A Study of Information Privacy and Smartphone Users

Siobhán Foley

A dissertation submitted to the University of Dublin

in partial fulfilment of the requirements for the degree of

MSc in Management of Information Systems

1st September 2017

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: Siobhán Foley

Siobhán Foley.
1st September 2017.

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: Siobhán Foley

Siobhán Foley.
1st September 2017.

Acknowledgements

I would like to thank my supervisor PJ Wall for his help, guidance and sound advice during the completion of this dissertation. My thanks also to the lecturers and college staff for all their help over the last two years.

I am grateful to my family, friends and colleagues who have been patient, supportive and encouraging of this endeavour.

Finally, I would like to express my sincere appreciation to all those who agreed to be interviewed and were so generous with their time and input. A very big thank you to them.

Abstract

Over the last ten years the smartphone has moved from niche product to become an almost universally adopted device. Its success has been helped by the continual improvements in network connection speeds, the convergence of disparate devices into one and the vast range of services offered through mobile app software. Smartphones became the first technical device that was also personal resulting in societal changes in how people collaborate, consume content, capture events and build interpersonal networks. This has brought convenience in the completion of many daily tasks but it also introduces potential risks to information privacy.

The unique traits of a persistent connection to the internet and being constantly in the procession of the user has led to the creation, transmission and sharing of vast amounts of information that capture what individuals are doing while also tracking their location. The purpose of this research is to explore the attitudes of smartphone users towards their information privacy in the context of these unique abilities.

Data was gathered through semi-structured interviews with a small sample of experienced smartphone users. A qualitative inductive method of analysis was used to interrogate the collected data and develop themes.

The findings revealed that users do have concerns about their information privacy that was in concert with the academic literature. While self-regulation against disclosure had been used as a means of protection, it had not been deemed a wholly successful approach by participants with some of them being unsure of what information they had shared and which entities it was shared with. There was divergence in the treatment of disclosure level on different social media platforms depending on the perception of control over the flow of information.

Table of Contents

Table of Figures and Tables

List of Abbreviations

API	Application Programming Interface
App	Mobile application
CFIP	Concern for Information Privacy
DOI	Diffusion of Innovations Theory
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act of 1996
IP	Internet protocol address
IT	Information technology
IUIPC	Internet users' information privacy concerns
LBS	Location Based Services
MIM	Mobile Instant Messaging
MUIPC	Mobile Users' Information Privacy Concerns
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
SMS	Short message service
Spam	Unsolicited electronic mail.
U.S	United States
Wi-Fi	Wireless Area Local Network (IEEE 802.11 standard)

1. Introduction

1.1 Background and Context

The first industrial revolution saw the invention of the steam engine, this was followed in the early 1900s by the introduction of electricity and the second industrial revolution. More recently electronics and computing have been the basis of the third. Each of these innovations of progress has been disruptive to the status quo, the 'creative destruction' that economist Joseph Schumpeter described. These advances have facilitated the creation of new opportunities for commerce and socialisation that over time reshaped society as a whole.

Now is the time of the digital age and what has been termed by Schwab (2017) as the beginning of the fourth industrial revolution that will see technology become more embedded into every aspect of daily life. Today it is common for people to be persistently connected to the internet and to be constantly generating data about all aspects of their life. According to Cisco (2017) data generated in 2016 from mobile devices grew 63% worldwide on 2015 figures. They predict that this will increase and accelerate over the coming years with a possible compound annual growth rate of 47% over the next five years. In 2015 at the World Economic Forum in Davos, Google's chairman Eric Schmidt made the claim that the 'The Internet will disappear'. He was speaking about how pervasive connected devices will become and our interaction with them will become so seamless that the gap between technology and human will disappear (Smith, 2015).

Smartphones are one of the primary enablers of this transition. They are seen by many as user friendly devices that allow people to have persistent connections to the internet and each other. There has been a hyper convergence of disparate gadgets into this single powerful pocket-sized personal device. The standard check before leaving home has become wallet, keys and phone. With mobile payment services becoming a widely used form of payment it will not be long before a physical wallet will no longer be needed.

Combining the functions of telephony and computing into a single portable device, smartphones allow activities that were once physical, tethered to time and place to become digital, mobile and always available, from conversations and photography to watching a movie or navigating an unfamiliar route. Each technological advancement in communications has raised questions about implications for user privacy. These questions are especially pertinent in relation to the smartphone due to the wide range of capabilities it offers. A smartphone is usually powered on and carried by the user allowing for the collection of information not just about what the user is doing but also their precise location.

The Apple iPhone released in 2007 marked the beginning of mainstream availability of smartphones. The ten year anniversary of the iPhone launch is a timely juncture to examine user attitudes towards information privacy when using their smartphone.

The adoption rate of mobile phone technology has been faster than preceding communication forms achieving a 40% adoption rate in the United States (U.S) over a ten year period something the telephone took forty years to do (McGrath, 2013). Improvements in both mobile network speeds and broadband coverage combined with reducing data transmission costs have helped with the speed of adoption. Figure 1 shows the unit shipments of smartphones globally from 2013-2016 with 1.4 billion units being shipped in 2016.

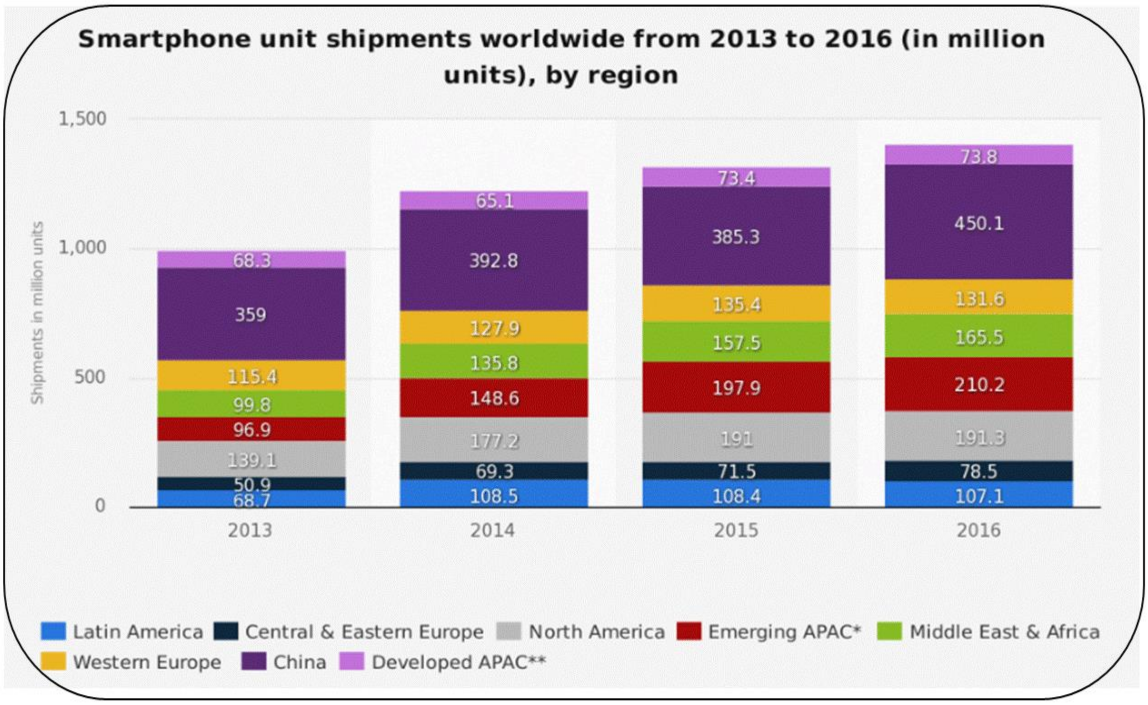


Figure 1 Worldwide Smartphone Unit Sales 2013-2016 by region (Statista, 2017a)

This equates to almost 20% of the world population buying a smartphone in a single year. In December 2016, of the 4.95 million mobile subscriptions in Ireland, almost 88% of them were for smartphones (Commission for Communication Regulation, 2017) demonstrating how ubiquitous this technology has become.

The range of functions that a smartphone can perform has expanded greatly since their introduction offering users convenience in the completion of many daily tasks like banking, shopping, travel and entertainment. With this convenience comes an element of risk, breach of information privacy through the loss or theft of the smartphone itself or unintended disclosure through unconscious sharing by the user. The storage repositories of the data collectors may become a target for hacking and theft. Users may see the potential loss of privacy as a fair exchange for the range of services they receive or they may not be aware in the first instance of the myriad of ways that information they have shared can be further disseminated in legitimate ways.

Smartphones have in addition to common computing capabilities like email, web browsing and office tools contributed to the creation of a software development subsystem dedicated to mobile application development. These mobile applications known colloquially as ‘apps’ are written specifically to run on mobile devices. The first apps that were developed were for the electronic personal digital assistant (PDA) a precursor to the smartphone. They performed a limited set of simple tasks like calendar management, contacts list and note taking but were written in a proprietary programming language for a specific device. Today apps are developed to be agnostic of the hardware device and support multiple mobile operating systems (OS). In 2009 Apple launched a marketing campaign entitled ‘There’s an app for that’ to promote the variety of apps available, the phrase became so popular, it was later patent protected by them (Gross, 2010). That was just the beginning of this fledgling software industry, as of March 2017 there were 2.8 million apps available in the Google Play store for the Android OS and 2.2 million in the App store for Apple iOS, the two largest smartphone OSes (Statista, 2017b). This offers users huge choice in how to consume services across a range of categories from social networking, news and entertainment to weather reports and illustrates the size and variety of the mobile apps market.

While some apps have a fixed cost or operate on a subscription model, many are available free of charge and their business model relies on monetisation of the service in other ways using information for target marketing as an example. Businesses have been created and thrive based on information sharing. Social media companies like Twitter and Instagram have harnessed the possibilities that smartphones offer and become well-known brands in a relatively short time period. There are questions to be asked as to how open and transparent organisations are with users as to the type and extent of information they are collecting and for what purposes.

Current smartphones contain sensors that can track location, pedometers that count activity, pulse readers that can measure health information and personal assistants that are summoned through the microphone. They are sophisticated devices that are improved upon and enhanced with each new release. These sensors in themselves are of no benefit unless there is some way of harnessing the data they can collect.

Clive Humby a mathematician from the UK coined the term 'Data is the new oil' in 2006, and like oil he explained that in its raw form data is of little value but just as oil becomes valuable once it has been processed, it is only after analysis that raw data becomes information. The value of information lies in its ability to offer insight to business to identify new opportunities and new revenue streams (Palmer, 2006). It was neatly summarised by Nissenbaum when she said that information has become the 'supreme currency' in this digital age (2011, p.33).

The information collected from activities performed on smartphones is being used by business and government to provide contextualised user experiences, build a more personal relationship or provide services in a more efficient manner. The potential value of information has been recognised by business and government but there is a question as to whether users place a value on their information as they would other personal assets.

1.2 Research Question

Since the introduction of the newspaper printing press when Warren and Brandeis (1890) wrote an article on 'The Right to Privacy', each technological evolution sees a return to the debate about privacy and individual rights to it. This research is seeking to explore the attitude of users towards information privacy when using their smartphones. The ease and speed with which a person can upload or transmit information through a smartphone does not support taking the time to reflect on the longer term consequences. Any operation that is performed online may be tracked and information about it stored indefinitely. It is not only the analytic capabilities of today that users need to be cognisant of but to be aware that unknown future analytical capabilities could be executed on the stored information. There is no way of retracting information that has been shared online, once it has been shared the privacy of it is gone forever. When smartphones were introduced they had limited functionality and the longer term implications of information sharing may not have been considered. Today the smartphone has become for many an embedded part of daily life and unlike other computing devices they are as much a tool for socialisation or a status symbol as they are a technical one (Srivastava, 2005). In the Western World one of the rites of passage has become the first smartphone a child receives. Many of the most popular apps used by smartphone users are categorised under the social media umbrella. As of April 2017, globally there were 3.8 billion active internet users and 2.7 billion of those were mobile social media users (Statista 2017c). The continued success of these apps is dependent on users sharing personal information making this an important area to explore.

The primary research question is

What is the attitude among smartphone users about information privacy when using a smartphone?

This leads to the following sub questions

How important is information privacy to them?

Are users aware of what information they have agreed to share and with whom?

What actions have users taken to protect their privacy when using their smartphone?

1.3 Scope

This research will adopt a mainly qualitative approach to data collection by conducting semi structured interviews with a number of smartphone users. The participants are from varied backgrounds but do not have an explicit expertise in information privacy or information technology (IT). The rationale for taking this approach will be discussed in detail in Chapter 3.

There are a number of ways information privacy can be violated, information that has been legitimately collected with the consent of the user but which is inadvertently leaked or illegally accessed by hacking. Information can be illegally obtained from users through bogus emails or texts purporting to come from legitimate business requesting confidential information. This research will not focus on misuse of these types, it is concerned with how users treat their information privacy when using their smartphones.

1.4 Benefits of the Research

As has already been stated, mobile technology is evolving at a rapid pace through the continuous improvements in smartphone devices and the widespread availability of high speed networks. With a software ecosystem that offers apps to cater for every interest and vast amounts of cloud storage accessible from anywhere, this confluence of innovations has had a profound impact on society leaving no facet untouched. It has changed the way people work and collaborate, how they are educated, how friends are made, life partners found, medical opinion sought and news consumed. There are a wide range of activities completed everyday by people using these sophisticated devices that leaves a digital trail of information about themselves and their actions.

This research in exploring user attitudes towards information privacy when using their smartphone will expand on existing knowledge to benefit academics in the ongoing research of information privacy and technology. It may be considered by policy makers and regulators who are developing the frameworks that govern this area to ensure a fair and sustainable environment for both user and technology provider into the future. It behoves everyone to be guardians of their assets and information as an asset deserves protection, this paper may help users to get a better insight into the topic of information privacy and by providing some insight into how preferences impact what information is shared may be used to guide their decisions making.

1.5 Dissertation Structure

The dissertation is structured as follows:

Chapter 1. Introduction

This section provides an introduction to the topic, gives background on the context and reasoning for undertaking this area of study. The research question is outlined and the scope of the research is defined. It provides an overview of the benefits of the research and a roadmap to the rest of the document.

Chapter 2. Literature Review

The literature review presents a review and analysis of relevant literature pertaining to information privacy, smartphone usage and mobile applications.

Chapter 3. Research Methodology

This chapter explores the methodological approaches available to carry out this research project. It explores the reasons that the chosen philosophical perspectives, research methods and methodology were selected. It discusses the ethical considerations of a research project and concludes by highlighting the limitations of this study and how it might be improved upon in the future.

Chapter 4. Findings and Analysis

This chapter details how the research was conducted. It presents the primary data collected, analyses it and interprets the findings in relation to the research question.

Chapter 5. Conclusion

The study concludes by emphasising the key findings from the gathered data and how this expands upon the body of knowledge to date. It acknowledges the limitations of the research and suggests areas of interest for future study.

