Bournemouth
University

I declare that this dissertation/project is all my own work and the sources of information and the material I have used (including the internet) have been fully identified and properly acknowledged as required in the guidelines given in the student handbook I have received.

Student signature ……………………………………………

Date …………………………………………………………..

To what extent may the public undervalue their personal data at a cost to privacy?

BA (Hons) Digital Media Design

2014-2017

Media Academic Group

Bournemouth Media School

Word Count: 9786

Abstract

There is no question that mass surveillance by governments and businesses is invading the privacy of people worldwide. The growth in personal data collection and the ubiquity of algorithmic surveillance is an increasing issue in modern societies, as the Big Data theory encourages collection of all data, even if usefulness is not yet clear. This dissertation critically analyses the effects this has on individual liberties and freedoms, whilst focusing on this question: *Why and to what extent does the public neglect or undervalue their personal data at a cost to privacy?* The dissertation centres on the collection and analysis of email interviews from experts that work in legal and technology sectors. In doing so, the study was focused on online communications due to the pervasiveness of social media. Importantly, the enquiry follows a form of logic, where the study proceeded from initial observation and the identification of patterns within the data to the development of a tentative theory. What was established is that scenario planning for security measures in the future is becoming increasingly difficult, due to the speed with which things are changing and that the ability of being able to imagine long term consequences has faded. I conclude that the complex and uncertain world today is around the issue of a new temporality, where it is as though time seems to have shrunk to an ‘eternal now’ and it is only at a certain critical point when society realises just how much freedom and personal data they have given away.

Acknowledgements

I would first and foremost like to thank my tutor Simon Perkins for the help and support he has given to me throughout the course of this dissertation. I much appreciate the time you have dedicated to me and the many long conversations that have been filled with knowledge and guidance.

I would also like to thank the participants who took part in the study and helped me achieve a more thorough investigation.

Finally, I would like to thank Elyssa Whyte-Baker, Josh Faull, Alex Miller, Taylan Siseci and Calum Sagar for their support, encouragement and positivity that have given me the determination to complete this dissertation.

Contents Page

Introduction

There is no question that mass surveillance by businesses and governments is invading the privacy of innocent people worldwide (Timm 2014). There has been a rapid growth in collecting personal data and the ubiquity of algorithmic surveillance, which is an increasing issue in modern societies. This paper will critically analyse the effects this has on individual liberties and freedoms, within modern democratic societies, online today. The longitudinal study led by the Pew Research Center showed that American perceptions of privacy and surveillance has changed, since the Snowden revelations (Madden 2014). As a result, this is significant – both in the northern American context, as well as contexts such as the UK. It is significant because it points to a shift away from traditional perspectives around freedom and risk. This is exemplified by the notion of the '*Risk Society'* (Beck and Ritter 1992), in understanding around privacy and surveillance in the post Snowden era, or what Michael Seemann calls '*Kontrollverlust'* that translates to the '*loss of control'* (Seemann 2014).

The dissertation aims to critically understand common conceptions around the monitoring of personal data and its interpretation by state and corporate agencies. In doing so, the study focuses on online communications within the context of the UK because of its commonly recognised impact on society's daily lives, due to the pervasiveness of social media. It will also explore the impact data monitoring may have on individuals. Another aim is to scrutinise the nature of society that the public live in today and explore the ways in which the public's freedom to act and express themselves online may be constrained. What is argued is that there is a sense of a new temporality; the new way people have today of experiencing time, where it is as though the way things are changing has sped up. One of the key debates that will inform this dissertation is; if privacy can longer be controlled by current technologies and policies, and conflicts between using personal data for the purposes of creating meaningful and efficient services for consumers vs. using personal data to exploit consumers as a means for financial gain are growing – is this really the best way to protect citizens within a country at a cost to human rights, safety and privacy? The concepts that will be reviewed within the literature review are: *big data*, *the irretrievable loss of privacy*, *the era of the query* and *filter bubbles*. Key themes and relevant discussions will be investigated in order to inform this dissertation on public identity, the effects that undervaluing personal data can have and a technological change in society can have.

Perceptions of privacy can vary, but ultimately it is conceived as doing something in either cyber-space or in the real world. Whether it is reading a book, listening to music, messaging or having a conversation with somebody, viewing content or just doing banking arrangements, people like to have some kind of barrier between them and external forces. Forming this notion of barrier creates a sense of curiosity from external sources (humans or automated computer systems). Wherever they appear, people try to break barriers down. For example, the Berlin wall successfully was, the Israeli's West Bank barrier is in constant threat from the Palestinians and United State's President Donald Trump's proposition to build a wall between Mexico is also getting enormous criticism. Society simply does not like barriers, so people will always try to find a way to go over it, under it or penetrate through it. It is important to consider that no barriers are one hundred percent permeable and are always prone to be under threat. The first instance within modern eras of the destruction of global barriers was the creation of the Internet.

Chapter One: Literature Review

There were particularly beneficial readings that informed the secondary research of this dissertation. In the light of Edward Snowden's revelations in 2013, various concepts have been brought to the public eye more. Reviews have been organised accordingly to a series of conceptual categories due to the relevance of these concepts and the relationships between them, as they relate to the central thesis of the dissertation. The concepts that will be critically analysed within this literature review are:

- Big Data
- The irretrievable loss of privacy
- Era of the query
- Filter bubbles

1.1 Big Data

The big data theory suggests "an ephemeral and seemingly endless storage space" (Niederer and Taudin Chabot 2015). It drives a range of benefits from innovative business to new ways to treat diseases. Automated practises arise from it such as data analytics. Conflicts between privacy and new technology occur since various technologies collect so much data and analyses them so efficiently. A report written to Barak Obama, the former President of the United States of America, by his council of advisors on science and technology informs the analysis of big-data implications for policy and the need for preserving privacy. Within this report Holdren and Lander addressed:

> "The ubiquity of computing and electronic communication technologies has led to the exponential growth of data from both digital and analog sources. New capabilities to gather, analyze, disseminate, and preserve vast quantities of data raise new concerns about the nature of privacy and the means by which individual privacy might be compromised or protected" (Holdren and Lander 2014).

Vast amounts of personal data play in the hands of the public and private sector, such as economists, computer scientists, mathematicians, political scientists, sociologists and others. Various diverse industries demand access to extensively exceeding quantities of information produced by and about people and their interactions with things. The volume of individuals that are having data collected about them is extensive and one where the individual loses a part of their intentionality. The data gathered from individuals is enormous and are ones which an individual intentionally enters. As the Internet of Things (IOT) continues to grow at a rapid pace from: email, text messaging, input via mouse-clicks, taps, swipes, to social media interactions, health records, phone logs and other digital traces left by people, the implications of this theory begin to appear significant. One being the possibility for wide-spread compromising of personal data. As cited in the journal Information, Communication and Society, the authors express concern that Big Data is a socio-technical phenomenon:

> "Will large-scale search data help us create better tools, services, and public goods? Or will it usher in a new wave of privacy incursions and invasive marketing? Will data analytics help us understand online communities and political movements? Or will it be used to track protesters and suppress speech? Will it transform how we study human communication and culture, or narrow the palette of research options and alter what 'research' means?" (Boyd and Crawford 2012).

It is apparent that there is scepticism surrounding big data since there seems to be extreme amounts of uncertainty and no end to it. It drives an increasing ethical issue in society today that is privacy. The conflict between privacy, personalisation and innovation is ongoing, but unethical issues emerge if people are unaware that their data is being analysed and disseminated. However, for 'data enthusiasts' privacy risks are considered mere "afterthoughts" in the pursuit of complete information (Polonetsky and Tene 2013), which compounds challenges to public policy.

It is widely held that Facebook's growth is due in part of big data, as well as all the other big systems that dominate the Internet, such as YouTube, Twitter and Google. While the organisation Facebook helps connect people worldwide, it has become a producer of big data and will continue to fuel its growth. Algorithms are relied on by Facebook and other social media to continuously identify connections between users and select types of posts that will be more visible in newsfeeds than others. One of the algorithms that is used by Facebook is called EdgeRank. Information used by this algorithm is gleaned from users to potentially connect them with others of similar interest, guiding the presentation of information accordingly to each individual's interests (Bucher 2012), and of course to publish ads. It could be argued that Facebook has become one of the world's largest repositories of personal data, which has an increasing range of potential uses (McCracken 2015). That is why it is paramount to monetise data in a social network because what is deemed not useful data in the present could be useful for the future.

