and organisations collect from you?

- I think the amount of information they collect is reasonable
- I would be happy to share more if they asked me to
- I would not want to share any additional information
- I think the amount of information they collect is unreasonable
- Don't know
- Prefer not to say

Have you ever refused to share a piece of information (such as your mobile phone number or date of birth) with a company?

- Yes
- Why?
- Prefer not to say
- No
- Don't know

- ○ Prefer not to say

Do you ever provide false information to online companies and organisations to keep your privacy?

- ○ Yes
- ○ Why?
- ○ Prefer not to say
- ○ No
- ○ Don't know
- ○ Prefer not to say

If an online company asked you for information that you were uncomfortable with sharing, what would you do?

- ○ Refuse to share the information, even if it meant not using that product/service
- ○ Consider the product/service being offered and weigh-up whether it is worth sharing the information to access it
- ○ Share the information anyway
- ○ Provide false information so that you are still able to use that product/service
- ○ Other (please specify)
- ○ Don’t know
- ○ Prefer not to say

How strongly would you agree or disagree with the following statement? “I accept that online services are more personalised because of the increased access online companies and organisations have to my personal data.”

- ○ Strongly Agree

- ○ Agree
- ○ Disagree
- ○ Strongly disagree
- ○ Don’t know
- ○ Prefer not to say

How strongly would you agree or disagree with the following statement? "I am willing to share some information about myself with online companies and organisations in order to use their services for free."

- ○ Strongly agree
- ○ Agree
- ○ Disagree
- ○ Strongly disagree
- ○ Don't know
- ○ Prefer not to say

How strongly would you agree or disagree with the following statement? "I would be willing to pay more for a service or product if it meant I could share less information."

- ○ Strongly agree
- ○ Agree
- ○ Disagree
- ○ Strongly disagree
- ○ Don't know
- ○ Prefer not to say

Do you think that being particularly concerned about privacy means that you would miss out on useful products or services?

- ○ Yes
- ○ No
- ○ Don't know/Not sure
- ○ Prefer not to say

Control

In this section, the questions are asking you about how much control you feel you have over the information you are asked to share with online companies and organisations, as well as concerns you may have about what could happen if you lost control over your information. By control, I mean your ability to choose which pieces of information you share (or not) with companies, as well as what happens to it after you share it.

Do you feel that you are in control of your data and what it is used for?

- ○ Always
- ○ Often
- ○ Sometimes
- ○ Rarely
- ○ Never
- ○ Don't know
- ○ Prefer not to say

What kinds of data do you feel you have control over? (Please select all that apply).

- [ ] Personal financial data (such as your credit record, salary or taxes)
- [ ] Personal demographic data (such as your date of birth, place of work or where you live)
- [ ] Personal communications data (such as texts or e-mails you have sent or received; any communication that is not intended to be shared publicly)
- [ ] Online behaviour data (such as browsing, searching viewing or purchasing activity on the internet)
- [ ] Social data (such as your social networking profile(s) or status updates, gaming profile, or dating app profile)
- [ ] Medical data (such as your health records, prescription information or test results
- [ ] Other (please specify)
- [ ] I don’t feel I have control over any of my data
- [ ] Don’t know
- [ ] Prefer not to say

Would you like to have more control over your information and who has access to it?

- ○ Yes, I would like to have more control
- ○ No, I have enough control
- ○ I don't care either way
- ○ Don't know
- ○ Prefer not to say

What do you think stops you from having more control?

- ○ I don’t have enough technical knowledge
- ○ It would require a lot of additional time and effort on my part
- ○ Both of the above
- ○ Other (please specify)
- ○ Don’t know
- ○ Prefer not to say

Which of the following statements comes closest to your view of the consequences of your information being hacked?

- ○ It would cause some significant problems
- ○ It would be a minor inconvenience
- ○ Don’t know
- ○ Prefer not to say

Are you worried about your information being passed on or sold to third-parties without your knowledge?

- ○ Yes
  - o What worries you in particular?
- ○ No
- ○ Don’t know
- ○ Prefer not to say

Do you feel that you know enough to be able to fully agree to what happens to your data after you give it to an online company or organisation?

- ○ Yes
- ○ No

- ○ Why not?
- ○ Don't know
- ○ Prefer not to say

Trust

In this section, the questions are asking you to think about the trust you may or may not have in online companies and organisations that you share your information with, including how you believe they should treat your information once you have shared it.