2. Literature Review

2.1 Introduction

This chapter will examine the body of literature relating to the academic areas of information privacy and smartphone technologies. Literature has been drawn from a variety of sources including academic journal articles, newspapers and industry analysis reports.

The chapter commences by charting the evolution of mobile technologies since their beginnings in the 1980s to the current proliferation of smartphones. Secondly it explores concepts of privacy and information privacy in particular. Thirdly it goes on to examine the research into the information privacy concerns and attitudes to privacy on the part of users and the relationship between attitude and behaviour. Finally the chapter concludes by looking at how some of the future trends may impact information privacy and smart technologies into the future.

2.2 Evolution of the smartphone

This section will discuss how mobile technologies have evolved over the last four decades from a niche product with limited capabilities to an advanced piece of technology with global reach.

When mobile phones were first launched they could perform a trivial number of functions and had limited reach due to prohibitive costs and partial telecom network coverage. The release of the first generally available smartphone in the guise of the Apple iPhone came as network speeds and coverage increased and costs became more affordable (Grabham, 2016; ITU, 2011). This helped popularise the smartphone. Since then the array of functions a smartphone can perform has expanded and been enhanced making some devices like music players and cameras redundant. Telecom networks speeds continue to increase and individuals are using their smartphones to access digital platforms where they can learn, find employment, share their story, contribute to debates and build their interpersonal networks. This has resulted in exponential increases in data volumes being transmitted, while smartphones only represented 45% of mobile connected devices in 2016, they were responsible for 81% of the data traffic (Cisco, 2017).

In recent years ‘Smart’ has become a prefix that is appended to devices to indicate they have some embedded intelligence via sensors, actuators, and communications capability.

In the case of a smartphone as well as the above, Gartner (2017a) define it as having an identifiable open OS with application programming interfaces (APIs) that allow third party developers to write applications that can run on the device's OS. Applications can be installed and removed, and the phone must be able to support multiple tasks simultaneously similar to the way a personal computer (PC) operates.

Smartphones have become an indispensable device for many people, the number of smartphones sold in 2016 was approximately 1.4 billion (Statista, 2017a) versus 270m PCs (Statista, 2017d). Reviewing the advertising and in-store displays of the mobile phone stores, smartphones options are more widely promoted and available. In May 2017 Vodafone had thirty five smartphone options available versus three basic phones (Vodafone, 2017) and this is reflected across other providers. The limited choice of basic phones may influence some users to move to smartphone technology even if they do not need the advanced functionality it offers.

There is a hierarchy of information shared by the smartphone and other internet capable devices as can be seen in Figure 2.

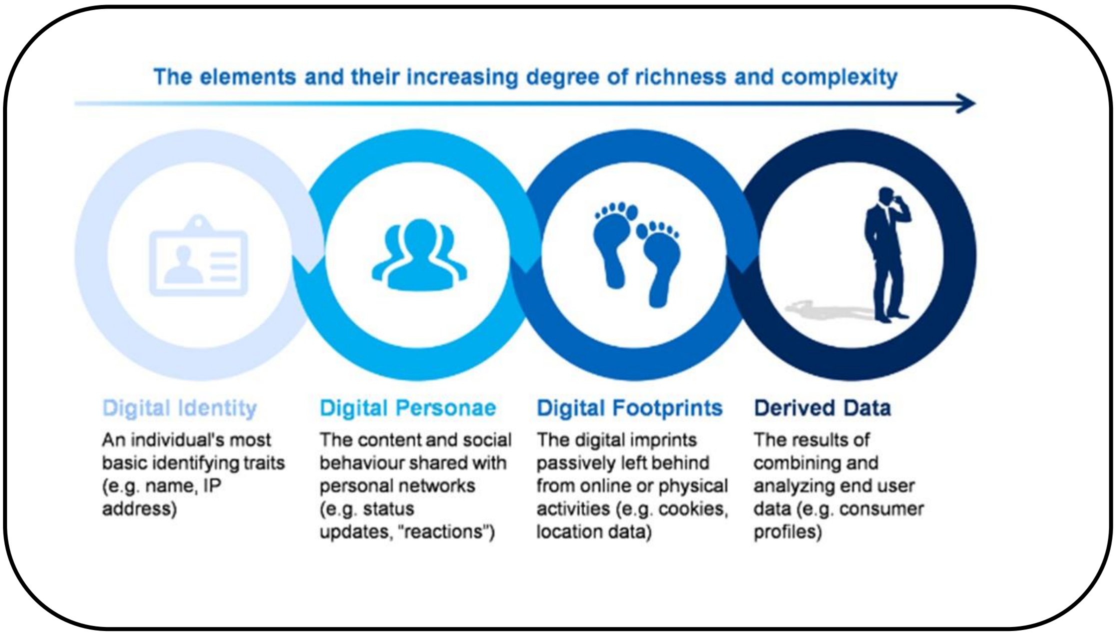

The elements and their increasing degree of richness and complexity
Digital Identity
An individual's most basic identifying traits (e.g. name, IP address)
Digital Personae
The content and social behaviour shared with personal networks (e.g. status updates, "reactions")
Digital Footprints
The digital imprints passively left behind from online or physical activities (e.g. cookies, location data)
Derived Data
The results of combining and analyzing end user data (e.g. consumer profiles)

Figure 2 The Value Personal Data Framework (World Economic Forum, 2017)

At the low end of data disclosure is the identifying internet address (IP) of the device, it is necessary to maintain the internet connection to the device once it has established a connection, this has limited ability to uniquely identify the individual user. The digital personae and digital footprints comprise the details of a user's online activity, it includes the information they share, transactions conducted as well as identifying tags like cookies or location that are automatically captured. When this rich data is analysed, aggregated across users or combined with third party data it can create personalised behaviour profiles that can be used to predict decision making or design context based services. This derived information is recognised as valuable by service providers and government, it provides insight into new opportunities that can be targeted by them. Sometimes this information may be provided without much thought on the part of the user and this can raise the question as to whether users see their information as valuable.

As has been discussed the smartphone has changed the way people interact with the world and each other and this has resulted in information being constantly transmitted by them and about them. The next section will discuss information privacy in more detail.

2.3 Information Privacy

Information privacy is not a new idea, it may not have been labelled as such but it has existed as long as it has been possible to capture and convey material about someone. The following section will discuss the concept of information privacy, place changing attitudes in context and look at some of the models that have been developed to capture individual attitudes.

The importance of privacy and the right to privacy is enshrined in many constitutions and charters around the world, article twelve of Universal Declaration of Human Rights states that:

'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' *(*UN General Assembly, 1948).

Westin (1967, p.7) who was the first researcher to study consumer information privacy defined it as the 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.' The variables of when, how and extent are subjective with variation determined by the culture, context and motivation of the individual (Acquisti, 2015).

Westin conducted surveys about privacy from the 1970s to the early 2000s, he categorised respondents into three groups, privacy fundamentalists; privacy pragmatists and those unconcerned with privacy. Privacy fundamentalists are suspicious of organisations, are unwilling to disclose information and favour protective regulation. The unconcerned group are open and have no issue with information disclosure. The privacy pragmatists take a hybrid approach, evaluating each circumstance and making a decision to share information or not based on its merit (Kamaraguru & Cranor, 2005).

As the capabilities of IT have expanded so too have the factors to be considered when defining information privacy. Smith et al. (2011) identified three categories: information privacy as a commodity where information is exchanged in return for a service, information as a state of limited access whereby a person can limit access to their information and information privacy as control. In the case of control, it means allowing the user control over what information about them is shared and whom it is shared with. These different approaches illustrate the difficulty of trying to have a single definition that can be applied in all situations.

In the decade following World War II, there was a high degree of public trust in government and commercial organisations engaged in information collection. Media coverage of the same was benign and the ability to capture and process information was limited. Attitudes began to change from the 1960s onwards, information privacy became a topic of debate and concerns were raised by both academic researchers and the media. This coincided with the initial wave of IT as a discipline and the advent of centralised databases (Smith et. al, 2011). Since then stated concerns about information privacy among the general public have risen, media reports of information privacy concerns have become more common and the technological capabilities to collect, transmit and analyse information has expanded (Westin, 2003). To assuage user concerns government regulation regarding information privacy began to come into effect in the 1990s. In 1995 the Europe Union (EU) introduced Directive 95/46/EC of the European Parliament and of the Council that sought to protect citizens of the EU with regard to the processing of their personal information and restrict the movement of same outside of the EU unless similar protections were in place at the destination point. The United States (U.S) introduced the Children's Online Privacy Protection Act of 1998 to regulate the collection of information online from children under 13 by requiring parental consent to do so and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was introduced to protect the privacy of patient health information. Regulation in this area continues to evolve to try to keep pace with technological advancements, the General Data Protection Regulation (GDPR) will replace

Directive 95/46/EC in 2018 and it seeks to strengthen the protections offered to citizens with regards their information privacy.

To measure the degree of information privacy concern among users, a number of frameworks have been developed. Smith et al. (1996) developed the Concern for Information Privacy (CFIP), it was mainly applied to offline information collection. It concentrated on user concerns about the breath of collection, improper access to information, unauthorised secondary use and inadequate protections against correcting errors in the collected information.

Malhortra et al. (2004) enhanced the CIFP model to be more applicable to online activity. Their framework is called the Internet users' information privacy concerns (IUIPC). Their hypothesis is that concerns for information privacy are routed in a sense of fairness and natural justice. They surmised that there were three main areas to be considered, collection, control and awareness. Like Smith et al. (1996) they saw concerns around collection being related to the volume of information being collected as being appropriate for the purpose of collection. Users wanted control over their information and to be able to explicitly approve collection or stop the processing of their information and cancel collection at any time. The sense of fairness requires that acquiesce to information collection should be an active deliberate process. The third factor they consider is how awareness of the privacy practices of the organisations responsible for collecting the data impacts user concerns. In addition to the main factors, three context specific variables that may influence the degree of user concerns were identified, trust beliefs, risk beliefs and behaviour intention. Trust and risk work in opposition to each other, the greater the level of trust a user has in an organisation then their level of perceived risk is reduced. They proposed that behaviour intention when considered in conjunction with trust and risk beliefs is a good indication of what actual behaviour will be.

Building on the IUIPC model, Xu et al. (2012) developed a hypothesis based on Mobile users' information privacy concerns (MUIPC). This framework was prompted by the enhanced capabilities of the smartphone to be always connected to the internet, capable of continuous data transmission and being able to provide exact location details. In the MUIPC model, data collection is categorised as perceived surveillance. This encapsulates the idea that the combination of data and metadata generated by a smartphone can provide a complete view of an individual's activities. Data is the content of the transmission, the emails or instant messages. The metadata is the detail about the transmission, it captures details like who the message was sent to, time and location of device when it was sent. The second factor they consider is perceived intrusion which covers collected information being accessed inappropriately or used in a way that has not been approved by the user. It also covers where collected information is used to disrupt or disturb the user. This would manifest itself as adverts and notifications targeted at the user. The final factor is secondary use where information collected for one purpose is used for another or shared with another entity without permission.

There are common themes between all three models, they all view the scope of information collection as core to user concerns. It needs to be appropriate for the service or transaction being requested. All frameworks agree that users like to have control over how their information is used and have the opportunity to stop collection or processing. The concept of control is also relevant to the area of secondary use as when control is lost, the number of secondary entities that may have access without consent can multiply quickly with the capabilities of IT today. As Niessenbaum (2011, p.34) said ‘constraints on streams of information from us and about us seem to respond not to social, ethical, and political logic but to the logic of technical possibility’. The perceived sensitivity of the requested information will also be factor (Norberg et al., 2007) in how a user will judge the level of privacy to be applied.

Section 2.3 has discussed information privacy in general and some of the models that have been developed to measure its importance to individuals, the following section will go on to examine the attitudes that have been recently expressed by users towards privacy of their information when online.

2.4 Attitudes toward Information Privacy

The following data is taken from a report completed by the European Commission in 2016 ((European Commission, 2016). It surveyed over 26,000 people from various social and demographic categories across the 28 EU States about a number of privacy related areas. The following section takes a subset of that report to show user attitudes towards online information privacy.

Of the ~22000 citizens that this question was relevant to, the vast majority placed information privacy as important or very important for both their devices and for online. As can be seen in Figure 3, almost 80% of those surveyed thought it was very important that the data on their device was not accessed without their permission.

Over 90% thought it was very important or fairly important that the content of messages was kept private and over 80% also thought it was very important or fairly important that their online activity not be monitored without consent. Despite this desire to be free from monitoring, there was little appetite to pay for the benefit with 74% responding that it was unacceptable to be charged to remain anonymous.

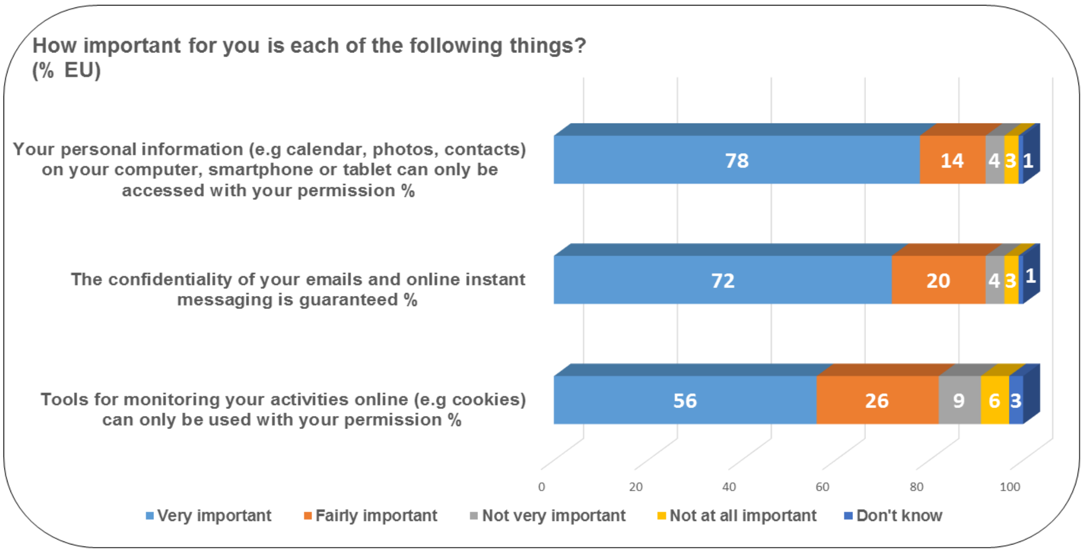


Figure 3 Attitude to Online Information Privacy across EU States (European Commission, 2016)

A breakdown of Irish respondents taken on their own shows a similar picture. when the percentages of very important and fairly important are combined they almost mirror the EU averages with slightly more emphasis placed on very important by Irish users as can be seen in Figure 4.