The concept of big data also forms a broader emphasis in its role in society today. The Snowden revelations in 2013 disclosed that government programmes have been designed to mass collect data, not only from domestic citizens, but around the world (Greenwald 2013). Engagements with digital infrastructures, such as everything from a mouse click and communication, to how long somebody stays on a web page for indicates the extent to which contemporary forms of governance are increasingly based on the ability to monitor, track and potentially predict the behaviour of entire populations (Dencik, Hintz and Cable 2016). Professor Lyon argued (2015) a surveillance society emerged from the intensified security surveillance that followed the 11 September 2001 and the "so-called war on terror" (Lyon 2015). Such uncertainty of threats justifies profusely the necessity of such monitoring of data.

The problem with big data is that data is being generated at such a rate by consumers, companies and government agencies. It currently exceeds technological capabilities to accurately capture, process, store and analyse data for any meaningful insight, in a reasonable amount of time. Society can no longer depend on technology alone to address the varying challenges that big data brings. The right to privacy raises questions about who is in ownership of data? Another is, what are the systems entitled to do with the data, which ubiquitously monitors society online? The Internet increasingly permits the public to live their lives publically in cyber-space. Facebook and Twitter are two prime examples for encouraging this phenomenon. It is important for individuals to consider that any person, company or agency worldwide can watch and observe them, whether they want them to or not. Security is another challenge to big data since opportunities for breaching data grows with it, either by organisations or cyber criminals (Sadowski 2016). Trust and ethics could also be considered significant challenges to big data because they are at the essence of privacy, and is what upkeeps data infrastructures between users and businesses.

Transparency is crucial and righteous for people in society in order for them to understand what decisions are being made about them, how algorithms work and what data specifically is being used. Treating privacy as a UK issue ignores the global reach of technology companies and policies, since the Internet is extremely vast and belongs to no geographic borders.

1.2 Irretrievable loss of privacy

Concerns about privacy and state surveillance kindles many interesting and challenging debates that revolve around the problems and difficulties that German sociologist Ulrich Beck calls '*second modernity'* (Beck and Ritter 1992) or what Michael Seemann is calling *kontrollverlust (the loss of control)* (Seemann 2014). *Digital Tailspin: Ten Rules for the Internet After Snowden* is a publication written by the author Michael Seemann that examines how information is retrieved in the '*new game*' where it is free flowing without borders and with no gatekeepers (Seemann 2014, p.25-27). The book also presented ideas that explored the nature of society in technologically advanced parts of the world. It argued a concept that I had not considered before: *the irretrievable loss of privacy*.

This is Seeman's proposition which is a profoundly controversial thesis, particularly in Germany. What underlies so much of the distrust, that the German state has got over surveillance, is the whole notion of privacy (Seemann 2014, p.10). Consequently, Germany has the strictest data protection laws in the world (Gabel 2014). This relates back to the time of the communist regime in East Germany, which was very much a surveillance based state. Though it was not the kind of surveillance that societies embrace now – where every single mouse click is instantly traceable. The very nature of surveillance was dissimilar based on huge numbers of the population being part of the Stasi (the European secret police). During this period, everything from career prospects to even one's fate could be changed due to friends or even family reporting back about their behaviour, which essentially created an atmosphere of paranoia. Hence, that notion of a surveillance society and resistance to it is profoundly embedded in the German Democratic Republic (GDR). Thus, a degree of fear of that has made the German population somewhat allergic towards any form of state surveillance whatsoever. However, the level of trust that a democratic population of any given country has towards its government varies. Indeed, this applies to both public and private sectors in these countries as well. Some countries are completely relaxed about the Snowden revelations of worldwide mass surveillance through the National Security Agency (NSA). In other parts of the world, particularly those that previously had a big dominance of state surveillance, are far more paranoid about that and that includes Germany. Trust is an issue that has a profound effect on how individual citizens look at this issue of control, via information gathering.

Nassim Taleb's theory contained in his book The Black Swan, describes the impact of the highly improbable (Taleb 2007). It can be applied to understand how and why society is always trying to predict the future and how we are living in a world where there is radical uncertainty. It is a theory that can be used to understand this '*new game*' that we have transitioned in to, whereby a sincere sense of *kontrollverlust* is apparent (Seemann 2014). According to Taleb, *black swans* comprise of three attributes: 1) rarity 2) extreme impact 3) retrospective predictability (Taleb 2007). The *black swan* is a metaphor that illustrates the period when before the British arrived in Australia for the first time, it was believed that swans could only be white. When they arrived at this new country (new world) they realised that their whole observation of the world had changed. To understand this '*new game*' (Seemann 2014), society must now "sink their ships" to leave behind the knowledge they once knew.

Ulrich Beck coined the term '*The Risk Society*'. His proposition was that in the first era of modernity, the Industrial Revolution, you had a society which was very much based around calculable risk – the idea of probabilities; which is based around the fact that although individual risk and life chances cannot be calculable, if that is aggregated to large numbers then conclusions can be drawn. This means that risk overall is calculable (Beck and Ritter 1992). What has happened in industrial society since however, is the idea that risk can ultimately be controlled by science and rationality, and that is something upon which all democratic societies have been based. What Beck suggested was that *second modernity* (the second revolution of modern society) had materialised (Beck and Ritter 1992). This is when modernity starts to modernise itself and the world turns to be ever more complex and reflexive, where the systems that inhabit it also become the danger as well as the solution. The concerns and difficulties that are involved with *second modernity* are becoming increasingly problematic, as online privacy can no longer be controlled by science and rationality as well as the current technologies that society have today, which some may view as traditional as they are compounded by challenges to privacy (Holdren and Lander 2014). Total surveillance and the concept of *filter bubbles* and *big data*, broadly speaking, underlie the problematic issues that affect an individual's privacy online. Exactly how society is being surveilled and the ubiquity of it are of huge concern. It has changed and transformed exponentially since the first era of modernity; the industrial revolution, with the rapid and overwhelming surge of using digital technologies such as smartphones and the Internet.

We can see the concept of *the irretrievable loss of privacy* materialising around society, wherever it is in the world due to law and policies put forth by Governments, typically after the programs and systems have already been built and implemented in to it in the first place. If we consider the USA, since 2001 the surveillance program PRISM, constructed by the NSA, has been running under section 215 of the Patriot Act. It later expanded to include the Foreign Intelligence Surveillance Act (FISA), which permits warrantless 'wire-tapping' when given permission by the secret FISA court (Ackerman 2016). Standing highly controversial, personal data can be accessed on request from companies such as Google, Facebook, Yahoo and Apple amongst others. XKeyscore is also an NSA tool that collects "nearly everything a user does on the internet daily" by analysing global Internet traffic (Greenwald 2013). Its components are incorporated in Tempora – a formerly secret computer system used by the British Government Communications Headquarters (GCHQ), which taps fibre-optic cables to access vast quantities of global communications networks, such as: email messages, Facebook posts, Internet histories and calls (MacAskill et al. 2013). GCHQ also developed a range of tools named the "Smurf Suite" that can turn a phone on or off, activate its hot mic and even the geo-location with much greater precision than the triangulation of telephone towers, regardless if it is even switched on or off (Taylor 2015). Furthermore, the UK have arguably legalised the most extreme surveillance in western democracy, passing the very recent Investigatory Powers Bill in November 2016 (MacAskill 2016). Some of its requirements are that by law phone and web companies must store records of every citizen for 12 months, as well as the security services to collect large volumes of personal communications data and to hack into and bug computers. If the surveillance programs that we are a part of not keeping us safe and are making us miss vital connections between information we already have – such as the terrorist Paris attacks in 2015 or the new year's eve Turkey night club shooting in 2016 – is this really the best way to protect Citizens within a country at a cost to human rights, safety and privacy?

This concept of *the irretrievable loss of privacy* interested me to further read in to the ethics of computer algorithmic surveillance. It led me to consider a report on personal data where it states that Governments, corporations, institutions and various groups globally are accumulating extensive amounts of personal data about individuals, with minimal concern for it (Haddadi et al. 2015, pp.1-5).