Do you think online companies and organisations currently provide you with enough information about what happens to the data you share with them?

- ○ Yes
- ○ No
- ○ Don't know
- ○ Prefer not to say

Overall, do you believe that outline companies and organisations will keep your information secure?

- ○ Yes - all of the time
- ○ Yes - most of the time
- ○ Some of the time
- ○ No - never
- ○ Don't know
- ○ Prefer not to say

Do you trust online companies and organisations that you share your information with to only use it for the purpose it was collected?

- ○ Yes - all of the time
- ○ Yes - most of the time
- ○ Some of the time
- ○ No - never
- ○ Don't know
- ○ Prefer not to say

Do you trust online companies and organisations that you share your information with not to pass it on to third-parties (unless you have authorised them to do so)?

- ○ Yes - all of the time
- ○ Yes - most of the time
- ○ Some of the time
- ○ No - never
- ○ Don't know
- ○ Prefer not to say

Context

This final section is looking at how you feel about sharing particular pieces of information about yourself. This is in terms of what you generally consider to be the most important information about yourself. It is also asking you to think about which groups or individuals in particular you would have concerns over knowing specific information about you.

Can you think of any particular situations in which you are especially concerned about your privacy?

- ○ Yes
    - When?
    - Why?
- ○ Prefer not to say
- ○ No
- ○ Don't know
- ○ Prefer not to say

Thinking about your personal financial data please state how concerned you would be about it being shared with each of the potential 'audiences' by selecting the radio button under the number which corresponds with your level of concern. Personal financial data refers to information such as your credit record, salary or taxes. (1- Not at all concerned – 5-Extremely concerned)

	0 Unsure	**1**	**2**	**3**	**4**	**5**
Spouse:	❍	❍	❍	❍	❍	❍
Immediate family:	❍	❍	❍	❍	❍	❍
Friends:	❍	❍	❍	❍	❍	❍
Neighbours:	❍	❍	❍	❍	❍	❍
Work colleague/employer:	❍	❍	❍	❍	❍	❍
Stranger:	❍	❍	❍	❍	❍	❍
3rd party online companies and organisations*:	❍	❍	❍	❍	❍	❍
The Government/police:	❍	❍	❍	❍	❍	❍

*By 3rd party company, I am referring to online companies and organisations you have not directly shared your information with.

Thinking about your personal demographic data please state how concerned you would be about it being shared with each of the potential 'audiences' by selecting the radio button under the number which corresponds with your level of concern. Personal demographic data refers to information such as your date of birth, place of work or where you live.

	0 Unsure	**1**	**2**	**3**	**4**	**5**
Spouse:	❍	❍	❍	❍	❍	❍
Immediate family:	❍	❍	❍	❍	❍	❍
Friends:	❍	❍	❍	❍	❍	❍
Neighbours:	❍	❍	❍	❍	❍	❍
Work colleague/employer:	❍	❍	❍	❍	❍	❍
Stranger:	❍	❍	❍	❍	❍	❍
3rd party online companies and organisations*:	❍	❍	❍	❍	❍	❍
The Government/police:	❍	❍	❍	❍	❍	❍

*By 3rd party company, I am referring to online companies and organisations you have not directly shared your information with.

Thinking about your personal communications data please state how concerned you would be about it being shared with each of the potential 'audiences' by selecting the radio button under the number which corresponds with your level of concern.

Personal communications data refers to information such as texts or e-mails you have sent or received; any communication that is not intended to be shared publicly.

	0 Unsure	**1**	**2**	**3**	**4**	**5**
Spouse:	❍	❍	❍	❍	❍	❍
Immediate family:	❍	❍	❍	❍	❍	❍
Friends:	❍	❍	❍	❍	❍	❍
Neighbours:	❍	❍	❍	❍	❍	❍
Work colleague/employer:	❍	❍	❍	❍	❍	❍
Stranger:	❍	❍	❍	❍	❍	❍
3rd party online companies and organisations*:	❍	❍	❍	❍	❍	❍
The Government/police:	❍	❍	❍	❍	❍	❍

*By 3rd party company, I am referring to online companies and organisations you have not directly shared your information with.

Thinking about your online behaviour data please state how concerned you would be about it being shared with each of the potential 'audiences' by selecting the radio button under the number which corresponds with your level of concern. Online behaviour data refers to information such as browsing, searching, viewing or purchasing activity on the internet.