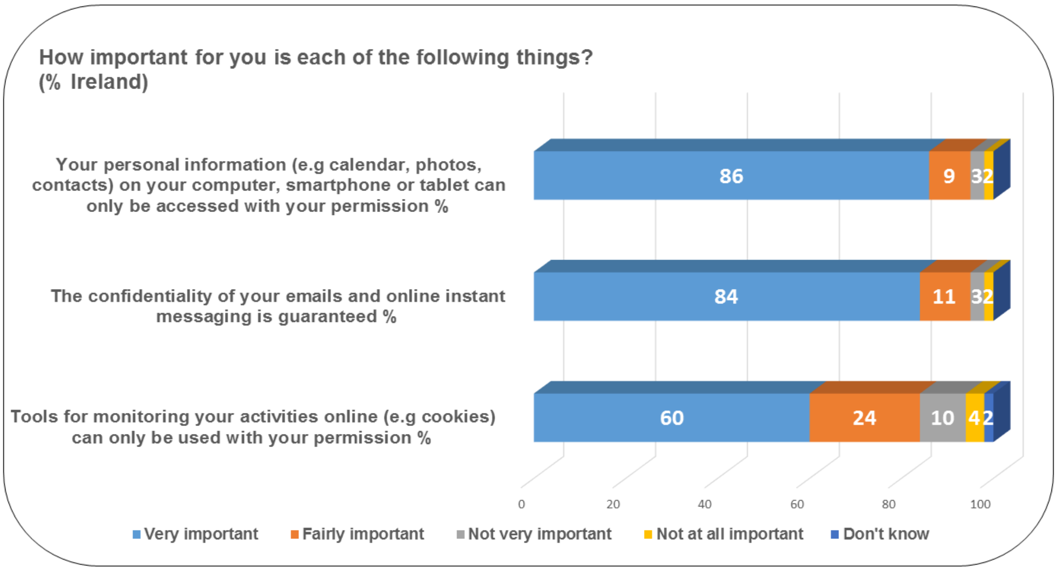


Figure 4 Attitude to Online Information Privacy in Ireland (European Commission, 2016)

This survey like many of the models used to measure attitudes rely on self-reporting scales and there is an argument that stated intentions often do not match actual behaviour, this inconsistency has been labelled the privacy paradox. Brown (2001) while studying online shopping behaviour found that while users expressed concerns about sharing information with online retailers, it did not prevent them from shopping online.

In trying to explain this phenomenon, Acquisti et al. (2015) proposed that users in evaluating information privacy are not sure about where to make the appropriate trade-off as the consequences of information sharing are not fully understood by them. The online collection of information is so seamless that it is often not evident to users that anything is being collected at all (Acquisti et al., (2015). Making an informed decision requires a level of digital literacy and time to consider the risks and benefits before deciding on what information to share but the instant nature of clicking on a website or installing a mobile app does not offer the time to pause and evaluate (Baek, 2014).

The gap that has been found between attitude and behaviour may be influenced by context. When users are questioned to get an understanding of their attitude to information privacy, risk is likely to be elevated in their mind (Norberg et al., 2007) and so may influence their response. When they are actually using their smartphone as part of their daily routine they may be more concerned with completing the task at hand and potential risks become less prominent and have less influence.

Another possible explanation for the discrepancy between attitude and behaviour is the variety of information types. While users may in broad terms worry about keeping their information private, there are segregated levels of importance, something sensitive or the potential to cause embarrassment if revealed will have a higher value than something deemed non sensitive (White, 2004; Mothersbaugh et al., 2012; Acquisti et al., 2015). Users may deem disclosing inconsequential information to be an appropriate fee to access a service. A report by Pew Research Center in 2014 found that 55% of those surveyed were willing to share some of their information in order to receive a service for free. In that survey categories of information identified as sensitive were social security details, health information, call and message content and location. Of less importance to users were buying habits, media preferences, religious and political views.

Raynes-Goldie (2010) found in her social networks research project that individuals differentiated privacy based on social or institutional parameters with more concern shown for the former. By social privacy users meant being able to fine-tune access to the information in their social network based on their relationship to the contact. What was visible to employers or acquaintances should be different to that seen by close friends.

There was less concern expressed about what commercial organisations might do with their collected information than something getting shared inappropriately with the social group.

After reviewing some recent metrics collected about online information privacy attitudes and looking at some of the reasons why self-reporting cannot be relied on to be completely accurate, the next section will look at smartphone apps one of the main means used to share information.

2.5 Smartphone applications and permissions

The release of the smartphone has led to a revolution in software development where long development cycles had been the norm. The open OS that runs on smartphones has facilitated the creation of a subsystem of software development dedicated to applications for mobile devices known as ‘apps’. Today there is an explosion of apps available that are developed quickly, can be downloaded in minutes and constant feedback is provided to developers. The volume and variety of apps has given individuals enormous choice over how they manage their daily lives and has led to new ways of conducting business, citizen participation and entertainment.

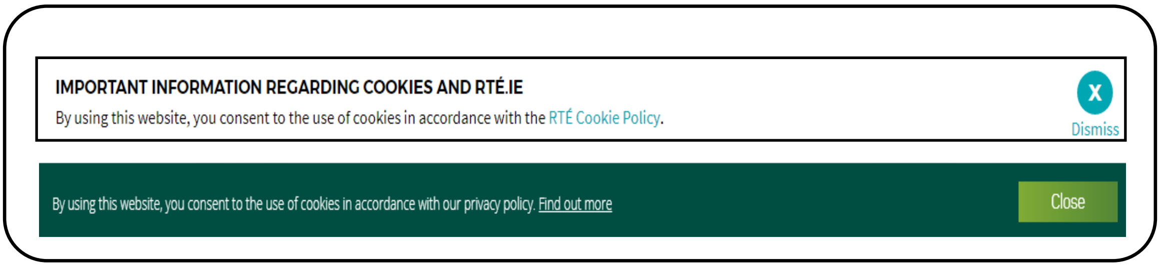
There were 2.8 million apps in the Google play store in March 2017 (Statista, 2017c) segmented into approximately thirty categories covering diverse interests that range from android wear to weather. Consenting to information sharing is a prerequisite to using most apps and this is done via a permission request as an app is installed.

There are a significant number of permissions that an app can request as part of its terms of use. In the Google Play store, the figure is approximately 240, 160+ relating to the device and 70+ to user information (Pew Research, 2015). Some common permissions that are requested by apps are access to location, contacts or camera. The social media service Facebook is one of the most downloaded apps and it requests 46 permissions (Pew Research, 2015).

Online activities that are transacted directly with a website or browser may also be tracked via ‘cookies’, a type of memory for the web. They are stored in the browser and enable a site to retain details between visits allowing for a more personalised experience. They are useful to retain personal preferences like language or currency, shopping basket contents and previous searches. This information retention can over time build up a behaviour profile based on user actions and can be valuable in creating targeted marketing, bespoke services or to offer personalised content.

Both apps and websites must have consent granted by the user to access their content or storing cookies on their device. This granting on consent has left the responsibility for protection of one's information with the user. This may be problematic because in many case the user may not have the expertise in this complex area (Nissenbaum, 2011)

The European Commission Directive 2009/136/EC based on mandated disclosure requires that users must be informed and consent to the use of their information giving them control over the privacy of their online information. Users of a website will be presented with a privacy policy or a terms of use statement that they agree to or cease using the service. This form of regulation is known as 'Notice & Choice' or 'Notice & Consent'. It works on the principle that giving users factual detail about how information collected about or from them will be used allows them to make an informed decision following review of the policy. The notification is usually prominently displayed but the privacy policy details will be contained in a separate link as can be seen in Figure 5 below. There is often no possibility of negotiation or clarification (Nissenbaum, 2011), it is a notification to accept the terms or cease using the website.



IMPORTANT INFORMATION REGARDING COOKIES AND RTÉ.IE

By using this website, you consent to the use of cookies in accordance with the RTÉ Cookie Policy.

By using this website, you consent to the use of cookies in accordance with our privacy policy. Find out more

Figure 5 Samples of Website Cookie Statements (RTE; Dublin Airport, 2017)

Privacy policies are long 2,227 words on average, often use imprecise language that is open to interpretation and omit important details about how information will be collected, shared and used (Marotta-Wurgler, 2015). McDonald and Cranor (2008) estimated the time to read privacy policies at approximately 200 hours per year based on 1,462 unique website visits annually. This was based on only reviewing each policy once.

The obligation is on the provider to supply all the detail a user needs to make an informed decision about consent but this is a challenging task. Online services use complex data flows that may include aggregation of data across website visits, across devices, sharing of data within and between organisations. Privacy policies are subject to regular change as new ways of analysing information becomes possible or new entities enter the ecosystem (Nissenbaum, 2011). It is the responsibility of the provider to articulate these changes clearly and there is an onus on the user to keep themselves informed of amendments as they arise.

There are competing objectives at play in privacy policies, on one side users need to be accurately informed about how their information will be used and on the other to do so in a way that is easily understood. The Directive 2002/58/EC of the European Parliament stated that users be given ‘clear and comprehensive information’ about the nature of data processing. Nissenbaum (2011) calls this the transparency paradox where she argues to achieve both objectives in an evolving online environment is impossible. There are also the competing goals of speed versus due diligence. The advantage of online services is their speed of completion but speed acts as a disadvantage when there is a need to perform due diligence that the correct privacy and security protections are in place (Berinato, 2015).

Users are at a disadvantage to know if a privacy policy is breached Martin (2013). The complex data flows and number of organisation involved in many transactions complicates finding the responsible party in a breach situation. In the Ashley Madison data hack of 2015, it transpired that despite charging users a fee to delete their information, it was never deleted. As well as the embarrassment of having private details released to the world, the users learned that deletion requests they had paid for were not honoured (Guardian, 2015).

Offline people have become used to supplying information about themselves on a frequent basis, a contact number to book a restaurant, home address for takeaway delivery, passport as identification to access a bank account in person. This level of sharing has not led to negative consequences (Norberg et al., 2007) and may have led to the normalisation of sharing information in an online setting and a judgement of it being relatively risk free.

In unison with the rise of mobile technologies and the availability of ‘apps’ has been the explosion of social media and social networking. The success of these new businesses depend on user engagement to create content or build virtual communities. To encourage users to participate and share information, many of these companies have developed expertise in gathering the maximum amount of information with the least number of restrictions (Acquisti et al., 2015). These social media companies are commercial organisations who are trying to get the best returns for their investors so they will try to gain advantage over competitors by leveraging their user base and the information that has been shared with them. Gartner have predicted that by 2021 information portfolios will form part of a company valuation. The volume, variety and quality of collected information and how it is analysed for value will impact the balance sheet (Gartner, 2017b).

Facebook is one of the most widely used social media sites with 2 billion active users (Facebook, 2017), figures released in 2016 stated that 93% of users access the service via a mobile device (Facebook, 2016). The rise of celebrities sharing their lifestyle has become familiar, users also want to be curators of their own life and many experience positive feedback though their social media interactions (Mosteller and Podder, 2017).

Facebook has changed its terms of service and enhanced its service significantly since it launched in 2004, these changes have sometimes impacted on user privacy and received negative feedback from users. In 2007 it introduced beacons that shared user actions with third parties, this was withdrawn in 2009 in part settlement of a lawsuit (Computerworld, 2009). In 2009 in an effort to encourage more open sharing it presented users with an opportunity to update their privacy settings, the default was set to share with everyone, restricting sharing required an active selection (boyd & Hargittai, 2010). Figure 6 shows how the default setting moved from predominately not visible to visible over time.

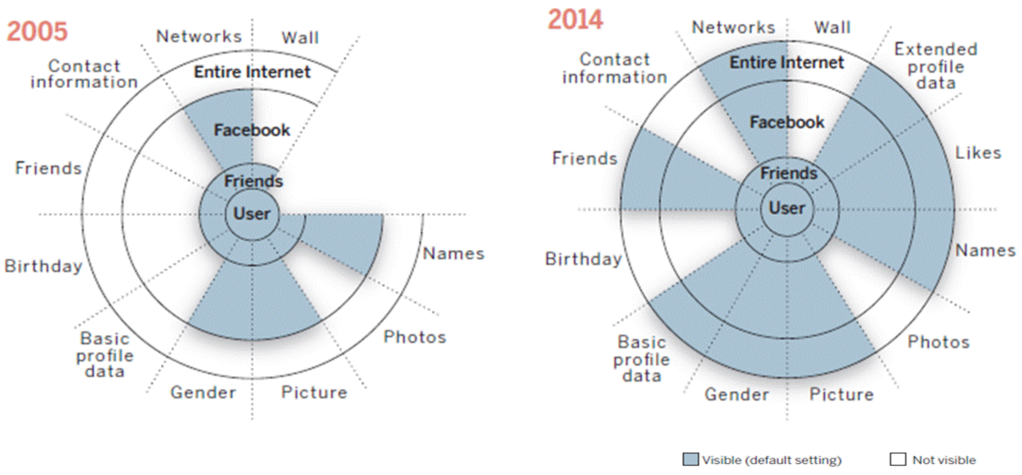


Figure 6 Default Visibility settings in Facebook over time (Acquisti et al., 2015)

People are social by nature and social networking offers an opportunity to expand or maintain social connections. It has allowed users to reconnect with lost friends or enabled them to keep up to date with family and friends living far away in a richer way than a phone call or mail alone can. Acquisti et al. (2015) found that users over time became more comfortable with sharing personal information with their friends on social networks while at the same time they reduced the amount of information shared more publicly highlighting that users are conscious of who and what they want to share. Lowry et al. (2011) also examined the competing objectives of retaining privacy but wanting to realise the interpersonal benefits offered by social media communication finding that users were willing to disclose information about themselves if they believed the benefit accruing from such disclosure was worth it.

Another social networking service that has been widely adopted on smartphones is Mobile Instant Messaging (MIM). As of July 2017, WhatsApp and Messenger had over 1.2 billion users each while the market leader in China, Wechat had almost 1 billion users (Statista, 2017e). WhatsApp claims to have 1 billion daily active users sending 55 billion messages and sharing 4.5 billion photographs (WhatsApp, 2017). Over the last year many of these services have introduced end to end encryption to ensure the messages remain private between the sender and recipient (Pocket-lint, 2017).

Photographs and videos comprise much of the content shared by users through the various social media, for many people their smartphone is their main camera. This makes much of the stored material on the device unique and most users will want protect that information from loss. Many smartphones by default will as part of their set-up create a cloud storage account and implement a synchronisation process to back everything up. This has the benefits of keeping a second copy of the information at a remote location which can be accessed by other devices owned by the user or can be shared with third parties by granting them access.

These services are governed by the same privacy policies and terms of service already discussed and the same due diligence should be applied to ensure the privacy of the stored information is protected.

As has already been mentioned a number of directives have been enacted by the EU and the U.S to protect the information privacy rights of its citizens. The success of these directives rely to some degree on individuals having alternatives to choose from allowing them to select the websites or services that employ privacy policies that are in line with their own views. This model of choice is undermined when organisations merge and the range of options shrinks swaying the balance of power to the service provider. Smartphones have become integrated in the social life of users and many of the apps and services used are selected based on popularity. Once a tipping point has been reached where there is mass adoption and that service becomes the de facto standard. The popularity of Facebook has seen the demise of Bebo, Frendster and MySpace which were popular social networking sites in the early 2000s. Figure 7 shows the leading social network apps in July 2017, Facebook owns four of the top five companies listed, the top two instant messaging apps Messenger and WhatsApp and Instagram. This sphere of influence exerted by Facebook puts them in a dominant market position.