1.3 Era of the query

In the chapter: *Knowing Is Asking the Right Questions*, Seemann's concept of civil societies hypothetically living in the *era of the query* rationalises the behaviour of individuals and the actions that they participate in online. The concept attempts to encourage one to think about how much of their personality and their life is determined by the queries they make. It offers an interesting insight in to the nature of the public, since the proposition that the author is putting here is we should "start to think of audiences differently to the public" (Seemann

2014, pp.25-27). One may express that the query is a form of surveillance, which this dissertation describes as the ubiquitous eye, due to the increase in pattern recognition and algorithmic surveillance. It is also central as a means of structuring content in the *new game*, as the way users experience content today is through asking questions and generating queries. The Internet created this shift in how information flows and how it is received, where there are no borders nor gatekeepers to control the flow of information, which was present in the *old game* (Pariser 2011).

The thesis authored by Lincoln Dahlberg helped me to understand the historical context of the public sphere. Living within a democracy requires society to continuously consider the public. It is a continuous process generated through what is deemed public opinion. Yet, the public is a strange phenomenon and is a bit amorphous. Its identity is not as clearly defined and rooted in modern democracy as one might think (Dahlberg 2000). Politicians, amongst others across an array of diverse industries, are constantly having to balance their decision-making processes against the notion of public opinion. One might question how does a society determine what public opinion is? According to Dahlberg (2000), modern democracies must be incredibly respectful of the public (Dahlberg 2000). It is a powerful force that is susceptible to explode now and again, which politicians and legislators must deal with and they never know where it is going to come from. These explosions are liable to be issue driven and issues create publics. Looking at how privacy issues appear shows how particular issues can mobilise publics, which are capable of triggering and shaping democratic decision-making processes (Berg-Larsen 2015).

Web tracking is an issue that is profoundly embedded in all societies. Especially in Dutch society. A journal article authored by Lonneke van der Velden reviews a range of ‘privacy enhancing’ tools that can track Web tracking networks (van der Velden 2014, pp.195-213). A research group called Digital Methods, whom are based in Amsterdam, specialise in creating software packages, amongst other things, that tracks the trackers (Rogers 2016). These tools track issue networks and they see the way that publics emerge from them. It aims to help users assess their trust with different networks as well as offering transparency that is open source. This notion of societies today, being in the *era of the query*, means that publics are identified and collated through the questions they ask, either to each other or to search engines and other online platforms. Nonetheless, queries come together aggregated and shape political opinion (Scott and Kosslyn 2015, pp.2). New technologies and systems across the board are frequently employed to evaluate who individuals are or what various groups they fit in to, so that they can be monitorised, controlled or influenced in some political discussion.

There is an American artist called Evan Roth who’s work intends to engage the audience with larger issues of technology “through a veneer of light hearted irreverence” (Popovich 2013). He concisely draws attention to how the nature of the public, of any given state, has changed in the *era of the query*, or what may be described as the *era of ubiquitous enquiry*. Google now thinks that Roth is the biggest “bad ass mother fucker” by a process that he set in motion, yet does not control. It is automated via Search Engine Optimisation (SEO). What Roth did was illustrate how algorithm processes are being automated via a set of instructions; by handing out business cards that show the expression “bad ass mother fucker” typed in to Google’s search field, with the mouse hovering over the search function *I’m Feeling Lucky*. Now, he is populated at the very top of Google’s search results when somebody queries for a “bad ass mother fucker”, and the more people that follow the instructions to look this up, the more intimately Roth’s name becomes linked to the phrase in Google’s algorithms, which are then linked to his website. His own profile and his attribution as being a “bad ass mother fucker” is continually being reinforced, not by himself, but by the public and the audience that is created by this process that he sets in motion, but then does not control. What is most interesting is the fact that Roth does not participate in this process of attribution himself for it is automated. Google’s algorithm via the searcher is a connection that becomes one, which needs to be maintained and continually reanimated. Others are meant to perform a particular Google search, thereby feasibly fabricating the particular reality themselves. People are making their own reality through the searches they make. Roth's work is a reflection on society – the audience. Not on him – the artist.

This is a new and highly specific notion of the public domain. It is entirely different from the publics of the past such as those that began in ancient Greek democracies; this notion of people speaking out and having some kind of control over discourse, parading themselves in the streets, speaking in parliament or standing on Speaker's corner. This is a notion of the public that emerges through the questions that people ask the search engines. This is the *era of the query.*

1.4 Filter bubbles

Filter bubbles are a concept that was coined by Eli Pariser in his book *The Filter Bubble: What the Internet is Hiding From You*. The author goes in to great depths examining this concept, whereby online digital filtering mechanisms limit a user's exposure to potential attitude-challenging information. This has been shown to lead to adopting more extreme attitudes over time and misperceiving facts about current events. His concern is that an individual's notion of reality is increasingly directed by algorithmically determined content (Pariser 2011). He cites Google and Facebook as some of the primary offenders in the filter bubble phenomenon. He further notes that Facebook users are increasingly exposed to less and less ideologically opposing narratives within their news feed, and that Google's search engine uses fifty-seven attributes to customise a user's search results, based on their search history and "everything from what kind of computer you're on to what kind of browser you're using to where you're located" (Pariser 2011). The idea is that the *filter bubble* locks an individual in to filtering mechanisms. Roth's work, that was mentioned formerly in the concept of the *era of the query*; where individuals shape their reality themselves through the searches they make, is often why people are very concerned about societies' ever growing reality of politics being digested via social media, since individuals online are exposed to people with whom they naturally agree with. Instead of having discussions with others who hold opposing world views, which is the essence of democracy, what society is effectively doing is perpetuating self-reinforcing-echo-chambers (Seemann 2014). This is a notion often considered as social sorting, where versions of opinion and ideas are recycled back to oneself, insulating them from alternate perspectives. For example, this concept was used as a way of understanding the outcome from both perspectives of the recent UK EU referendum and the US Presidential election (Flaxman, Goel and Rao 2016, pp.298-320).

However, there has been some evidence that calls in to question the concept of the filter bubble phenomenon. In 2016, Facebook published a paper that concluded that individual users had a significantly more impact on "limiting exposure to cross-cutting content" than "algorithmic ranking" (Bakshy, Messing and Adamic 2015, pp.1130-1132). However, this paper has been widely criticised by data scientists who examined the study. Professor Zeynep Tufekci of the University of North Carolina, Chapel Hill, closely examined the study and found that:

> "The research was conducted on a small, skewed subset of Facebook users who chose to self-identify their political affiliation on Facebook and regularly log on to Facebook, about ~4% of the population available for the study. This is super important because this sampling confounds the dependent variable" (Tufekci 2015).

Consequently, what should be discussion simply becomes assertion with no possibility of reaching compromise, and this can be noticed in many countries today. In an environment where people are increasingly becoming more isolated ideologically and informatively, due to the 'filter bubble effect', the range of negative impact on society can be vast and far reaching, from cultural fragmentation to the undermining of a nation's entire democratic process.

It may be argued that the public tends to forget or may not even know the detail of profiling that exists around individuals and how individual profiles are being articulated at such a fine grain level of detail. Pariser notes in a Ted Talk that no two people would ever get the same list of results in Google for the same query (Pariser 2011). One might contemplate their differences between them as individuals, in both reality and in the way that they are perceived by the network. Therefore, each member of society lives in their own unique universe of the *filter bubble*. They are designed by engineers from big systems companies who have their own agendas (often that of financial gain). Seemann (2014) believes that in today's world filters are so significant because they control to a huge extent the way in which people are perceived by forces that have enormous power over their lives (Seemann 2014).

There are many ways of interpreting this process of individualisation and some create polarised opinions. It could be considered emancipatory, where members of society are no longer the victims of one monolithic mass medium that tells everybody what to think collectively. Thus, it could be argued that members of all societies have been recognised by the machines as individuals and their individualities being responded to and shaped. On the contrary however, it could be considered an erosion of the collective shared conversation that is democracy. That is what makes this era so challenging and why it is so important for society to consider that if one surrenders the sovereignty of its filers, then it subsequently risks living in an Orwellian world.

Together, these four concepts hypothetically underpin the nature of society in today's world inside the UK, and the effects they have on it. The state of it before and currently in the present has been addressed to understand what it transitioned from, when society could manage risk, to today where the flow of data within its environment are becoming increasingly out of control and the number of unpredictabilities has increased. Hence, Seemann's (2014) notion of the *digital tailspin* (Seemann 2014). Moore's law is the observation that the processing power of computers double each year (Brock and Moore 2006). Therefore, it could be argued that the uncertainties about preserving privacy increases with it.