	0 Unsure	**1**	**2**	**3**	**4**	**5**
Spouse:	❍	❍	❍	❍	❍	❍
Immediate family:	❍	❍	❍	❍	❍	❍
Friends:	❍	❍	❍	❍	❍	❍
Neighbours:	❍	❍	❍	❍	❍	❍
Work colleague/employer:	❍	❍	❍	❍	❍	❍
Stranger:	❍	❍	❍	❍	❍	❍
3rd party online companies and organisations*:	❍	❍	❍	❍	❍	❍
The Government/police:	❍	❍	❍	❍	❍	❍

*By 3rd party company, I am referring to online companies and organisations you have not directly shared your information with.

Thinking about your social data please state how concerned you would be about it being shared with each of the potential 'audiences' by selecting the radio button under the number which corresponds with your level of concern.

Social data refers to information such as your social networking profile(s) or status updates, gaming profile, or dating app profile.

	0 Unsure	**1**	**2**	**3**	**4**	**5**
Spouse:	❍	❍	❍	❍	❍	❍
Immediate family:	❍	❍	❍	❍	❍	❍
Friends:	❍	❍	❍	❍	❍	❍
Neighbours:	❍	❍	❍	❍	❍	❍
Work colleague/employer:	❍	❍	❍	❍	❍	❍
Stranger:	❍	❍	❍	❍	❍	❍
3rd party online companies and organisations*:	❍	❍	❍	❍	❍	❍
The Government/police:	❍	❍	❍	❍	❍	❍

*By 3rd party company, I am referring to online companies and organisations you have not directly shared your information with.

Thinking about your medical data please state how concerned you would be about it being shared with each of the potential 'audiences' by selecting the radio button under the number which corresponds with your level of concern. Medical data refers to information such as your health records, prescription information or test results.

	0 Unsure	**1**	**2**	**3**	**4**	**5**
Spouse:	❍	❍	❍	❍	❍	❍
Immediate family:	❍	❍	❍	❍	❍	❍
Friends:	❍	❍	❍	❍	❍	❍
Neighbours:	❍	❍	❍	❍	❍	❍
Work colleague/employer:	❍	❍	❍	❍	❍	❍
Stranger:	❍	❍	❍	❍	❍	❍
3rd party online companies and organisations*:	❍	❍	❍	❍	❍	❍
The Government/police:	❍	❍	❍	❍	❍	❍

*By 3rd party company, I am referring to online companies and organisations you have not directly shared your information with.

Demographic questions

This section asks questions about you. The information is needed to help in the analysis of the survey responses. The information you share here will not be used to personally identify you and will not be shared with anyone else. If you are not comfortable answering a particular question, please select the 'Prefer not to say' option before moving on to the next question.

What is your gender?

- ○ Female
- ○ Male
- ○ Non-binary/third gender
- ○ Prefer to self-describe (please state)

What is your age?

- ○ 20-24
- ○ 25-29
- ○ 30-34
- ○ 35-39
- ○ Prefer not to say

What is the highest level of education you have completed? If you are currently studying, please select the highest qualification that you have completed.

- ○ No schooling
- ○ Finished secondary school, no GCSEs/vocational qualifications
- ○ GCSEs/Vocational qualifications
- ○ 6th form/A levels
- ○ Undergraduate degree
- ○ Master's degree

- ○ Professional degree
- ○ PhD
- ○ Prefer not to say

Which social networking sites do you use at least once a week? (Pleas select all that apply)

- ☐ Facebook
- ☐ Twitter
- ☐ Instagram
- ☐ LinkedIn
- ☐ Pinterest
- ☐ Flickr
- ☐ WhatsApp
- ☐ Snapchat
- ☐ YouTube
- ☐ Other (please specify)
- ☐ Prefer not to say

Where did you hear about this survey?

- ○ Post on Facebook
- ○ Post on Twitter
- ○ Forwarded survey information in an e-mail
- ○ Other (please specify)
- ○ Can't remember
- ○ Prefer not to say

Thank you for participating in this survey. If you would like to be entered into a prize drawer for a £25 iTunes voucher (or equivalent), please enter your e-mail

address in the box below. Please note, your e-mail address will not be linked with any of your responses.

Survey Powered By Qualtrics