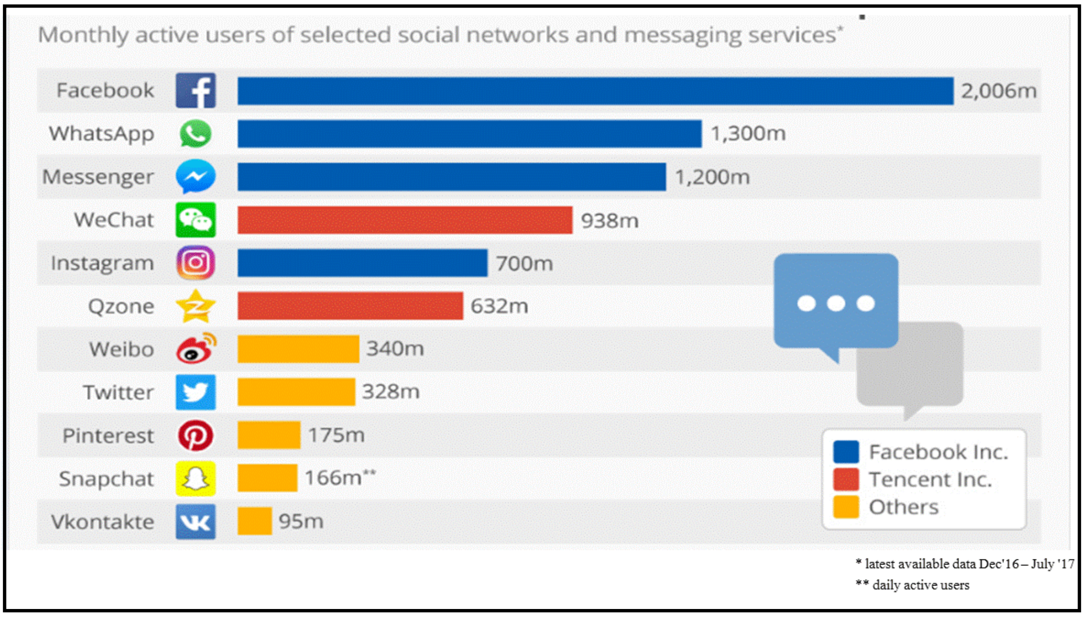


Figure 7 Leading Social Media and Messaging services worldwide 2017 (Statista, 2017e)

This dominance has not gone unnoticed by the EU who investigated the commitments made by Facebook at the time of their takeover of WhatsApp in 2014 when it stated it did not have the capabilities to link the accounts of users of both services. In August 2016 the privacy policy statement of WhatsApp changed to inform users it would be sharing user data with its parent company. This change of privacy policy led the European commission to query whether the sharing of information from both companies had always been the intent. In May 2017 they ruled they had been misled and fined Facebook €110 million (EU Commission, 2017).

Reflecting on some of the numbers that have been shared already: 1.4billion smartphones sold in 2016, 2 billion active Facebook users, 55 billion WhatsApp messages per day, there can be no doubt about the amount of data that is being generated. There has been an understanding within the IT industry that individual information privacy could be protected by anonymising data prior to analysis. One of the techniques used is to remove any unique identifiers like a passport number or address contained in the data set. This would allow large volumes of this anonymous data to be analysed and insights derived without compromising the privacy of any single individual. This method of an anonymisation has been questioned by De Montjoye (2013) who has carried out a number of experiments using anonymous mobile phone location information only and he was able to uniquely identify 95% of the users. This puts into doubt that information once it has been collected remaining private no matter how few identifiers are contained within it.

Section 2.5 has discussed the development of unique app software for mobile devices. It looked at the role of permissions and consent has in the relationship between the user and the service provider and the challenges that exist on both sides to meet their obligations. Finally there was a brief review of some examples of how information sharing is manifesting itself. The next part will look briefly at the some of the reasons why smartphone technology has become so embedded in society.

2.6 Social Imperative

The reason smartphones has been globally adopted in such vast number has been driven as much by social imperative to be part of the community as any technological advances. The most common way for offline events to be suggested, co-ordinated and captured is through a variety of online tools and those who are not part of the online communities may miss out.

When mobile phones were introduced they offered a chance for person to person communication, the dependence on the shared fixed landline and shared answering service were eliminated. This freedom created the environment for the mobile phone and subsequently smartphones to become associated with personal identity in a way other technologies never have (Strivastava, 2005). This can be described as a type of attachment, based on symbolism, aesthetics and necessity (Wu et al., 2017). Each new Apple iPhone generation has been accompanied by people queueing for days ahead to purchase it (Telegraph, 2016). Buying the latest model of smartphone is not just about getting the improved technological capabilities, it has been influenced by its symbol of status and the elegance of design (Wu et al., 2017).

Society is governed by social norms, unwritten rules that people adhere to that allow the smooth operation of daily activities. These may differ by culture but they accumulate over time to become rooted in the social group. The pace of change in technology has outpaced the slow progression of social norms (Sloan & Warner, 2014).

There is the argument that users are not being forced to buy a smartphone or to participate in social networks or use apps that require sharing but that ignores the social cost and general inconvenience of not participating (Raynes-Goldie, 2010). An online identify is becoming as necessary as an offline one. A brief example of this was reported in the Guardian (2014) when a woman had problems using Airbnb to book accommodation as she did not have enough Facebook friends to verify her online identity, a hundred online friends was deemed to be an acceptable number.

2.7 Summary

The literature has demonstrated the complexity of this field, the many facets of what is meant by information privacy and shifting boundaries between shared and private. The desire to benefit from the convenience offered by technology while maintaining control of information flow has been discussed. This chapter has considered how the smartphone has become a universal device in the space of ten years, how it has been a transforming influence across the spectrum of human endeavour through apps and persistent connectivity. This has led to the creation and sharing of more information than ever before. This is set to continue with other connected smart devices becoming more pervasive leading to more information being generated from an expanded range of sources. Smart homes, self-drive cars and personal robots are no longer future concepts they are here.

Technology will continue to advance and present more challenges regarding information privacy. Recently, 32Market a U.S company is offering employees the option to have a microchip implanted in their hand. Those who avail of the offer will be able to use the chip for site access, to purchase food and sign-on to their PC (32Market, 2017). This is one of the early implementations of digital and biology combining for convenience. This specific device is not trackable but in future it can be expected that the range of functions an embedded chip could perform will increase and implantation may become the norm.

These innovations offers new possibilities to create knowledge, provide a better user experience and offer enhanced services to everyone. On the other side the implications for privacy should be continually monitored and an appropriate balance established between individual rights and the greater good of humankind. The future possibilities that technology offers are limitless but it is important that they are not blindly embraced without due diligence.

3. Methodology and Fieldwork

3.1 Introduction

The purpose of research is discovery carried out with purpose in a logical and systematic manner (Saunders et al., 2016). There is not a single research strategy that is appropriate to answer every research problem, and it is accepted within the academic community that there are a number of schools of thought and approaches available. While there are disagreements on a single best approach there is consensus that there is an interdependence between the research philosophy, research design, research problem and research method in guiding the approach adopted (Creswell, 2014; Saunders et al., 2016). Denscombe (2010) adds the important caveat that the chosen strategy must be both feasible and ethical.

Based on these considerations, the following chapter will describe and justify the research strategy adopted to answer the research problem. The chapter begins by discussing the research framework and how it influences the philosophical choice and research design. There is an overview of current research philosophies and how they apply within this study. Then there is an examination of the approaches available with their associated benefits and limitations. The chapter concludes by outlining the data collection method followed and some of the limitations that were encountered over the course of the project.

3.2 Research Framework

The research question is concerned with exploring the attitude that users have towards information privacy when using their smartphone. In answering the question this research paper will follow a constructivist ontology, an interpretive epistemology and inductive methodology in the analysis of the data. This is in harmony with the research question that is investigating the opinion of smartphone users and interpreting meaning from the data collected.

The starting point of this research project was defining the framework or worldview in which to situate it. In establishing the framework, there are some fundamental questions that need to be addressed: the axiological, ontological and epistemological position in relation to the research question. The answers to these questions influence and are influenced by the research topic.

The Axiological Question

Axiology is concerned with the role that values and ethics have in a research project. It asks a researcher to reflect on how their own principles and biases will influence the research process. The values held by the research participants must also be considered. These ethical questions are especially pertinent in a qualitative interpretivist study where the values held by researcher and participants are integral to the process. The ethics of a researcher directly impacts the data collected and how it is interpreted (Creswell, 2013).

The Ontological Question

This explores the nature of reality and how can it be understood. It splits into two theories, objectivism and constructivism or subjectivism.

Objectivism proposes that there is a single defined reality that exists independently of people and at its extreme everyone experiences the same thing and this reality is unchanging (Saunders et al., 2016). Objects have value in their own right and that value exists independent of human interaction (Crotty, 1998), in this approach a researcher is objectively examining a phenomena that is constant and not influenced by human actions. This is suited to statistical, repeatable and mathematical research where a researcher does not influence the data and can analyse it in an objective detached manner.

Constructivism takes an opposing interpretation, it works from the perspective that there is not a single reality but multiple realities that are ever changing based on interpretation. It is mostly associated with the social sciences. It is the actions and interactions of individuals that create or construct these multiple realities based on their understanding and experience of a situation. Meanings are not discovered but constructed (Crotty, 1998). This viewpoint accepts that the realities may be influenced by a researcher, the participants of the study and those reading the findings (Creswell, 2013).

To answer the research question about attitudes users have towards the privacy of their information when using a smartphone requires getting feedback from individual smartphone users. These views are subjective based on unique personal experiences and this lends itself to a subjective than objective perspective.

The Epistemological Question

Once the nature of reality is defined, in this case a constructivist one, it leads into the question of how knowledge can be acquired or what constitutes as knowledge within the parameters of this reality. There are different categories of knowledge from accepted facts and figures to beliefs, opinions and stories. The type of knowledge being sought and the relationship between researcher and research subject governs the choice of epistemology. Saunders et al. (2016) categorise the choices under the umbrella of research philosophy.

3.3 Research Philosophy

The espoused philosophy will guide the research approach that is undertaken and all subsequent decisions that will be taken. Saunders et al. (2016) developed the concept of the research onion to provide guidance around the decisions that will need to be taken during the lifecycle of a research project. At the outer edge of the research onion shown in Figure 8 are the research philosophies, identified as positivism, critical realism, interpretivism and pragmatism.

Positivism

Positivism is focused on measurable facts and figures rather than feelings or impressions, it is concerned with the importance of 'the given' (Saunders et al., 2016, p.136) or 'the posited' (Crotty, 1998, p.19). The positivist's aim is accurate verifiable data collected in a detached objective manner as in scientific research. Human factors should not influence the data, either on the part of a researcher or participant contributions. It is important that distance is maintained between a researcher and their research subject to ensure objectivity. Quantitative data collection providing large volumes of data that offer statistical accuracy is most associated with this philosophy. Positivist inquiry mostly adopts a deductive approach to theory development where repetition of testing and verification of findings is important. This repetition allows results to be confirmed and may be seen as more credible research form than one which discovers something unique that cannot be replicated. It is not suitable to apply to research involving subjective data that requires interpretation making it inappropriate for this research project (Saunders et al., 2016).

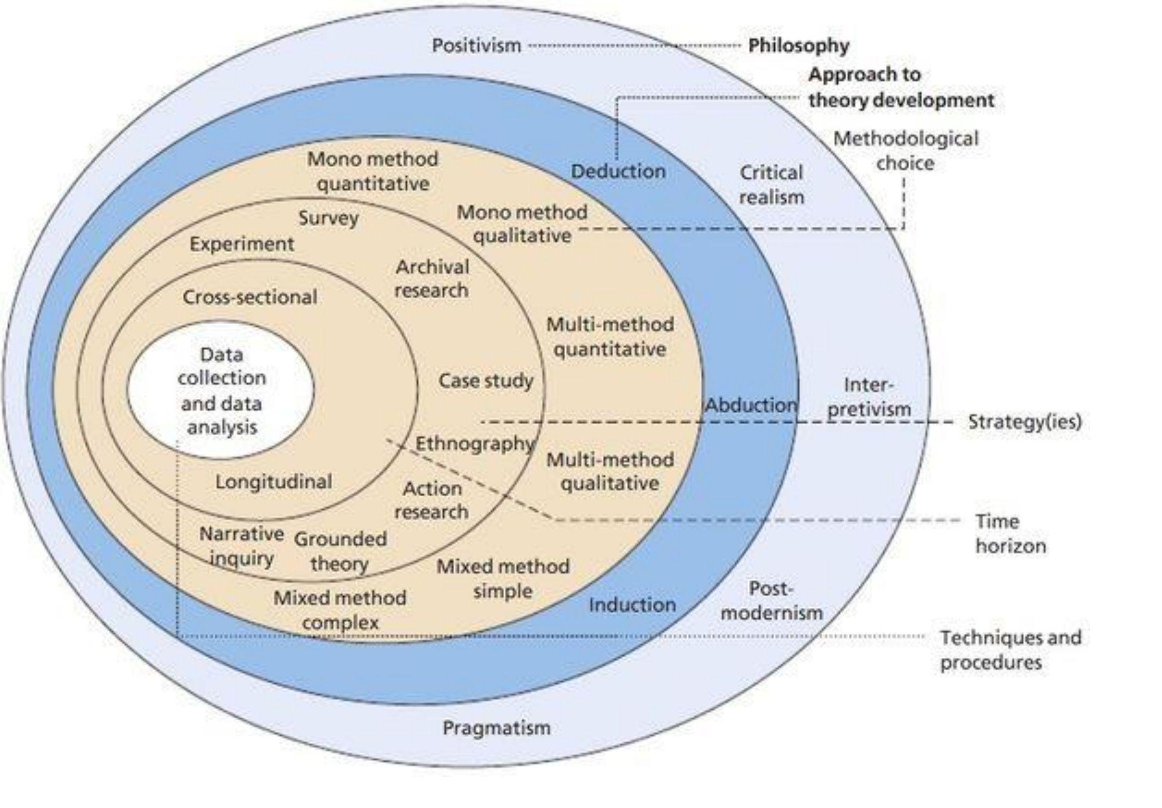


Figure 8 The Research Onion (Saunders et al., 2016)

Critical Realism

This shares many attributes with positivism but unlike positivism it believes that the objective reality that exists can be deceptive and observing using human senses alone cannot be trusted to be wholly accurate (Sekaran and Bougie, 2013). The theory developed by Bhaskar in the late 1970s strives to separate the reality as it exists from how it is interpreted. It poses that the way knowledge is acquired is always influenced by the social constructs from which it is being viewed and that this interpretation can change over time. Critical realists argue that research findings should be viewed in the context of the time period when they were produced and the influences of that period be taken into account. Like positivism it is associated with objective data and was not deemed an appropriate approach for this project (Saunders et al., 2016).