Chapter Two: Methodology and Research Methods

2.1 Methodology

This dissertation follows a social science model centring on the collection and analysis of primary research data relating to public perceptions of privacy and surveillance within the UK. The thesis is supported through a literature review of secondary data derived from publically available discussions online, as well as key journals and news articles on the topic. Importantly, the enquiry followed an inductive reasoning logic, where the study proceeded from initial observation and the identification of patterns within the data to the development of a tentative theory. The study focused on the UK context of public perceptions around privacy and surveillance, as one major poll suggests they are anticipated to have changed after the Edward Snowden revelations (Madden 2014). Additionally, because of the wide-ranging scope of the original Pew Research Center's report and because of the limitations of undertaking work of this scope as an undergraduate student, I chose to focus the enquiry around the specific issue of undervaluing data. The research method of email interviews had been chosen for the gathering of primary data. In doing so, questions were framed around discovering answers to the following dissertation research question: *To what extent may the public undervalue their personal data at a cost to privacy?*

2.2 Approach to sampling and selection

Purposive sampling was be used as my primary means of focusing the data collection process. This decision was made to limit the scope of the interview topics through ensuring that only respondents who have particular insight about the topic area are interviewed. This is in contrast with other sampling methods such as 'random sampling' for example, which is designed to provide much broader and generally much less focused perspectives. The research uses the '*expert sampling'* (the purposive sampling variant) to evaluate the perceptions of privacy and surveillance from members of the public, that work in the technology sector and areas involved in policy and legislative measures. This is the best way to elicit the views of persons who have specific expertise in these fields and understand the possible different ways members of the public may undervalue their personal data, at a cost to privacy. During the exploratory phase, this type of sampling formed the basis of my research as it requires a focus on individuals with particular expertise. Qualitative primary research was employed for the study as Miles and Huberman's book (1994) suggests qualitative data analysis is not merely a method for analysing and displaying qualitative data, but for reflecting insights into a social science led project (Miles and Huberman 1994, p.329). This dissertation aims to gain an understanding of the underlying reasons, opinions and motivations for undervaluing personal data, in the public sense and reveal potential consequences for doing so. Questions for each respondent were structured so that they move from the more general to the specific, in terms of the way that they attend to the research focus of the dissertation. Refer to Appendix A for details. The responses received have been critically analysed in the research findings and the varying issues that were addressed in the study have been reviewed accordingly.

Chapter 3: Research Findings

This dissertation began with the question: To what extent may the public undervalue their personal data at a cost to privacy? The study in to this enquiry does not present any straight forward answers. It proceeds from initial observation and the identification of patterns within the opinions, insights and social media experiences from experts of industry, to the development of a tentative theory. The analysis will discuss the most relevant results in the data collected to shed light on perceptions of privacy and the impact data monitoring can have on individuals. Underlying themes do reoccur that appear to influence and link to a changing temporality and nature of society.

The primary focus of this research has been based around the way the public relate with their personal data. The Black Swan theory provides instances of events that brought about unpredictable change and radical uncertainty (Taleb 2007). There is a correlation between the Black Swan theory and the fear of the potential consequences that undervaluing personal data may have. The questions for each of the respondents are structured so that they move from the more general to the specific, in terms of the way that they attend to the research focus of the dissertation. Refer to Appendix A for details. In doing so, the more general questions are designed to develop understanding about the context of the problem being addressed in the research, while the specific questions aim to reveal insights about particular cases. The questions are designed to discover insight about societal perceptions of security and privacy, through the lens of industry professionals who work in the technology sector and areas involved in policy and legislative measures. In doing this, the questions had objectives and these issues were addressed in the following sequence:

3.1 The growth in personal data collection

The issue of personal data collection is particularly significant in relation to the enquiry of the possible ways the public may undervalue their personal data, at a cost to privacy. The objective was to discover informed views and opinions of data collection from experts, and get insight about the value of personal data. The responses received indicated that there was a general consensus when it came to expressing the value of personal data. There were common themes in their opinions of why this is. These were monetary gain, economic dominance and due to the ever-increasing use and number of devices collecting data (R1, R2, R3, R4). However, there were key differences expressed in these insights surrounding the matter of economic control. Respondent 1 noted that it is because the Internet is generally a free service, as in Google, YouTube and Facebook (R1). They further reiterated this point, noting it is the commercial backbone of organisations' business models. Respondent 3 claimed the theory of Big Data encourages it and that "there is a frenzy to make money from personal data, even if usefulness is not yet clear" (R3). The other respondents, 2 and 4, stated it is for security and marketing purposes, whilst indicating a viewpoint of social control too and expressed a concern towards the issue of the potential for marketers to get hold of software used by security agencies, such as facial recognition (R2, R4). They also expressed that data collection leads to providing better and more efficient services to consumers. This reiterates the conflict of using personal data for the purposes of creating meaningful and efficient services for consumers vs. using personal data to exploit consumers as a means for financial gain. These findings were important because it highlights the reality of personal data collection, indicating some of the ways the public could undervalue their personal data online. Using services for free is one of them, which is in their every interest to glean personal data from users, or using the very devices that collect personal data. The responses indicated that amongst industry professionals there is wide-spread concern over continued mass collection of personal data. The theory of society experiencing *kontrollverlust* (Seemann 2014) can be applied to critically understand one of the possible reasons for mass media organisations to collect as much data as possible.

(Refer to Appendix B for details).

3.2 Technology and policy concerns about privacy

The respondents brought up issues within the technology sector and policy making that are compounded by growing challenges to privacy (R1, R2, R3, R4). This is significant in relation to understanding the perceptions of how the public may undervalue their personal data. The objective was to discover knowledge and reveal insights about how various industries approach and think about privacy in modernity. There were common themes in the responses that indicated a concern for global law and policies. However, all of them revealed different insights concerning how this is approached by their industry and the various practises of organisations and agencies in Britain and worldwide. Insights in to how technology and mass media organisations approach and think about privacy revealed the difficulties of applying global privacy policies, whilst adhering to individual countries' diverse privacy laws (R1). The need for Cyber Security was also addressed to balance the increasing importance of trust from their consumers (R4). Another insight is the storing and structuring of personal data, especially as they attempt to reduce costs by having processing done in other countries that are less concerned about preserving the privacy of individuals (R2). Another concern expressed was that there is information being created and articulated that is not actually supported by the original data (R2). However, a significant insight was one with direct focus to areas of law. The implementation of the EU's General Data Protection Regulation (GDPR) and notably the uncertainties for what happens after Brexit are both very challenging (R3). Another concern expressed by respondent 3 surrounds security services having access to personal data and how governments will regulate this to what is necessary and proportional in a democratic society (R3). These findings are significant because they indicate a variety of ways how personal data could be breached by businesses, corporations and agencies, sometimes unwittingly. Another significant finding was how planning for security measures in the future is becoming increasingly difficult for society today. The nuance of policies and decision making suggests an increasing lack of control over personal data, as the state of the 'new world' has transformed the flow of information (Seemann 2014) and problems emerge when there are perhaps huge degrees of autonomy and very little oversight by the businesses, corporations or agencies.

Taleb avows that a modern world is a world where insurance companies and all kinds of diverse industries are based on the premise that it is not possible to control individual risk, but be able through calculation to be able to come to very firm conclusions about levels of risk in society (Taleb 2007, pp.135-140). The former Secretary of Defence for the United States of America, Donald Rumsfeld, argues that his proposition of the "Unknown Unknowns" claims that is not the case (Graham 2014); the things that nobody could ever predict have a significant influence on the way in which history happens, the way in which development happens and the ways in which individual lives take place. On an individual level, it could be argued that people within all kinds of society do what they can to predict things for themselves, to make sure they have all the best possible chances. However, inevitably the real incidents and occurrences that change people's lives, for better or for worse, are the things that come out of nowhere. The more complex the world becomes and the more complex the information environment within it grows to be, the greater the impact unpredictability has on the way that things develop, both individually and in terms of corporations, nations and the world. The notion of the Black Swan illustrates a profound underestimation in terms of understanding how good and bad change happens in society. Rumsfeld describes this best after the tragic events that occurred on September 11th 2001. He discussed the effects and risks out there that a society is familiar with, coined as the

‘*Known Knowns*’. The ‘*Known Unknowns*’ is another term coined by him that describes the threats out there that we know about, yet we do not know the real details of due to a lack of information that would perhaps be able to control them. This relates to the very recent disclosure of a hack where one billion Yahoo accounts were compromised, which happened between 2013 and 2014 (Thielman 2016). Yet, what Rumsfeld stated that is the most frightening and distinguishable from anything else is the ‘*Unknown Unknowns*’ (Rumsfeld 2011). These are the threats that are out there which will come at society and there is no way that it can know of them. How can anybody manage risk in a society where the number of ‘*Unknown Unknowns*’ has accelerated? After the catastrophic events of September 11th 2001 one may believe you no longer could.

(Refer to Appendix B for details).

3.3 The phenomenon of social sorting in social media

As social sorting tends to insulate people from alternate perspectives, it is significant because it specifically relates to the potential for undervaluing personal data. The objective was to discover the views and opinions of what the experts think are the ultimate consequences of this phenomenon. There was a general consensus that social sorting in social media experiences is a reality. The common theme being that echo chambers were apparent to them in their personal social media experiences and that information being exchanged is often inaccurate, yet treated as credible. One insight indicated how they noticed a geographical divide on their Facebook Timeline during the UK EU referendum, with a kind of “tribalism” occurring (R1). Another insight claimed that social media can only be considered as a ‘transmit only’ medium and “the ravings of a self-opinionated minority” with no measured debate (R2, R4). One example of this is the information and disinformation about the civil war in Syria (R2). R3’s insight took a more measured approach in considering the potential for the undermining of democracies (R3). They note that it may be necessary to address the issue of algorithms causing online social and informational echo-chambers, by making said algorithms transparent, allowing users of the internet to turn them on and off at their own discretion (R3).

These findings were significant because they reveal the potential for which the public may undervalue their personal data and how the ubiquity of algorithmic surveillance and pattern recognition can affect society, via cultural fragmentation through no measure in debate. This may lead people astray because culture is supposed to be conversation and not a monologue. The disinformation surrounding the Syrian civil war, as respondent 2 noted (R2), reflects on the issue of ‘clickbaiting’ articles which contains ‘fake news’ for the sole purpose of disseminating false information (Chen, Conroy and Rubin 2015). By critically understanding this fact there is the potential that an individual may undervalue their personal data unwittingly, not just on the platform that is being used, but through being directed to somewhere else entirely on the Internet as well. The concept of living in the era of the query can be applied to rationalise the behaviour of users and not only understand that society is being recognised by the machines, but is always under surveillance by something or someone (Seemann 2014). Professor David Lyon of Sociology at Queen’s University, Kingston, Ontario, states everyday surveillance of personal data is a key feature in society today and argues that there are dangers inherent in the filtering systems, whose coding mechanisms involve categories derived from stereotypical or prejudicial sources. (Lyon 2003, pp.2).

(Refer to Appendix B for details).

3.4 Self-censorship online

The issue of self-censorship is significant in relation to how this may limit the freedom to act and express oneself online. The objective was to explore the expert's personal self-censoring habits. The common theme amongst the responses received was that all of the respondents felt obliged to self-censor all of the time (R1, R2, R3, R4). However, one insight expressed their need for strongly encrypted services (R3). Another reveals the potential implications for not self-censoring, noting that information anyone transmits online is there forever. They cite it most certainly will and could be used in the future, and that there is yet the discovery of information that one publishes online (R2). They further state that companies, such as Facebook, take in to account the long-term implications of people undervaluing their privacy and broadcasting themselves (often) indiscriminately (R2). An example of this could be that Facebook now recognises untagged photos of people (Gates 2011). These findings were important because they implied how personal data may be undervalued if self-censorship is not practised and the potential consequences of the radical uncertainties that stem from that. It could be argued that these include the context in which one's personal data could be used in the future and the potential to have information stolen. It could also be argued that this reinforces the concept of the *irretrievable loss of privacy* (Seemann 2014) and how much of an impact unpredictable change can have.

(Refer to Appendix B for details).

3.5 Perceptions of privacy and personal freedom online

As personal freedom and privacy today could be challenged online, it may have negative effects when personal data is undervalued to some degree. The objective was to explore the informed perceptions of personal freedom and privacy. From the responses received, there were similarities that showed to some degree personal freedoms could be constrained online, but the extent of which is due to individual perceptions of risk (R1, R2, R3, R4). Another common theme was that all the respondents expressed concern that their personal data had been compromised in the past (R1, R2, R3, R4). One respondent claimed they certainly had both their Facebook and Twitter accounts broken in to (R3). With regards to the potential that civil liberties may be constrained online, one insight indicated that it could be a moral decision that may constrain an individual's freedom to act and express themselves online (R1). They note that there is the possibility family could a) read information intended for friends, or b) know that something particularly left-field has been 'liked' or 'viewed' (R1). Respondent 4 also expressed this issue could relate to the topic or issue of discussion and the channel which it is taking place on (such as Twitter or Facebook) (R4). A significant insight highlighted the risk of the potential for personal data being stored by myriad public and private entities, to be structured in such a way that in the future information may not be received in the context it was originally disseminated (R2). These findings were significant as they revealed the extent of which observation could potentially restrict one's liberty and the ultimate consequences of undervaluing personal data, such as having online accounts broken in to and having personal data sold online (Farand 2017). The data received also reiterated the value of personal data. Depending on the position and profile an individual has, personal data may be worth more than others, thus being more vulnerable to cyber security threats. These findings also point towards that the constraints surrounding personal freedom online may be subject to the awareness and perception of whom has power over the user. As Seemann states:

> "The power to punish those not in compliance with the observers' expectations makes all the difference between observation and surveillance" (Seemann 2014, pp.21).

(Refer to Appendix B for details).

3.6 If you are not paying for it, you are the product

The issue of the statement “If you are not paying for it, you are the product” is significant to the enquiry because it indicates how frequently personal data may be undervalued, as most of the dominant services on the Internet are free (as in Facebook, Twitter and YouTube). Furthermore, it contextualises putting advertisers first and users second. An example of this might be Whatsapp giving their users’ personal data to their mother company Facebook, who is constantly forming a profile of its users in order to sell hyper-targeted ads (Gupta, Gupta, Ahamad and Kumaraguru 2015). The objective was to discover insight in to this phenomenon and potential ethical concerns surrounding it. From the data that was received there was a general consensus that the statement presented to them was correct (R1, R2, R3, R4). There was a common theme in the responses that emphasised concern about the ethics and the implications of this phenomenon. One insight in particular claimed it to be unjust and disheartening, but understood the need for it since “information is power” (R1). Another insight took a more measured approach, stating that there needs to be more education from a very age to be more careful with personal data, noting one must be cynical as publishing something online may be viewed the same as giving it to strangers in public (R2). A significant insight was made by respondent 4, claiming Facebook has turned in to a “revenue stream” having monetised the personal data of its users, which is more profitable than keeping it safe (R4). These findings were particularly significant because they contextualised the issue of the changing landscapes of advertising, emphasising the disheartening consequences of the growing conflict between meaningful and exploitative use of personal data. The findings also implied that users may be viewed as mere commodities to various businesses, corporations and agencies who are continually tailoring their services to its users. Moreover, it may be argued what is more worrying is that data inferences constructed by advertising agencies are trading cookies and personal data between third-parties. In Norway, there was a survey led by Sintef that revealed twenty-one Android applications between November and December in 2015 were communicating with 600 different primary and third-party domains (Roska Langum, Lien and Larssen 2016). Many of these third-party domains are trackers, which pose a threat to one’s privacy and many do not know for sure how they collect, store and connect user data. Evidently, there is a great lack of transparency given to the public and this provokes questions about the role of it within a society, yet more importantly who has control of their data and who truly owns it? If countries cease to consider the public, democracy subsequently diminishes.

(Refer to Appendix B for details).

Conclusion

The study in to experts' perceptions of privacy, surveillance and personal data has maintained a comprehensive analysis, that correlates several core themes from the literature review, with the information gathered from the respondents. The focus of the study has been enhanced by email interviews, that offered the respondents an opportunity to express their various insights, views and opinions on the subject. They critiqued the state of which society has transitioned to, which encourages and influences the way members of the public may undervalue their personal data, within the context of the UK. Although the study has given depth to the analysis and underlined some key points where the public may undervalue their data, due to this study's small sample size conclusions remain tentative. Taking this in to account, there are clearly opportunities for further research, such as increasing the volume of participants in the study and using a different approach to sampling might produce more generalised data.