Pragmatism

Pragmatism is about adopting an approach which places the research question at the centre of the strategy. Pragmatists do not limit themselves to a single philosophical approach to answer a research question. They can combine interpretivist and positivist viewpoints and use both qualitative and quantitative research methods to get the greatest understanding and multiple viewpoints (Creswell, 2014). Their research purpose is to provide practical answers that can be implemented rather than contributing to theoretical debates (Saunders et al., 2016). This research question does not lend itself to a solution type answer eliminating pragmatism as a suitable approach.

Interpretivism

Interpretivism distinguishes research involving people and social constructs to be different to that involving physical objects. It appreciates that people are subjective and bring different perspectives to a problem depending on their own experiences and this perspective can evolve over time or within different social settings. Subjectivity exists on behalf of both the research participants and the researcher. Interpretivism tries to capture the richness and complexity of diverse opinions and make sense of them (Creswell, 2014). While inquiry based on positivism and realism attempts to find consistency in their findings, interpretivism is seeking to uncover something unique, the point of view of the individual (Crotty, 1998). Where the emphasis is on words and feelings, empathy on behalf of a researcher is important to gain trust and uncover meaningful insights into participants experiences (Saunders et al., 2016). This philosophy benefits from a researcher getting close to those being studied (Creswell, 2013).

This research question is concerned with examining the attitude users have towards the privacy of their information when using a smartphone. This is a relatively new phenomena that is evolving and changing as the technology advances as has been discussed in Chapter 2. To answer the research question entails uncovering the distinct and multiple opinions of individual smartphone users. These subjective opinions have been formed based on personal experiences and by the influences of social and cultural norms. This results in complex and varied data that requires interpretation.

To satisfy the complexities identified, a constructivist ontology that accepts that reality is an ever changing social construct and an interpretive epistemology that will focus on uncovering meanings from the collected qualitative data has been adopted.

3.4 Theory Development

Theory development and testing is used to explain and contextualise collected data. There are two main approaches to the development of theory inductive and deductive, whereby the former is primarily concerned with generation of a theory, the latter in validation of an existing theory (Creswell, 2013).

While neither is prescribed to a given philosophy, an interpretivist philosophy is usually associated with an inductive approach using qualitative data while a deductive approach is mostly linked to a positivist, objectivist perspective using quantitative data. Table 1 gives a high level comparison between the two philosophies.

	Qualitative	Quantitative
Principal orientation to the role of theory in relation to research	Inductive: generation of theory	Deductive: testing of theory
Epistemological orientation	Interpretivism	Natural science model in particular positivism
Ontological orientation	Constructionism	Objectivism

Table 1 Fundamental differences between quantitative and qualitative research strategies (Bryman, 2016)

Inductive versus Deductive

A deductive approach begins with a theory and from it a hypothesis to test is developed. The hypothesis is concerned with identifying a relationship or link between defined variables under prescribed conditions. Sekaran and Bougie (2013) describe it as starting with a general theory and applying it in a specific instance. Data is collected and used to test the validity or not of the hypothesis. The test or tests are predefined and the variables are usually measureable. Findings are generalised requiring large sample sizes making quantitative data most appropriate (Saunders et al., 2016). The type of data that can be collected is narrow in scope in order to meet the pre-requisites of the hypothesis and does not allow for deviation. The success of this type of approach relies on the experience of a researcher to develop a robust hypothesis and prescriptively define the test data required ahead of data collection (Bryman, 2016). A deductive approach is often associated with natural scientific research. The lifecycle of this approach can be seen Figure 9.

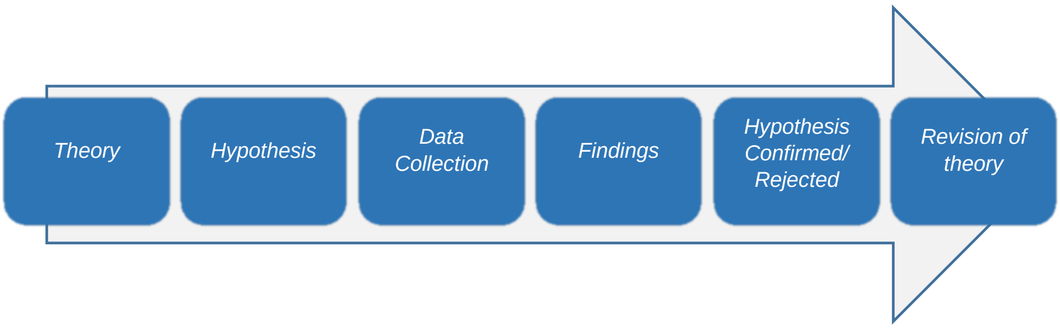


Figure 9 The process of deduction (Bryman, 2016)

An inductive research approach works in the opposite way. It takes collected data and from it tries to understand the meanings, patterns and relationships that exist. From this a theory is developed to explain the phenomena as shown in Figures 10. There are no preconceived hypotheses at the beginning of the process and this gives a researcher scope to expand or delve deeper into particular aspects of the research topic that prove relevant. It allows for rich data to be captured using words and images and allows complex situations to be investigated and analysed. The sample size is usually small allowing for in-depth investigation. The aim is to take specific instances and see if they can be applied in a more general sense. Following an inductive approach theory becomes the outcome of research (Bryman, 2016) and it is most associated with the social sciences.

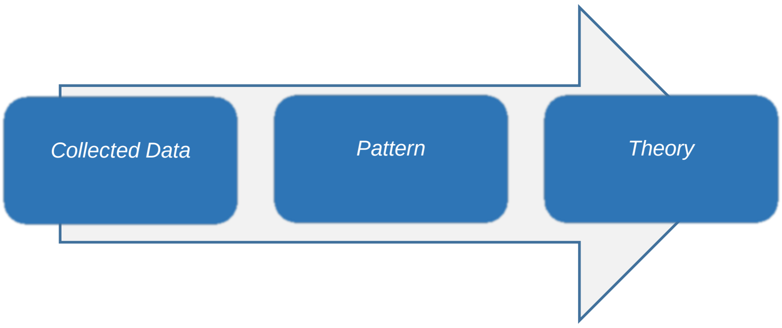


Figure 10 Inductive Reasoning Approach

This research question is exploring the attitude of users towards information privacy when using their smartphone. The aim is to capture the opinion of smartphone users who have a variety of experiences and perspectives. There was not a defining theory at the start of the project to test against, making a deductive approach inappropriate. An inductive approach that seeks to understand the phenomena is suited to answering the research question and it is in harmony with the constructivist ontology and interpretivist philosophy already selected.

3.5 Research Methodology

Following on from the philosophical assumptions underpinning the research approach and the interpretive lens through which to parse the data are decisions around the mode of enquiry (Kumar, 2014). This can be characterised into two broad practices of data types, qualitative and quantitative.

Quantitative research is commonly associated with numerical data, the emphasis is on measurable objective facts that are detached from a researcher (Denscombe, 2010). It is often associated with a positivist philosophy. Typical research methods used include surveys, questionnaires and experiments. These methods are pre-set and offer little flexibility once they have been set in motion.

Qualitative research using words or images as data allows for a more subjective interpretation and is more frequently linked with an interpretivist philosophy which is in keeping with this research project. The data collection methods available include interview, focus group or observation. These methods allow some flexibility to change during the process of data collection if it is of benefit to the study (Kumar, 2014).

Quantitative data collection methods are well established and mechanisms to measure validity and reliability have been defined (Saunders et al., 2016). The same measures cannot be applied to the gathering of qualitative data. Creswell (2013) discusses some of the approaches that can be used instead to develop rigor. He explores options like building trust with participants to help with the accuracy of the collected data, use of multiple sources and accurate presentation of all findings especially anomalies to show a realistic representation. He suggests presenting findings with a ‘rich thick description’ (p. 252) so the reader can place the results in context.

Traditionally either a quantitative or qualitative method was followed resulting in a mono approach (Saunders et al., 2016) but there is also the possibility of combining the two in a mixed methods approach. Following a mixed methods approach allows for complimentary data to be collected and may provide a more comprehensive answer to the research problem.

To address this research problem, a qualitative approach was chosen. This was to allow a holistic picture of the attitudes users have about smartphone privacy to emerge. It was decided that a quantitative approach would be more rigid in nature and had limited scope to provide the detailed data required for this exploratory research.

There are a number of data collection methods that can be used to provide qualitative data, some of the most common are: observation, focus groups and interview.

Observation was not appropriate in this project as it would not provide any insight into the reasoning behind the actions participants would take. It could be useful as a tool to verify that actions matched statements. This was not practical given the scope and time span of this project.

Focus groups have the ability to provide the rich data required but they are difficult to organise and manage so that all opinions receive equal attention. For the reason of practicality they were not selected.

Interview was selected as appropriate in this instance as it allows for a more exploratory approach in answering the research question. It allows for clarification from both sides where there is any ambiguity about the question being asked or the answer given. There are three types of interview: structured, unstructured and semi structured.

A structured interview is similar to conducting a survey in that it uses predetermined closed questions with a limited number of answers. This tight structure allows for analysis and comparison of answers less complicated (Denscombe, 2010).

Unstructured interviews puts the interviewee at the centre of the process. There is little prompting from the interviewer and the interviewee is allowed to freely express themselves about the topic under investigation.

The semi-structured interview borrows from both the structured and unstructured approaches. While being flexible there are pre-set open questions that are used to guide the interview and keep focus on the area of interest. There is flexibility within a semi structured interview to explore or expand on areas that become relevant during the course of the interview. This gives the option to examine areas that might not have been considered by a researcher as part of the planning exercise (Sekaran & Bougie, 2013). The use of similar questions across all participants allows analysis of responses to be done more easily. This was the option selected to gather data for this research project.

A good interview is dependent on the skills of the interviewer to obtain quality data. A researcher needs to be listening for responses that are new or interesting and be aware of when it is appropriate to intervene or allow the conversation to flow. This level of responsibility brings disadvantages as there can be bias based on the perception of the interviewee to a researcher or sensitivity to the questions asked (Denscombe, 2010) which may influence the answers given. There also can be bias on the part of a researcher who may come with preconceptions of the expected answers.

3.6 Research Design

The research design is the detailed plan of how the research question will be answered in a valid, accurate and objective way within the already defined philosophical boundaries (Saunders et al., 2016). The detail provided within the plan should allow the study to be repeated independently by another researcher.

The plan will provide details around the following:

- Who will be part of the study?
- How will they be found?
- What method of data collection will be used?
- How will data collection be carried out?
- Over what time period will the study take place?

The participants in this study were experienced smartphone users who were proficient with the technology. The sample size was small with six participants.

Convenience sampling was used to identify participants who were contacted via email or by phone and asked to participate in the study. If they expressed an interest in participating during that initial contact they were provided with a participant information sheet detailing the background to the research project and the parameters around their contribution, a copy of this is contained in Appendix B. Following agreement to participate all interviewees were advised that their participation was voluntary and could be revoked at any time during the research process.

The data collection method was semi-structured interviews conducted face to face at a location and time chosen by the participant. The interviews were audio recorded in addition to note taking to enhance accuracy in conducting the analysis. This helped with reliable capture of the contribution of the participants. Permission to record was included on the consent form signed at the beginning of each interview, a copy is contained in Appendix C. Participants were assured of anonymity and that all data collected would be protected, kept confidential and destroyed when no longer needed. It is hoped that this assurance helped to get accurate and honest responses to the questions posed.

A draft schedule of questions was prepared as part of the ethics approval process to guide the interviews. The questions were designed to be open and unbiased with the aim of provoking accurate and thoughtful responses from the interviewees.

One pilot interview was completed to check the appropriateness of the proposed questions and ensure the structure of the interview was logical. Feedback about anything that the participant felt had been overlooked was sought. Based on this trial, some questions were deemed superfluous and the order of others was altered to improve the flow. The final list of the questions used are listed in Appendix D.

The questions were divided into five sections

General: these were designed to put the interviewee at ease and get an overview of their smartphone use and familiarity with technology. It also set the baseline for their attitude in general towards information privacy.

Online Activities: this explored what interviewees used their smartphone for and to explore activities that they would not use their smartphone for.

Mobile Applications: this looked at the number and type of ‘apps’ interviewees had on their smartphones and the rationale behind their selection.

Storage: this examined the type of information stored on the devices and the methods used to protect it.

Privacy: these questions were about the attitudes interviewees had towards their information privacy when using their smartphone and whether it was in agreement with their previous statements.

The data collection period lasted five weeks from 24th May to 30th June 2017.

3.7 Ethical Considerations

As already discussed in section 3.2, the ethics and values of a researcher are an important consideration in any research project. In addition to the personal values held by a researcher are the good governance practices adopted to ensure accuracy and validity are maintained throughout the process (Sekaran & Bougie, 2013; Saunders et al., 2016). When the area of study involves direct interaction with people then particular attention must be paid to ensure they are protected and commitments made by a researcher are adhered to. As this research project involved interviewing people, ethical approval from the school of Computer Science and Statistics, Trinity College Dublin was requested and granted.

A copy of the ethical application forms are included in Appendix A.

3.8 Limitations

This research project has a number of limitations due in some part to the time limit imposed to complete the study and some due to the lack of experience on behalf of the researcher.

A future study would benefit from an expanded sample size, this could be helped by using video calls as well as face to face interviews. Video interview would still allow body language to be observed while overcoming difficulties of scheduling face to face meetings.

Interviewing people is a skill that takes time and practice to develop. Each interview that was conducted brought new learnings. There were contradictory answers given in some of the interviews and challenging those without making an interviewee uncomfortable was difficult and clarifying the contradiction was not always achieved.

To enhance the accuracy of the data collected it would have been beneficial to be able to verify some of the statements made by participants especially those around cloud storage and use of location services. These functions are often enabled by default on a smartphone so a user may not be aware of all of the utilities they are using. Verification would have required interrogation of the smartphone itself and access to their smartphone history. This was not something that had been included in the ethical approval documents and it would require a greater commitment on the part of interviewees to grant this expanded access but it is something that should be considered in a future iteration of the study.

4. Findings and Analysis

4.1 Introduction

This chapter will present the analysis and findings from the primary data that was collected as part of this research project. As outlined in chapter 3, the method of collection was semi-structured interviews conducted face to face with six participants. Section 4.2 will elaborate on this.

The chapter will then go on to describe the approach to analysing the collected data. It will discuss the themes that emerged, the interpretation of those themes and how they adhere to some current IS theories.

4.2 Data Collection

The interviews took place between the 24th May and 30th June 2017. The detail pertaining to the selection process have already been provided in the previous chapter. It was estimated that interviews would take between 40 and 60 minutes, on average there were a little shorter at 35-40 minutes. As the research was of an exploratory nature into a social area of interest, semi structured interviews allowed for rich descriptive answers while keeping a boundary on the topics for discussion.