The literature review and the research findings contain key theories, various concepts and insights from senior industry professionals that were able to confirm that there has been a shift in society's communications structures and how information is received. Historically, media distribution has been controlled by small elite groups of intellectuals and thus media consumption has been very top down. The pervasiveness of social media has completely redefined society and communication structures. The Internet, as well as the growing surge of IOTs, increasingly enables consumers to transcend time and distance in an effort to consume media. Users of the Internet, all contribute to the network in a horizontal fashion, meaning there is an open level playing field for consuming media and society is increasingly being apart of cellular holonic systems.

It was established that personal data collection is growing and is driven by monetary gain and socio-economic control. With the increasing use of technologies, the potential for undervaluing personal data increases also. Desktops, laptops, phones and tablets, as well as the IOTs, are all technologies where the public are prone to undervaluing their personal data. Emails, text messages, inputs via mouse-clicks, taps on screen, social media interactions, phone logs and various other digital traces left by people can all permit wide-spread compromising of data. Furthermore, as most services on the Internet are free, such as Facebook, YouTube, Instagram, Messenger, Whatsapp and Twitter, it makes it a lot easier for the public to neglect their personal data all together. The Internet increasingly permits the public to live their lives publically in cyber space – Facebook and Twitter being two prime examples of this, thus society being more prone to having data compromised.

Informed opinions from senior industry professionals indicated the compounding challenges to privacy were mostly due to law and policies. Different businesses, organisations and agencies approach personal data differently. The way that it is stored and structured is increasingly challenging, especially as they attempt to reduce costs by having processing done in other countries. Adhering to global and different countries' privacy laws are issues that are directly facing technology companies today. With a lack of transparency, individuals cannot know where their personal data ends up. Concerns were expressed that information is being created in an entirely different context from what it was originally. Evidently there are a variety of ways that personal data could be breached by corporations and agencies, even unwittingly. Problems are only going to increase due to the increase of autonomy. The responses suggest that there is very little oversight by corporations and agencies too. This reflect Taleb's (2007) theory of black swans which describes society living in a time where there are enormous amounts of radical uncertainty.

The potential for undervaluing personal data play in the hands of everyday algorithmic surveillance. The ultimate consequences are that pattern recognition can affect society via cultural fragmentation to affecting individual personalities. In the experts' social media experiences during the UK EU referendum, they could see society perpetuating echo-chambers that have the ability to insulate opinions and thus being exosed to less and less ideologically opposing narratives. Information being exchanged is often inaccurate, yet treated as credible on social media. It causes cultural fragmentation with no measured debate, which leads to misinformation circulating online. Evidently, social media has the potential to undermine democracies and it may be necessary to address the issue of algorithms causing online social and informational echo-chambers, by making said algorithms transparent, allowing users of the internet to turn them on and off at their own discretion. With points about 'clickbaiting' and 'fake news' being raised also by the respondents, it could be understood that personal data may be undervalued unwittingly, not just on the platform that was initially intended.

More self censoring will be beneficial for society, since information that anyone transmits online is there forever, which increases the need for using encrypted services. Informed views and insights revealed the potential implications for not self censoring, which ultimately could lead to personal data being compromised. This reflects Seemann's concept of the *irretrievable loss of privacy* (2014) and how much of an impact unpredictable change can have (Seemann 2014). There is no doubt personal freedom and privacy online is challenged. This is in part due to the undervaluing of personal data. To a degree, personal freedoms could be constrained online, but the extent of which is due to individual perceptions of risk. If personal data has been compromised knowingly in the past, freedoms online may become constrained. It could also be due to the connections one has on a social network, such as colleagues, family or the profession holds – it is a moral decision. The consequences for undervaluing or potentially neglecting personal data altogether can be far reaching. There is the prospect of personal data being disseminated to and stored by myriad public and private entities, whilst also information being interpreted from it could be used in an entirely different context than it was in originally. Unmistakeably personal data is extremely valuable, so much so increasing numbers of it are sold online, but the data of some individuals may be worth more than others, depending on their position and profile. Therefore, with all of this being taken in to account, the extent of which a member of the public may undervalue their personal data is enormous.

What indicates how frequently personal data may be undervalued is the changing landscapes of advertising. It now places advertisers and other businesses before users that are on social networks, to sell hyper targeted ads. Although, insights have shown to understand that "information is power", there was a general sense of concern about the changing landscapes of advertising, since personal data can be breached and undervalued almost daily, and communicated with other companies. It is as though it has become routine for businesses to communicate the public's personal data with other businesses. This raises issues about the conflict between meaningful and exploitative use of personal data. What has been established in this dissertation is that planning for security measures in the future is becoming increasingly difficult, due to the speed with which things are changing and that the ability of being able to imagine long term consequences has faded. It is concluded that the complex and uncertain world today is around the issue of a new temporality, where it is as though time seems to have shrunk to an 'eternal now' and it is only at a certain critical point when society realises just how much of their personal data they have given away.

Reference list

Ackerman, S., 2016. Snowden disclosures helped reduce use of Patriot Act provision to acquire email records. [online] the Guardian. Available from: https://www.theguardian.com/us-news/2016/sep/29/edward-snowden-disclosures-patriot-act-fisa-court [Accessed 5 Jan. 2017].

Bakshy, E., Messing, S. and Adamic, L., 2015. Exposure to ideologically diverse news and opinion on Facebook. Science, [online] 348 (6239), 1130-1132. Available from: http://science.sciencemag.org/content/early/2015/05/08/science.aaa1160 [Accessed 15 Jan. 2017].

Beck, U. and Ritter, M., 1992. Risk society. London: Sage Publications.

Berg-Larsen, E., 2015. The Issue of Privacy in the European Union: Controversies of the General Data Protection Regulation. Post-gradutate. Univeristy of Oslo.

Boyd, D. and Crawford, K., 2012. CRITICAL QUESTIONS FOR BIG DATA. Information, Communication & Society, 15 (5). *"Will large-scale search data help us create better tools, services, and public goods? Or will it usher in a new wave of privacy incursions and invasive marketing? Will data analytics help us understand online communities and political movements? Or will it be used to track protesters and suppress speech? Will it transform how we study human communication and culture, or narrow the palette of research options and alter what 'research' means?".*

Brock, D. and Moore, G., 2006. Understanding Moore's law. 1st ed. Philadelphia, Pa.: Chemical Heritage Foundation.

Bucher, T., 2012. Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. New Media & Society, 14 (7).

Chen, Y., Conroy, N. and Rubin, V., 2015. Misleading Online Content. Proceedings of the 2015 ACM on Workshop on Multimodal Deception Detection - WMDD '15.

Dahlberg, L., 2000. The Internet and the Public Sphere: A Critical Analysis of the Possibility of Online Discourse Enhancing Deliberative Democracy. Ph.D. Massey University.

Dencik, L., Hintz, A. and Cable, J., 2016. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. Big Data & Society, 3 (2).

Farand, C., 2017. Undercover investigation reveals public's personal data being shared on a 'huge scale'. [online] The Independent. Available from: http://www.independent.co.uk/news/uk/which-investigation-undercover-personal-data-list-brokers-a7538936.html [Accessed 21 Jan. 2017].

Flaxman, S., Goel, S. and Rao, J., 2016. Filter Bubbles, Echo Chambers, and Online News Consumption. Public Opinion Quarterly, 80 (S1), 298-320.

Gabel, D., 2014. Germany to Tighten Data Protection Laws: Consumer Protection Associations shall be Granted Right to take Businesses to Court. [online] Whitecase.com. Available from: http://www.whitecase.com/publications/article/germany-tighten-data-protection-laws-consumer-protection-associations-shall-be [Accessed 20 Dec. 2016].

Gates, K., 2011. Our biometric future. 1st ed. New York: New York University Press.Thielman, S., 2016. Yahoo hack: 1bn accounts compromised by biggest data breach in history. [online] the Guardian. Available from: https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached [Accessed 29 Dec. 2016].

Graham, D., 2014. Rumsfeld's Knowns and Unknowns: The Intellectual History of a Quip. [online] The Atlantic. Available from: http://www.theatlantic.com/politics/archive/2014/03/rumsfelds-knowns-and-unknowns-the-intellectual-history-of-a-quip/359719/ [Accessed 28 Dec. 2016].

Greenwald, G., 2013. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. [online] the Guardian. Available from: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [Accessed 5 Jan. 2017].

Gupta, S., Gupta, P., Ahamad, M. and Kumaraguru, P., 2015. Abusing Phone Numbers and Cross-Application Features for Crafting Targeted Attacks. [online] Cornell University. Available from: https://arxiv.org/pdf/1512.07330v1.pdf [Accessed 19 Jan. 2017].

Haddadi, H., Howard, H., Chaudhry, A., Crowcroft, J., Madhavapeddy, A. and Mortier, R., 2015. Personal Data: Thinking Inside the Box. [online] London: ACM, pp.1-5. Available from: http://arxiv.org/pdf/1501.04737.pdf [Accessed 1 May 2016].

Holdren, J. and Lander, E., 2014. Big Data And Privacy: A Technological Perspective. Report to the Preseident. [online] Washington D.C: PCAST. Available from: https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [Accessed 10 Mar. 2016]. *"The ubiquity of computing and electronic communication technologies has led to the exponential growth of data from both digital and analog sources. New capabilities to gather, analyze, disseminate, and preserve vast quantities of data raise new concerns about the nature of privacy and the means by which individual privacy might be compromised or protected".*

Lyon, D., 2015. Surveillance after Snowden. 1st ed. New Jersey: John Wiley & Sons.

Lyon, D., 2003. Surveillance as social sorting. London: Routledge, pp.1-14.

MacAskill, E., 2016. 'Extreme surveillance' becomes UK law with barely a whimper. [online] the Guardian. Available from: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper [Accessed 6 Jan. 2017].

MacAskill, E., Borger, J., Hopkins, N., Davies, N. and Ball, J., 2013. GCHQ taps fibre-optic cables for secret access to world's communications. [online] the Guardian. Available from:

https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Accessed 5 Jan. 2017].

Madden, M., 2014. Public Perceptions of Privacy and Security in the Post-Snowden Era. [online] Pew Research Center: Internet, Science & Tech. Available from: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/#about-this-report [Accessed 1 Mar. 2016].

McCracken, H., 2015. Inside Mark Zuckerberg's Bold Plan For The Future Of Facebook. [online] Fast Company. Available from: https://www.fastcompany.com/3052885/mark-zuckerberg-facebook [Accessed 22 Jan. 2017].

Miles, M. and Huberman, A., 1994. Qualitative data analysis. Thousand Oaks: Sage Publications, p.329.

Niederer, S. and Taudin Chabot, R., 2015. Deconstructing the cloud: Responses to Big Data phenomena from social sciences, humanities and the arts. Big Data & Society, 2 (2), 1-8.

Pariser, E., 2011. Beware online "filter bubbles". [video] Available from: https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en [Accessed 8 Jan. 2017].

Pariser, E., 2011. The filter bubble. New York: Penguin Press, pp.1-18.

Polonetsky, J. and Tene, O., 2013. Privacy and Big Data | Stanford Law Review. [online] Stanford Law Review. Available from: https://www.stanfordlawreview.org/online/privacy-and-big-data-privacy-and-big-data/ [Accessed 22 Jan. 2017].

Popovich, N., 2013. Evan Roth: the badass artist hacking popular culture. [online] the Guardian. Available from: https://www.theguardian.com/culture/2013/aug/20/evan-roth-badass-hacktivist-artist [Accessed 9 Jan. 2017].

Rumsfeld, D., 2011. Known and unknown. 1st ed. New York: Sentinel.

Roska Langum, S., Lien, J. and Larssen, J., 2016. The New Privacy Law Demanded By The EU & The Surveillance Economy. Trondheim: NTNU Trondheim.

Rogers, R., 2016. DmiAbout < Dmi < digitalmethods.net. [online] Wiki.digitalmethods.net. Available from: https://wiki.digitalmethods.net/Dmi/DmiAbout [Accessed 9 Jan. 2017].

Sadowski, J., 2016. Companies are making money from our personal data – but at what cost?. [online] the Guardian. Available from: https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon [Accessed 22 Jan. 2017].

Scott, R. and Kosslyn, S., 2015. Emerging trends in the social and behavioral sciences. Amsterdam: John Wiley & Sons, Inc., pp.1, 2.

Seemann, M., 2014. Digital Tailspin: Ten Rules for the Internet After Snowden. 9th ed. [ebook] Amsterdam: Institute of Network Cultures, Amsterdam, pp. 10 - 27. Available from: http://networkcultures.org/blog/publication/no-09-digital-tailspin-ten-rules-for-the-internet-after-snowden-michael-seemann/ [Accessed 15 Mar. 2016]. “The power to punish those not in compliance with the observers’ expectations makes all the difference between observation and surveillance” (Seemann 2014, pp.21).

Taleb, N., 2007. The black swan. 1st ed. New York: Random House, pp.135-140.

Taylor, P., 2015. Edward Snowden interview: 'Smartphones can be taken over' - BBC News. [online] BBC News. Available from: http://www.bbc.co.uk/news/uk-34444233 [Accessed 5 Jan. 2017].

Timm, T., 2014. First Snowden. Then tracking you on wheels. Now spies on a plane. Yes, surveillance is everywhere | Trevor Timm. [online] the Guardian. Available from: https://www.theguardian.com/commentisfree/2014/nov/15/spies-plane-surveillance-us-marshals [Accessed 28 Nov. 2016].

Tufekci, Z., 2015. How Facebook’s Algorithm Suppresses Content Diversity (Modestly) & How the Newsfeed Rules the Clicks – The Message. [online] Medium. Available from: https://medium.com/message/how-facebook-s-algorithm-suppresses-content-diversity-modestly-how-the-newsfeed-rules-the-clicks-b5f8a4bb7bab#.v8mae6qa1 [Accessed 16 Jan. 2017]. “The research was conducted on a small, skewed subset of Facebook users who chose to self-identify their political affiliation on Facebook and regularly log on to Facebook, about ~4% of the population available for the study. This is super important because this sampling confounds the dependent variable”.

van der Velden, L., 2014. The Third Party Diary: Tracking the trackers on Dutch governmental websites. NECSUS. European Journal of Media Studies, 3 (1), 195-213.

Appendix A

Research questions:

1. Do you feel that there is a general increasing effort to collect personal data in the public sense, and why?

2. Through thinking about privacy issues what do you think are the key concerns currently facing the area of industry you work in?

3. There is a common critique about social media acting like an echo-chamber (social sorting) that insulates people from alternate perspectives. How do you feel about this? For example, in the recent UK EU referendum and the US Presidential election this was used as a way of understanding the outcome from both perspectives.

4. Can you talk about an example of where you have felt that you needed to self-censor information that you have shared online, via email or other digital communications?

5. To what extent is your freedom to act and express yourself constrained online and do you think that there are any situations where your sharing of personal data online may have been compromised?

6. How do you feel about the statement “If You're Not Paying for It; You're the Product”? – as it contextualises putting advertisers first and users second. An example of this might be Whatsapp giving their users’ personal data to their mother company Facebook, who is constantly forming a profile of its users in order to sell hyper-targeted ads.

Appendix B

Email interview transcriptions:

Respondent 1 (R1):

1. Q) *Do you feel that there is a general increasing effort to collect personal data in the public sense, and why?*

   A) I do feel there has been a sharp increase in terms of personal data collection over the past five years. This is down to the rapid growth of online connectivity, and given the internet is generally a free service (Google, YouTube, Facebook etc.) harvesting personal data is the commercial backbone of these organisations business model.

2. Q) *Through thinking about privacy issues what do you think are the key concerns currently facing mass media and technology organisations?*

   A) One of the major concerns mass media & technology organisations face is applying global privacy policies whilst trying to adhere to individual countries differing laws around privacy.

3. Q) *There is a common critique about social media acting like an echo chamber (social sorting) that insulates people from alternate perspectives. How do you feel about this? For example, in the recent UK EU referendum and the US Presidential election this was used as a way of understanding the outcome from both perspectives.*

   A) From my own personal experience of using social media during the UK EU referendum, I can attest that social sorting is very much a reality. I'm originally from Chester in the north of England, and I've been living in London for the past 8 years. I have quite an even split of friends on social media who live in the north and south of the country. I noticed a geographical divide on social media, where friends from the north advised they were voting out and friends from the south of the country were staunch remain voters. The leave voters were labelled 'stupid' and remain voters were labelled 'ignorant'. It was a very 'them and us' situation playing out on people's timelines.