The subjective nature of individual interviews relies on rapport and trust being established while at the same time maintaining distance so as not to lead interviewees in their answers (Kumar, 2014). In this project the interviewees were known to the researcher so gaining trust was not an issue but it may have influenced some of their answers as they would not have felt completely anonymous. The questions were designed to be open and unbiased so as not to suggest answers or show opinion in order to minimise the possibility of unreliable data being collected.

Each interviewee was asked the schedule of questions included in Appendix D, additional questions were asked to either elicit more detail based on a given response or for clarification purposes. Questions were not deemed to be sensitive in nature but prior to the commencement of each interview the participant was advised that they were free to decline to answer any question they did not feel comfortable answering. That situation did not arise and all questions were answered. The interview format grouped questions into logical categories beginning with the general and then moving into specific areas. Interviews were audio recorded and notes taken to supplement the recording. Following each interview the audio recording and notes were reviewed as recommended by Grbich (2007). This allowed for initial impressions to be formed and contemporaneous observations to be added to the notes. This initial review was useful as a form of critique of interview style and to identify gaps in the gathered data. There was an attempt to bring these learnings into subsequent interviews. Each participant has been designated a label from P1 to P6 to preserve their anonymity and quotes are attributed on that basis.

The data seeks to answers the following research question

What is the attitude among smartphone users towards their information privacy when using a smartphone?

4.3 Qualitative Data Analysis

Following completion of all the interviews, the process of data analysis began. The first step was to review all of the collected material as a whole and identify any common themes or distinct differences between the contributions. This can be characterised as an inductive analysis where the significant findings are allowed to emerge from the raw data (Thomas, 2006).

Unlike quantitative data that generally comprises of numerical data that can be analysed using statistical methods, qualitative data comprising of words does not lend itself easily to statistical analysis. The questions that were posed as part of this study were discursive in nature and analysis was an iterative process with multiple reviews of the collected data performed until no new insights were derived.

All of the interviewees while not specialists in IT or information privacy were familiar with technology and used it almost daily. They all declared themselves proficient users of IT and all have been smartphone users for at least seven years. The small sample size does not provide enough variation to attribute findings based on age profile or gender.

Early in the interview, participants were asked to rate how important they felt information privacy was. This was to garner their baseline attitude and to ground the concept in their mind. There was widespread agreement among all those interviewed that information privacy was important or very important and was something that should be protected. There was a caveat given by two interviewees that people be given a choice about how privacy measures are applied, they had an appreciation that what one person would deem private or sensitive would not be the same as another. At the top of the list for information privacy protection was information about minors, financial transactions and unique identification like a passport or a driving license number. Other categories that might be considered sensitive like political opinions or health information were not raised by anyone.

4.4 Smartphone Device Privacy

Access to the smartphone device is one way that information privacy can be breached and the majority of interviewees took basic precautions to prevent direct access to information on their smartphone. With the exception of one interviewee, everyone had set a password and enabled auto lock. The person who did not have a password set used a separate smartphone for work and that device was password enabled. When queried about a lack of password on his personal smartphone, he said he had 'nothing to hide' (P4) and there was nothing of value on the device. Everyone else had a single device for professional and personal use.

When more advanced measures were discussed like remote data wiping of the device, device tracking or the use of encryption software, application was limited.

All participants were aware or assumed that they could remotely track their device but no one was sure how to do it or had not enabled the function. 'I have but I don't use it. I haven't enabled that. I think I have on Android I know that's what's on the iPhone' (P1).

It was a similar situation with regards to the remote erasing of data on the device. Only one person had ever lost their smartphone and not recovered it and he thought he would not have been able to remotely remove everything off the device as it was already powered off. That is not an accurate interpretation of the capability. Provided that remote tracking was enabled, the next time it was powered on the erase function could have been initiated (Apple, 2017). This shows that are misunderstandings about some of the enhanced utilities available on smartphones.

Encryption or malware software was installed by some users but this was mostly as a result of enforcement by corporate IT policies. Two of the participants remarked that they had previously had encryption software installed but not on their current device. The reason given for not installing on their current device was they had not been mandated to by their IT department whereas previously they had been. On reflection, they did think it was a good protection measure to have in place and the interview prompted them to investigate installing it again.

Participants were conscious of clearing their information off a device when it was no longer in use by them. As all had been smartphone users for at least seven years they had replaced their device a number of times. Except where the device was broken beyond repair, all had deleted everything on the device and in addition half of those interviewed performed a factory reset. In the majority of cases the location of the old working devices were still known to the participant, they had either recycled them to a family member or kept securely stored.

In general everyone was applying updates to both the smartphone OS and the apps as they were made available. There was widespread trust in the providers that updates were secure and necessary.

4.5 Connecting Online

All participants said they were cautious about using unsecured Wi-Fi both from the perspective of the locations where they would use it and what they would use it for. Interviewees were more likely to use it in an establishment familiar to them than somewhere they did not know and would be especially careful when abroad. Familiarity was a bigger factor than any security based one.

‘Let’s say I use Dublin Airport open Wi-Fi, I use that a lot there’s a few hotels in the local area I’d have used that quite a bit. Em familiarity and gut feeling type of thing, there is no real technical logic behind it so to speak it is more of a familiarity and gut feeling I would say’ (P1)

All participants were reluctant to use open Wi-Fi if they needed to register and provide an email address. This was partly due to privacy concerns but mostly due to the potential of unwanted spam messages. All interviewees said they would not use unsecured Wi-Fi to perform sensitive transactions like banking or something relating to their job. It was useful to check news updates or to browse the web. Everyone estimated that they connected online via secure networks over 90% of the time and because of that there was no reason to use open Wi-Fi for anything sensitive. All interviewees were aware of the enhanced security that secure Wi-Fi or a virtual private network offered and would wait until either of those was available to complete activities they deemed private.

4.6 Smartphone Services

One of the capabilities that a smartphone possesses that other computing devices cannot offer with the same accuracy is location tracking. Interviewees were evenly divided into two distinct strategies on this. One group of users had location switched off specifically due to privacy concerns. They would only enable it when required for services like satellite navigation and then turned it off again as they did not want their movements to be tracked comparing it to 'surveillance'(P1) or 'tracking'(P2) or cited the collection of location information as 'very invasive'(P5).

One interviewee reported not installing apps that had requested access to location details when it did not make sense to them why it would need that type of information.

'For some of them where they are looking for your location em and I think the location is relevant I mightn't sign up for the app. So for example Spotify, I was going to set up Spotify on my phone but they were looking for my location and I decided not to set it up because of that' (P2)

The other group had it switched on permanently, were aware that it was constantly collecting information but did not have any concerns about this in connection to information privacy. There were some minor concerns about the potential of using collected information to perform user profiling and targeting of unwanted advertisements but to date that had not been an issue. They cited the vast amounts of information already held by the mobile operators and search engines and location was just another constituent. They did not think it added anything significant to what was already collected.

Services like mobile data and Wi-Fi were generally always on. Bluetooth use was limited by some participants but this was a measure to conserve battery.

4.6.1 App Usage

The number of apps downloaded by each person did not exceed thirty, with most having an additional ten to twenty apps to what was installed by default on their smartphone. Everyone interviewed said they only downloaded apps that were of particular interest or considered useful to them. Participants had not accessed the app stores to check on current trends or to download apps based on popularity. Word of mouth from peers was an important influence in deciding to use an app. Many of the participants commented that it was the main reason why they had downloaded some of apps they were using. People rarely removed an app even if they no longer used it. Exceptions were where it was found to be excessively consuming battery.

The only common social media application used by all participants was WhatsApp with most using it daily followed by Facebook which was used by less participants and on a less frequent basis at two to three times per week.

Some of the other social media apps in regular use were LinkedIn, Instagram, Twitter, Pintrest and Viber as shown in Figure 11 but none were used by all interviewees.

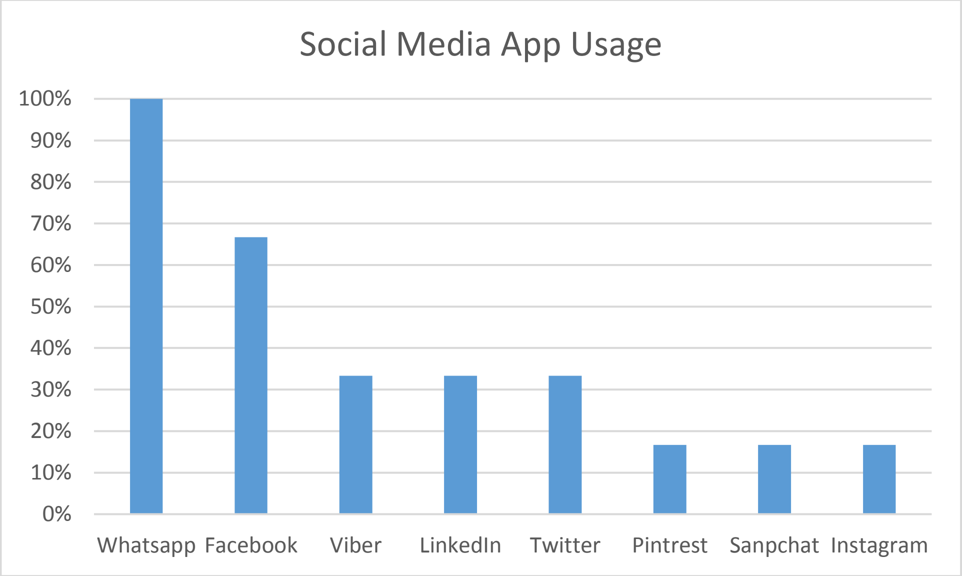


Figure 11 Social Media App Usage among Participants

Some of the reasons given for the popularity of WhatsApp were its ease of use, functionality, pervasiveness and it is free to use.

Interviewees liked the intuitive user friendly interface that allowed the easy sharing of updates including photographs and video. The ability to be able to create multiple distinct virtual networks and treat each one differently was listed as a benefit.

‘Lots of other people use it, it’s a brilliant way of sending messages and photos’ (P3)

Within a group message, the functionality allowing everyone to chat to each other and see all responses was preferable to text where only the initiator receives an update. One person remarked it was good for coordinating a group when travelling, acting as a failsafe if anyone got lost or into trouble. The widespread adoption among their peers allowed for virtual groups to be easily created. Viber was also used by some of the participants but they found creating a Viber group less straightforward as the probability of their peers using Viber were less likely. As one participant said of WhatsApp 'the fact that it's so popular makes it more popular' (P2).

Within social media use there was a distinction between what was shared through instant messaging and what was shared through other social media apps. Those who used Facebook in addition to WhatsApp felt they had more control over what they shared within a WhatsApp group than when sharing within Facebook. The perception of control when sharing information in WhatsApp was that participants felt the communication was person to person or person to a controlled group. 'You know where the content is going, you know who's involved' (P3). In contrast on Facebook there was a feeling of having little control over further sharing. 'If I take Facebook for an example you can go only share with friends, but then once you share with friends you have no control over what that friend decides to do with the information they could share with their friends so once it's out there you lose control' (P2).

One of the areas that was specifically identified as requiring privacy protection was information about minors, some of the interviewees who had children said they did not share information online about them. During the course of the interview the same participants acknowledged that they had shared photographs via WhatsApp while they would not have done the same on Facebook, again this was down to a feeling of control and knowing the boundary of sharing. 'When I put a picture on WhatsApp it's like person to person or even if it's a group, it's a group you have control over whereas with Facebook you have people requesting to be your friend and it is harder to ignore them and keep control.' (P5)

They was no mention of the encryption offered by WhatsApp, it was the understanding that there was a boundary set around the virtual group. WhatsApp appears to have become the de facto means of communicating for many social groups, sports teams and schools. It is perceived to be free as it uses Wi-Fi compared to SMS messages that incur a cost.

Everyone was aware that WhatsApp is owned by Facebook and there is some sharing of account details between the two companies but this was not a cause for concern with any of the interviewees. For those who did not have a Facebook account it made no difference to them and for those with an account they used both platforms and accepted that account information would be shared. Most of those interviewed commented that the majority of information they shared on the platform was not sensitive and for that reason they were not concerned if it got hacked or shared. This was in agreement with earlier statements about restricting what they shared.

Those that used Facebook reported they posted infrequently and used the platform primarily to keep up to date with what the contacts in their social group were doing. There was more reflection on what was posted on Facebook than shared via instant messaging. Some minor regrets were expressed about things that had been posted in the past. There was a sentiment that different decision criteria would be used now that there was more familiarity about the service. One participant commented that he was more aware now that everything posted was permanently kept by Facebook and that made him more reluctant to share content now than in the past. ‘Used to put up loads of pics, whatever pictures if you were out or whatever wouldn’t care, now I’d be more careful’ (P4)

For the participants who did not use Facebook there was a particular perception of it having the potential to encroach on their privacy more than other social media services. It was presented that by using Facebook in some way it would result in revealing much more about themselves than they would want. P6 commented that his reasons for not using it was ‘Don’t want everyone knowing about me’ and another participant said ‘pure privacy thing, don’t like people knowing what I’m doing every minute of the day and that’s what people use Facebook for’ (P1). Both participants had never had an account and it was interesting that the perception was using the service would result in a type of surveillance rather than voluntary participation.

On other social media apps like Twitter, LinkedIn and Instagram the main practice was to follow people and keep up to date with events. The creation and posting of content was done infrequently. ‘Twitter is very rarely posts, it’s just following a few people, em a few things, more from information receiving rather than information generation or sharing’ (P1).

There were a number of reasons given for not using some of the other social media apps or downloading additional apps. One interviewee did not see the need to have multiple ways of staying informed, ‘Most people post things on multiple platforms so if you are on two or three different platforms you’ll get the content, it’s just a duplication of the same stuff’ (P4).

Two participants stated that they did not know anyone using some of the other platforms and so they did not see any benefit to them by using them, ‘don’t see a need for them’ (P3). Participants felt that the time spent on a smartphone is already considerable and adding more apps would add to this and eat into leisure time when people could meet face to face instead of engaging in virtual networks.

‘I just think the phone takes up so much of your time anyway, the more applications and outlets that are on it the more time you spend on it so it is really to try to minimise the time spent on the device’ (P5)

‘It’s a work life balance, I don’t want my phone bleeping every five minutes with Twitter, I wouldn’t be tied to the phone at weekends only for voice calls’ (P6)

Other considerations were practical ones around battery and memory consumption when deciding to install apps

‘I used to have more apps on previous smartphones but it slows it down and eats battery so didn’t install on this one’ (P4)

Information privacy was not raised as a significant factor when it came to deciding what apps to use on their smartphone. Where an app was seeking what was deemed excessive permission to information on the device or credit card information there was a reluctance to install the app but most stated that if it was something they really wanted they would overlook the permission requirements. For the most part participants had downloaded apps that the considered useful to them and they were used regularly.

4.6.2 Financial Transactions

All interviewees listed financial transactions as one of the areas that they were most concerned about from an information privacy perspective. All except one person had a banking app installed, most said they used it to check balances rather than process transactions.

One participant said he had not used the banking app in about eight months but had never bothered to uninstall the app. He was concerned about privacy and the fact he was using his smartphone for so many other activities that there was a chance of information from it being captured by another app.

The widespread use of banking apps was attributed to trust in the institution that was providing the app and the convenience they offered. Interviewees were confident that the financial institution would have good security protocols built into their service. There was no research to base this on other than the existing relationship with their financial institution.

The same level of trust was not there when it came to mobile payments with no-one using it for banking payments but a number of people used a smartphone app to pay for parking or taxi journeys. They were comfortable with this as they felt the amounts were small and it was not linked directly to their bank account. The benefits of not needing to carry coins and the ability to easily track expenses from the consolidated statement delivered by the app provider outweighed any reservations.

The reluctance to use mobile payments for financial transactions was also linked to trust from the perspective of a lack of trust or confidence. One participant was concerned about responsibility in the case of a problem given the number of entities involved in a transaction. They questioned where responsibility would lie; the financial institution, the smartphone manufacturer, the app creator or the telecom carrier. Others were nervous citing they did not know enough about how it worked and would wait and see how it developed in the market before pursing it as an option. Another participant was reluctant to use it on the basis of potential for exposure when so much was consolidated into a single device. Conversely one person saw a potential benefit in that it would prevent a retail outlet direct access to card information but it was not something he would consider in the short term, he was adopting a wait and see approach.

4.7 Cloud storage

There was confusion among the majority of the interviewees as to whether their smartphone performs a backup of the information on the device. Most were confident that their emails, contact details and calendar appointments were cloud based and stored online as well as on the device.

All said that the smartphone was their main device for taking photographs and they would copy those to either their PC or an external hard drive on an ad hoc basis.

Files other than photographs were not considered important or sensitive and did not require a backup.

Some had set up synchronisation to a cloud based service but a number of participants were unsure if the smartphone did perform a backup to a cloud service and if it did they did not know what it was copying or where it was copying it to. It was assumed it would be using the default Google Cloud or Apple iCloud. A couple of participants said they accepted the default settings that came with the smartphone and so it may be backing up some files. They had not actively created an account to use cloud services but accepted that they had set up a user account as part of the setup process when initializing the smartphone.

‘I think there is an element of I’m using Google cloud for some photographs going up automatically. I have to check, I haven’t spent time on seeing where all my data is because I was using Dropbox for a while, I was using something else for a while and I never went in and cleared them down’ (P1)

‘I actually don’t know, if it’s an automated process on the iPhone which it may well be but I haven’t set up anything’ (P5)

Even where one participant had deliberately not signed up to the cloud backup service they questioned if their instant messages were being backed up automatically. That was not something they had considered before the interview.

I’m just trying to think what happens with WhatsApp and Viber but I think you lose all those messages actually I think they are only held locally on the device so no I haven’t anything set up to back up to the cloud.’ (P2)

When participants were queried why they had not investigated the backup settings on their device the main reason given was a lack of time and a perception that it might be complicated to find out. It was one of those things that was on their list of things to do. One participant disclosed that raising a question about backup in work might result in other questions being asked that they would not be able to answer and they preferred not to draw attention to the matter. The fact that only one person had ever lost their phone meant that the sample group had not had to restore their device from a backup and so they never had to investigate how or if the backup process worked.

4.8 Terms of Service

Everyone said ‘No’ or ‘Not really’ when asked about reading the privacy policies or cookie statements provided by websites. Two people commented that they read the cookie statement to the extent of finding out how they can dismiss them.

‘Click X get it out of there’ (P6)

‘I’d only read where the button is to hide it’ (P4)

Some of the participants remarked that there is no choice, if you want to use the website it is a case of accepting the terms of use or not using the web site at all and every website has cookies deployed. The reasons given for not reading privacy statements were down to the time required to read them and the perception that the language would be difficult to comprehend, likened to legal jargon. Policies were considered to be long and intentionally ambiguous. ‘If there is a tonne of stuff, I won’t read a tonne a stuff’ (P2)

There was more interest and attention paid to the permissions sought by apps that were downloaded, some of this was due the succinct pop up window that accompanies the download procedure. Where permission requests seemed to exceed what an app should need then some interviewees had not downloaded the app but most said that if it was something they found really useful they were willing to forgo their apprehensions. 'If I was downloading an app and I thought it was looking for too much then and I don't really need the app I'd say no I'm not downloading you' (P3)

This demonstrates that users are consciously making trade-offs and where the functionality is deemed to be of specific benefit then users are willing to compromise on some of the self-imposed restrictions they had set for themselves.

4.9 Information Privacy

At the beginning of the interview, participants were asked about the importance they placed on information privacy in general which they all agreed was important or very important. In respect of own information privacy the sentiments were mirrored. There was an appreciation within the sample interviewed that information is valuable and as an asset it should be protected.

'Data is key to everything now and there is so much data available to so many organisations' (P1)

The final part of the interview focused on how confident participants were about knowing what information they had shared and how confident they felt about the control they had over their information privacy. This was in the context of reviewing their behaviours against their own information privacy values.

The consensus from participants was when they reflected on their behaviours they did not feel completely confident they knew what information they had shared. While they all had to some degree employed a policy of restricting what they shared, some observed there was a possibility of information being online that they had not 'knowingly' shared. 'If someone was to show me a profile of what data I have shared to various different establishments, I'd probably be surprised, in a way probably be surprised' (P1).

There was an acknowledgement of not having control of how information was processed once it was in the domain of a third party. It was noted that often there is no way of knowing if information has been compromised or disseminated beyond its original purpose. Some participants related their lack of knowledge back to the example of the smartphone performing an automatic backup of their information that they were not fully au fait with. There was a potential there were other processes occurring in the background that they were not aware of. There was an assertion that the volume of daily activity performed on a smartphone made it impossible to be alert to every information sharing transaction. There was also an acceptance that this is part of life now, 'a lot of these things I'm saying I have got concerns but because it's so much part of how you live I am still going ahead and using all these apps even though I still feel slightly that I do have concerns it doesn't really stop me from using the apps' (P2)

Most interviewees had a pragmatic attitude to online sharing, an acceptance that once something is shared online it is online forever and it is beyond the complete control of the originator. 'I suppose what I'm the way I think about that is that I am aware that anything that leaves from the phone is out of my control' (P3)

There was a general feeling among participants that the companies who are providing the services they use, whether that is an app or cloud storage or a search engine that they are big corporations who will have security measures in place. It was expected that it is in their interest to protect user information so as to keep their customers and reputation intact. There was an acceptance by all participants that when viewed in the round, the services they were receiving were worth the trade-off of foregoing some information privacy for the benefits gained.

'ease of use and what it gives in terms of communication and eh social interaction at the moment the trade-off I would say is worth for what your maybe giving information to other companies'(P1)

There was an also a level of apathy among users, a certain amount of accepting the defaults or not being more proactive about protecting their information because of the effort it would require.

'It's pure convenience of another way in saying ah yeah sure it's only this, what harm is it, there's an element of don't have the time to spend locking everything down and then secondly if you were to do that and then some of the things you might like to use would be a pain to use' (P3)

The familiarity with technology has meant that there is more awareness of how information is captured, stored and used but likewise this familiarity has meant that devices fade into the background as well. 'I'd say we know of the threats for sure and what people could use it for but saying that people want to access information in the now and they're a bit blasé at same time' (P6)

While everyone was conscious of the potential threats that exist to their information privacy no-one had to their knowledge suffered a breach to their data or had a negative experience resulting from their behaviour. Beyond the odd comment about annoying advertisements that were ignored or some spam messages the individual experience everyone interviewed has had using a smartphone has been largely positive. The benefits of being able to perform a multitude of activities at anytime from anywhere far outweighed any possible negatives. The main negative cited was related to the time spent using the device and how it can become a bit addictive and seem indispensable.

4.10 IS Theory comparison

The data collected shows a link to the privacy paradox phenomenon (Brown, 2001) discussed in Chapter 2. While participants spoke about not wanting to disclose certain categories of information they were sometimes willing to compromise if the benefit or convenience offered by using an app or a website was considered to be great enough. When this dichotomy was explored, the deviation from intentions was not always completely explained and sometimes the users themselves were a little confused as to the actions they took when reviewed in hindsight. This may be partly explained by the speed with which online services are transacted as discussed by Acquisti et al. (2015) and Baek (2014) leaving little time to reflect on future outcomes. Several participants mentioned speed and urgency when using services and not having the time to read all of the notifications that came with the service.

As the only social media app that was used by all participants and on a more regular basis than the other social media apps mentioned it is interesting to look at the popularity and usage of WhatsApp in a little more detail. It holds a dominant position in the instant messaging category. Since it was launched in 2010 it has grown to 1.3 billion monthly active users (Statista, 2017d). Figure 12 shows some of the usage statistics released by the company in July 2017.

The Diffusion of Innovations Theory (DOI) developed by Rogers (2003) is a useful lens to view the widespread adoption and frequency of use which the participants of this project put at daily. Rogers proposed that social networks are a significant contributor to the adoption of new innovations, diffusion in this scenario is understood to be the mechanism by which the idea is communicated among the social group over time. The speed of adoption is largely influenced by five main factor that he listed as: relative advantage, compatibility, complexity, trialability and observable results. These can be mapped to the popularity of WhatsApp.

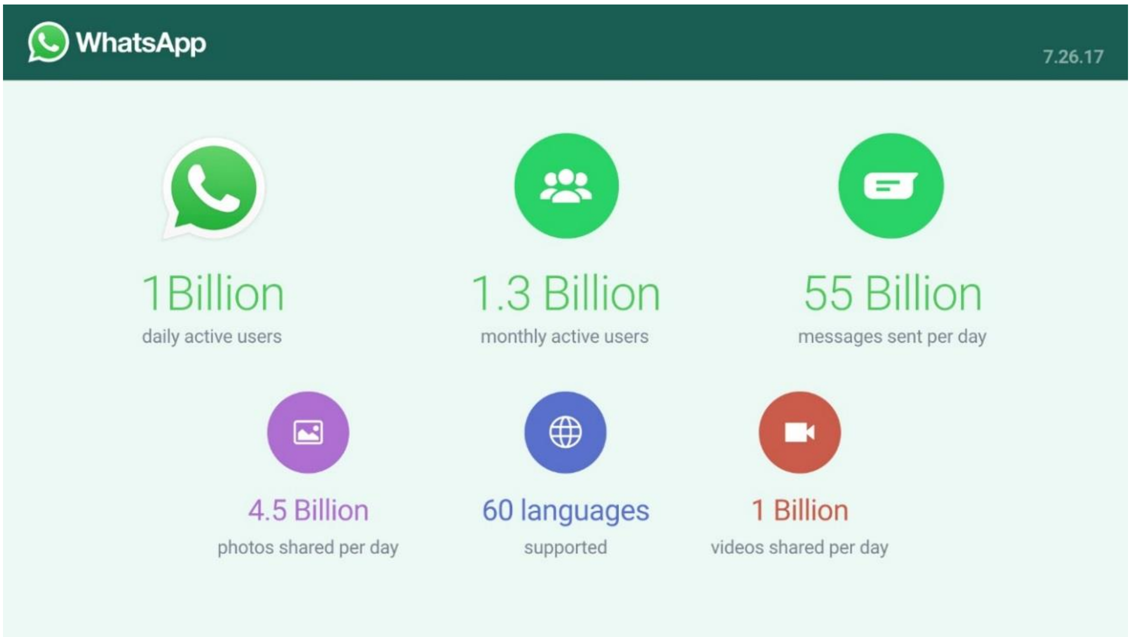


Figure 12 WhatsApp by numbers (WhatsApp, 2017)

The relative advantage is how much the new idea is perceived to be better than what is already available, the bigger the advantage is seen to be the more quickly an idea is likely to spread. In this example the advantages listed by participants were in comparison to traditional SMS messages. WhatsApp offered a way to easily create virtual groups and allow everyone in the group to participate in the conversation concurrently. People could see when messages were read and the status of their friends. It is perceived as free compared to SMS offering an economic benefit.

The adoption of WhatsApp in the context of a replacement or a supplement to SMS is it adheres to much the same format, short messages sent person to person or person to a defined group. SMS since it became available in the late 1990s was a popular way to quickly communicate when a voice call was inconvenient or the message being relayed was short. The enhancements that instant messaging bring are compatible with the existing social norms of communicating.

Ideas that are easy to understand and use will be adopted more quickly than those that are seen as complex. WhatsApp has an intuitive user interface that did not require interviewees to learn a new skill, they were able to install and use immediately.

Trialability is how easy it is for someone to test out an innovation with limited monetary or time commitment. WhatsApp was free to download from the app stores so easily accessible to run on a trial basis. There was a proposed charge after a year but this was dropped. It is agnostic about the smartphone OS requiring no financial outlay on hardware.

Observable results is probably the most critical determinant of diffusion of this type of service as it is how an idea works in reality and how successful it is demonstrated to be. It includes word of mouth promotion and this has played an important role in the extensive use of WhatsApp. Unlike email where a user does not need to be using the same provider to exchange messages, the WhatsApp instant messaging application is a closed platform and communication is restricted to only those who have it installed. As people began using it and finding it beneficial they promoted it to their peers and the more people who were using the platform the more benefits would accrue. One of the participants started using it when it was the primary method of co-ordinating a group holiday and then he encouraged his family to adopt it for organising family events. Another participants was encouraged by some of her friends living abroad to try it and found it brilliant and kept using it.

The objective of WhatsApp like other social media services is to encourage users to share information and to create online communities. It can be used as a text only communication but those interviewed spoke of the richness of communication as a reason for using it over standard text messaging. It was used by participants to share photographs and video including some of minors where there had been a range of responses from reluctance to explicit rejection of the same level of sharing on other platforms. It allows contacts to see the status of each other in real-time so the level of information disclosure on the platform is high yet it was seen to encroach less on privacy than other social media services that were in use. The perception among the majority interviewed was there were less chance of an information privacy breach by using it as sharing was bounded and creating the same level of access control in a service like Facebook was not deemed to be possible. Everyone interviewed was aware that Facebook owns WhatsApp but this did not cause concern for any of the participants. This agrees with the findings of Raynes-Goldie (2010) that maintaining privacy within the social group is more important than privacy from institutions.

5. Conclusions

5.1 Introduction

This chapter will highlight the conclusions drawn from the research findings presented in Chapter 4. The first section will demonstrate how the research question has been answered. The second section reviews some of the limitations encountered as part of the study. The chapter will conclude by outlining possible areas of further research that have been suggested by the findings.

Over the coming years, technology will continue to evolve and become more integrated in all aspects of life. As devices become more 'intelligent' or 'smart', the potential for new businesses and scientific breakthroughs is vast. Information will be integral to driving the digital economy forward. Those with the ability to capture it and derive insight from it will be best placed to take advantage of opportunities as they arise. Continued technological enhancements will face an ongoing challenge of balancing the rights of the individual versus the benefits that may be attained for the greater number of people.