4. Q) *Can you talk about an example of where you have felt that you needed to self-censor information that you have shared online, via email or other digital communications?*

   A) I self-censor myself every day on social media!

5. Q) *To what extent is your freedom to act and express yourself constrained online and do you think that there are any situations where your sharing of personal data online may have been compromised?*

   A) Within reason, I feel there are no constraints around expressing yourself online. It's more of a moral decision. Do you want your family to read something that's pretty leftfield, and intended for your close friends? I have a young daughter and if I'm about to tag or share a risqué video for example, I often think would I want my daughter to know I've watched this. I imagine my online data has been compromised before, but I don't know of any specific examples I can list.

6. Q) *How do you feel about the statement “If You're Not Paying for It; You're the Product”? - as it contextualises the issue of Whatsapp now putting advertisers first and their users second by giving their personal data to its mother company Facebook, who builds profiles about us to sell hyper-targeted ads.*

A) It’s wrong. It’s so wrong. But I understand the need for it. Information is power. This statement has never been truer now we are in the digital age.

Respondent 2 (R2):

1. Q) *Do you feel that there is a general increasing effort to collect personal data in the public sense, and why?*

   A) Yes. More data is being collected for marketing purposes than ever before: e.g. tracking spending and travel habits, social media use and opinions, in an attempt to build a picture of our likely buying habits and susceptibility to marketing messages. Especially in the UK, we've also seen an unprecedented tracking of individuals and their on- and off-line habits, ostensibly for security purposes. This is also an area where a lot of research is being done into things like software for facial recognition, which may later be used by marketers.

2. Q) *Through thinking about privacy issues what do you think are the key concerns currently facing the technology sector?*

   A) Storing and manipulating the vast amounts of data being collected while still preserving individuals' privacy is an issue, especially as companies attempt to reduce costs by having processing done in countries that are less concerned about such things. There is also the danger that 'information' may be created from the mass of data that is not actually supported by the original data.

3. Q) *There is a common critique about social media acting like an echo chamber (social sorting) that insulates people from alternate perspectives. How do you feel about this? For example, in the recent UK EU referendum and the US Presidential election this was used as a way of understanding the outcome from both perspectives.*

   A) At best, social media can only be considered the ravings of a self-opinionated minority. In my view, it's a 'transmit only' medium; people open the virtual door, shout something and then close the door (and their minds). Measured debate is absent. Because of this, it's then strange to me how, for example, 'professional' journalists treat anything said or reported on social media as true and representative; the information and disinformation about the civil war in Syria – tweeted by people hundreds of miles from Syria but treated as factual – is an obvious example.

4. Q) *Can you talk about an example of where you have felt that you needed to self-censor information that you have shared online, via email or other digital communications?*

   A) All of the time. One must always consider what the information one puts 'out there' will or could be used for in future. Many people have yet to discover that the things they publish (or are published about them) on the internet are there forever and may yet come back to bite them… (And companies like Facebook make that part of their business model, of course, even to the extent of 'recognising' untagged people in photos.)

5. Q) *To what extent is your freedom to act and express yourself constrained online and do you think that there are any situations where your sharing of personal data online may have been compromised?*

A) As per your questions above, the constraint is one’s own perception of the risk that data being stored by myriad public and private entities, and combined and recombined by them, may not in future be seen in the context in which it was originally shared. by

6. Q) *How do you feel about the statement “If You're Not Paying for It; You're the Product”? - as it contextualises the issue of Whatsapp now putting advertisers first before its users by giving their personal data to its mother company Facebook, who builds profiles about us to sell hyper-targeted ads.*

A) It’s absolutely true. There’s no such thing as a free lunch.
I’d make the general point here that there needs to be much much more education for people, from a very young age, to be very careful with their data. They need to be sceptical, even cynical; after all, publishing something on the internet is the same as giving it to random strangers one meets in the street, yet most folk would baulk at that.

Respondent 3 (R3):

1. Q) *Do you feel that there is a general increasing effort to collect personal data in the public sense, and why?*

   A) Yes. The number of devices collecting data is increasing. And so is their use. There is a frenzy to make money from personal data. And the Big Data theory encourages collection of all data, even if usefulness not yet clear.

2. Q) *Through thinking about privacy issues what do you think are the key concerns currently facing law and policies established in the UK?*

   A) Implementation of the GDPR and what happens after BREXIT. And: Access by security services to personal data, and how to limit this to what is necessary and proportional in a democratic society.

3. Q) *There is a common critique about social media acting like an echo chamber (social sorting) that insulates people from alternate perspectives. How do you feel about this? For example, in the recent UK EU referendum and the US Presidential election this was used as a way of understanding the outcome from both perspectives.*

   A) This is a serious problem, with the potential to undermine democracy. What is necessary is that algorithms causing such echo chambers must be made transparent and it must be possible to turn them off if using search.

4. Q) *Can you talk about an example of where you have felt that you needed to self-censor information that you have shared online, via email or other digital communications?*

   A) Me personally no. But I am very consciously using only strongly encrypted services.

5. Q) *To what extent is your freedom to act and express yourself constrained online and do you think that there are any situations where your sharing of personal data online may have been compromised?*

   A) I had both my Facebook and Twitter accounts already broken into.

6. Q) *How do you feel about the statement "If You're Not Paying for It; You're the Product"? - as it contextualises the issue of Whatsapp now putting advertisers first and their users second by giving their personal data to its mother company Facebook, who builds profiles about us to sell hyper-targeted ads.*

   A) The statement is correct.

Respondent 4 (R4):

1. Q) *Do you feel that there is a general increasing effort to collect personal data in the public sense, and why?*

   A) Yes – conditions relate to the purpose/s for which the information is intended to be used as well as creating personal user profiles. This increase is leading to providing a better, more efficient service to customers across a range of sectors.

2. Q) *Through thinking about privacy issues what do you think are the key concerns currently facing Marketing and Communications companies?*

   A) Cyber security – The need to protect customers/consumers in a digitised world ie breach of profile data, which can do serious damage to a company's reputation.
   Surveillance and Drones – being flown into 'private spaces' without advising people around them; subject to monitoring activity without consent.
   The technology of big data and the IoTs is growing on a daily basis - Companies need to be evaluating what data they are gathering and how they are using it. They need to pay more attention to their downstream vendors and partners, who can capitalise on data more than ever before. And companies need to think about the increasingly important issue of trust from consumers and others, about how their data is being used and what commitments are being made about this data.

3. Q) *There is a common critique about social media acting like an echo chamber (social sorting) that insulates people from alternate perspectives. How do you feel about this? For example, in the recent UK EU referendum and the US Presidential election this was used as a way of understanding the outcome from both perspectives.*

   A) This is concerning as it is insulting people from other perspectives and not allowing them access other view points. With personalised algorithms on individual online newsfeeds, these social communities are fragmented, as like-minded people hear arguments in one specific direction – people trust evidence supplied by their own social group….social discussion and sharing suffer as people have a narrow information base.

4. Q) *Can you talk about an example of where you have felt that you needed to self-censor information that you have shared online, via email or other digital communications?*

   A) Due to instant feedback via social networking sites, self-censoring information from time to time, is paramount in keeping the conversation flowing and or sharing a personal experience.
   By contributing anonymously on a consumer review site, sharing information/experiences is another platform to voice opinion without being 'judged'.

5. Q) *To what extent is your freedom to act and express yourself constrained online and do you think that there are any situations where your sharing of personal data online may have been compromised?*

   A) The freedom to act and express yourself can be at times constrained online, depending on the debatable topic/issue and the channel the discussion is taking place ie twitter, facebook

More recently, Yahoo had a hacking incident whereby personal data may have been compromised. This coincides with receiving personal bank account notifications of unauthorised transactions.

6. Q) *How do you feel about the statement "If You're Not Paying for It; You're the Product"? - as it contextualises the issue of Whatsapp now putting advertisers first and their users second by giving their personal data to its mother company Facebook, who builds profiles about us to sell hyper-targeted ads.*

   A) The statement is concerning as Whatsapp/Facebook have put advertisers first and the end user second. Advertisers have first-hand information, data and user profiles on users, that otherwise would have been kept private.
   Facebook have monetised personal data by turning this into a revenue stream, which is more profitable than keeping the information safe ie your're not paying for it, you're the product.