5.2 Key findings

The pervasiveness of smartphone technology is a recent phenomenon, it has brought capabilities that were once only available on a PC to a device that fits in the hand. A smartphone allows persistent connectivity to the internet enabling a continuous flow of information to and from the device. It was in the context of this continuous almost imperceptible information flow that this research was undertaken.

The research question as outlined in chapter 1 is

What is the attitude among smartphone users about information privacy when using a smartphone?

The sub questions arising from the main question are

How important is information privacy to them?

Are users aware of what information they have agreed to share and with whom?

What actions have users taken to protect their privacy when using their smartphone?

The research findings showed that participants do have concerns about their information privacy and think that it is important that it is protected. Those interviewed did not consider all information to be of equal value and details about minors or financial matters were categorised as most important. Thus when participants implemented measures to keep information private, varying levels of protection were applied depending on how valuable they viewed the information to be. The protection measures adopted were mostly a policy of limited disclosure. Participants did not feel there was any way of keeping information completely private once it left their domain, once it had been shared it was out of their control.

Despite their stated intentions, participants did concede that they had behaved in ways which may have exposed information they would prefer to have kept private. The reasons given for diverging from their preferences were a mixture of not thinking through the consequences of doing something or where the benefit was deemed to be worth the trade-off. Participants accepted that they had downloaded and used apps that they found particularly useful knowing that the app was capturing information they would have preferred to keep private. This is in keeping with some of the findings of the privacy paradox (Brown, 2001) discussed in chapter 2. A number of the services used have become ingrained into their daily routine and to stop using them was not seen as practical.

This demonstrates that there is a constant negotiation going on for users between getting the benefit of a service and keeping control over what they share. People did consider their privacy and tried to protect it but there was a flexible approach. If the service or app was deemed useful to them then the information privacy concerns were moved down the priority list.

There was a degree of confusion about how the default settings on their devices impacted on information sharing. This was primarily in relation to backup and the use of cloud services. A majority of the participants did not know or were not sure if their device performed a backup of their files. They had not deliberately initiated a backup routine but they had accepted the prompted defaults at set-up and so were unsure what their backup status was. As they had never needed to restore files and all carried out a manual copy of important files they had never investigated into backup options. This implies that default settings are likely to be accepted by a user and may allow a service provider to promote terms that are preferable to them.

There were a number of social media apps that were widely used among those interviewed but WhatsApp was the only one that was mentioned by everyone. It was highlighted as being used almost daily and participants were willing to share photographs and video through it where they had not agreed to that level of sharing through other apps they used. While this type of sharing went against their stated intentions, there was a perception of maintaining control of their information and containing it within defined boundaries that was not available or not easily configurable on other online social networking platforms. There is nothing to prevent onward sharing of content through instant messaging but this does not seem to be part of the etiquette in contrast to the experiences interviewees had with Facebook

Users were bounded by practicality as much as by concerns over privacy loss, there were as many references to practical considerations for not using a smartphone for certain activities as privacy ones. Reasons given for not using a smartphone included preserving battery life, inappropriate screen size, websites not optimised for use on a smartphone. The location setting was the only function that users specifically turned off to maintain privacy over their movements.

The questions about how participants used their smartphone led to exploring how confident they were that they knew what information they had agreed to share. Most participants were not confident that they were fully aware of what information they had shared and they did not feel empowered to be able to tightly control the flow of information. There were comments that given the period of time spent using the device and the variety of tasks that it is used to complete, that it would be impossible to be keep track of everything.

There were a number of reasons given for the gap in knowledge about some of the concepts explored. Some of it was attributed to inertia and a lack of proactive management on the part of the user. There was an unwillingness on the part of participants to spend time reading terms of service or investigating functionality citing time pressure and the inherent complexity of the subject as barriers to understanding. The participants said that some responsibility must also lie with the IT providers given the complexity and interdependencies that exist in the subject. Frequent updates to apps and website terms seemed to be creating an environment where participants felt so overwhelmed at the prospect of keeping informed that they avoided the topic for the most part.

Those interviewed were conscious of the possibility of identity theft and financial loss if information they had shared was compromised. Intangible loss through profiling, targeted advertising or targeted pricing had not been considered to the same degree. There was some references to targeted advertisements which some found useful as part of a search to ‘creepy’ when prior searches were appearing as advertisements on another website or within an app.

Smartphones have the capability to act as sophisticated surveillance devices tracking movement, activity and conversations. Society is constantly evolving and adapting to social norms so as things become more widely adopted and accepted they cease to be noticed. The challenge of information privacy in the context of smartphone usage is not that the privacy requirements are unique and different but that the scope of information capture and subsequent use on every action and interaction is so wide Nissenbaum, (2011). It is important that users are educated and feel empowered to make decisions about how their information is used and that was not the feeling among the participants of this research project.

5.3 Limitations

The qualitative interviews were conducted with a small sample size that is not representative of the entire population. This did not allow for a wide range of opinions to be gathered and prevents findings being generalised. The research project was exploratory in nature, it took a broad view of the topic and a future study could focus on some of the themes that this research project uncovered. A larger sample size targeting respondents from different demographic and social groups would provide the range of data needed to generalise.

During the course of the interviews there was some confusion among participants about whether they were using some smartphone functions. It would have been beneficial to have been able to verify this by interrogating their device to check settings. This had not been considered as part of the research design. This expansion of scope would need to have been included in the ethics approval and receive agreement from participants prior to data collection commencing. This level of disclosure would require more commitment from participants and might discourage those who value privacy highly but it would give a more holistic view of the research subject.

5.4 Recommendations for future study

One of the themes that this research uncovered is the different level of disclosure that participants applied depending on the social media app. The reasons given were associated with keeping control and being able to contain the breath of sharing to a defined number of people within a social circle. There was not the same level of concern about how information might be used by a service provider. An area for future exploration would be to understand how these boundaries are set and what characteristics determine which sharing platform an individual will use.

Smartphones have become an indispensable piece of technology for many people and those interviewed could not see a way to keep their information completely private and still receive the benefits the technology offers. Users want and have become used to the convenience of the services enabled by a smartphone. The findings of the literature review and the results of the research undertaken show that many users perceive it as too difficult and time-consuming to comprehend the intricacies of smartphone technology. Consequently they do not feel empowered to deploy preferred protective measures. In agreeing to broad terms of service it might appear that users do not place a value on their privacy and are willing to share information without any discernment but that does not seem to be the case. There is an onus on everyone to take control of their digital literacy skills but there should be support available to help people achieve that goal. It would be interesting to examine how government and industry could work together to enable users to become more capable so they are making informed decisions confident that they have the right level of knowledge.

Except for one person all of those interviewed had a single device for personal and professional use. This introduces a blurring of boundaries between what used to be distinct areas of life. Social media has compounded this with personal and professional networks starting to merge. There were complaints about the amount of time spent using a smartphone and the concept of being always available. It would interesting to understand how people are managing the overlap between the two domains that technology including smartphones is enabling.

5.5 Closing remarks

Today, people are familiar with IT, the internet has been widely used for the last two decades and the smartphone is ten years old. Information creation and sharing is the norm and it happens at a frequency and speed that makes it seem transparent and not in need of oversight. Smartphones have brought huge benefits to business and society that seem essential to daily life. The breath of technology and its use will continue to evolve as more devices connect to the internet generating more information. It is important to harness the benefits that this will offer but it is equally important that citizens understand how their actions may impact on the privacy of their information privacy and they have the tools to be able to protect it in line with their wishes.

References

32Market (2017) 32M MICROCHIPS EMPLOYEES COMPANY-WIDE [online] available https://32market.wordpress.com/2017/07/21/32m-microchips-employees-company-wide/ [accessed 1 August 2017]

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015) 'Privacy and human behavior in the age of information', *Science*, 347(6221), 509-514.

Apple (2017) If your iPhone, iPad, or iPod touch is lost or stolen [online] available; https://support.apple.com/en-gb/HT201472 [accessed 1 August 2017]

Baek, Y. M. (2014) 'Solving the privacy paradox: A counter-argument experimental approach', *Computers in Human Behavior*, 38, 33-42.

Berinato, S. (2015) 'There's No Such Thing as Anonymous Data', *Harvard Business Review Digital Articles*, 2-4.

boyd, d. and Hargittai, E. (2010) *Facebook privacy settings: Who cares?* [online], 2010, available: http://firstmonday.org/ojs/index.php/fm/article/view/3086 [accessed 8 March 2017].

Brown B. (2001) Studying the internet experience. HP Laboratories Technical Report [online] available: http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf [accessed 15 March 2017].

Bryman, A. (2015) *Business research methods*, Fourth edition. ed., Oxford: Oxford University Press.

Bryman, A. (2016) *Social research methods*, Fifth edition. ed., Oxford: Oxford University Press.

Cisco (2017) *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021* [online] available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf [accessed 1 May 2017].

Commission for Communication Regulation (2017) '*Irish Communications Market Quarterly Key Data Report Q4 2016'* Irish Life Centre Lower Abbey Street, Dublin.

Computerworld (2009) Facebook will shut down Beacon to settle lawsuit [online] Available:http://www.computerworld.com/article/2527779/government-it/facebook-will-shut-down-beacon-to-settle-lawsuit.html [accessed 10 June 2017]

Creswell, J. W. (2013) *Qualitative inquiry and research design: choosing among five approaches*, 3rd edition. ed., Los Angeles: SAGE Publications.

Creswell, J. W. (2014) *Research design: qualitative, quantitative, and mixed methods approaches*, Fourth edition, international student edition. ed., Los Angeles, Calif.: Sage.

Crotty, M. (1998) *The foundations of social research: meaning and perspective in the research process*, London: Sage.

Denscombe, M. (2010) *The good research guide: for small-scale social research projects*, 4th ed., Maidenhead: McGraw-Hill/Open University Press.

De Montjoye, Y.A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D. (2013) Unique in the crowd: The privacy bounds of human mobility. *Scientific reports*, *3*, p.1376.

Dublin Airport (2017) Cookie Statement [online] https://www.dublinairport.com/ [accessed 8 August 2017]

European Commission Directive (1995) Directive 95/46/EC Protection of personal data [online] available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:31995L0046 [accessed 5 July 2017]

European Commission Directive (2002) Directive 2002/58/EC Directive on privacy and electronic communications [online] available: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [accessed 10 May 2017]

European Commission Directive (2009) DIRECTIVE 2009/136/EC Directive on privacy and electronic communications [online] available :http://eur-lex.europa.eu/legal-content/en/T/?uri=CELEX %3A32009L0136 [accessed 12 May 2017]

European Commission (2016) Flash Eurobarometer 443 e-Privacy Report [online] available: http://ec.europa.eu/COMMFrontOffice/PublicOpinion [accessed 15 April 2017]

European Commission (2017) Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover [online] available: http://europa.eu/rapid/press-release_IP-17-1369_en.htm. [accessed 21 May 2017]

Facebook (2016) Mobile User Statistics [online] available:https://s21.q4cdn.com/399680738/files/doc_presentations/FB-Q4'16-Earnings-Slides.pdf. [accessed 11 June 2017]

Facebook (2017) Facebook reach 2billion users [online] https://www.facebook.com/zuck/posts/10103831654565331[accessed 29 July 2017]

Gartner (2017a) IT Glossary [online] available:http://www.gartner.com/it-glossary/smartphone/ [accessed 9 April 2017]

Gartner (2017b) Organizations Will Be Valued on Their Information Portfolios [online] available: http://www.gartner.com/newsroom/id/3600817 [accessed 3 April 2017]

Grabham, D. (2016) *History of the iPhone 2007-2017* [online] available: http://www.t3.com/features/a-brief-history-of-the-iphone [accessed 28 May 2017].

Grbich, C. (2007) *Qualitative data analysis: an introduction*, London: Sage.

Gross, D. (2010) *Apple trademarks 'There's an app for that'* [online] available: http://edition.cnn.com/2010/TECH/mobile/10/12/app.for.that/ [accessed 16 February 2017].

Guardian (2014) I didn’t have enough Facebook friends to prove to Airbnb I was real [online] available: https://www.theguardian.com/money/blog/2014/nov/14/airbnb-wont-let-book-room-facebook-friends. [accessed 23 July 2017]

Guardian (2015) Ashley Madison database suggests paid-delete option left identifiable data intact [online] available:https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-paid-delete-option-left-data-identifying-users-post-claims [accessed 14 August 2017]

ITU (2011) *Measuring the Information Society 2011*, [online] available:http://itunews.itu.int/en/1686-Broadband-prices-are-falling.note.aspx [accessed 14 July 2017]

Kumaraguru, P. and Cranor, L.F. (2005) Privacy indexes: a survey of Westin's studies.

Kumar, R. (2014) *Research methodology: a step-by-step guide for beginners*, Fourth edition. ed., Los Angeles: Sage.

Lowry, P.B., Cao, J. Everard, A. (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), pp.163-200.

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

Marotta-Wurgler, M. (2015) Does “Notice and Choice” Disclosure Regulation Work?
An Empirical Study of Privacy Policies. NYU Law School

Martin, K. (2013) *Transaction Costs, privacy and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online* [online] available: http://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/4838/3802#author [accessed 16 May 2017].

McDonald, A.M., Cranor, L.F. (2008) The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society 4. 540-565*

McGrath, R. (2013) 'The pace of technology adoption is speeding up', *Harvard Business Review*, 25.

Mosteller, J., and Poddar, A. (2017) To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors, Journal of Interactive Marketing, 39 27-38

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E. and Wang, S. (2012) 'Disclosure antecedents in an online service context: the role of sensitivity of information', *Journal of service research*, 15(1), 76-98.

Nissenbaum, H. (2011) 'A Contextual Approach to Privacy Online', *Daedalus*, (4), 32.

Norberg, P. A., Horne, D. R. and Horne, D. A. (2007) 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors', *Journal of Consumer Affairs*, 41(1), 100-126.

Palmer, M. (2006) *Data is the new oil* [online] available: http://ana.blogs.com/maestros/2006/11/data_is_the_new.html [accessed 16 February 2017].

Pew Research Centre (2014) Public Perceptions of Privacy [online] available:http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/[accessed 10 June 2017]

Pew Research Centre (2015) Smartphone App permissions [online] available: http://www.pewinternet.org/interactives/apps-permissions//[accessed 3 April 2017]

Pocket-lint (2017) 7 best encrypted messaging apps [online] available:http://www.pocket-lint.com/news/140119-7-best-encrypted-messaging-apps-for-all-the-edward-snowdens-out-there [accessed 14 August 2017]

Raynes-Goldie, K. (2010) *Aliases, creeping and wall cleaning: Understanding privacy in the age of Facebook* [online] available: http://journals.uic.edu/ojs/index.php/fm/article/view/2775/2432 [accessed 21 July 2017].

Rogers, E. M. (2003) *Diffusion of innovations*, 5th ed., London: Simon & Schuster.

RTE.ie (2017) Cookie Statement [online] www.rte.ie [accessed 8 August 2017]

Saunders, M., Lewis, P. and Thornhill, A. (2016) *Research methods for business students*, Seventh edition. ed., Harlow: Pearson Education Limited.

Schwab, K. (2017) *The fourth industrial revolution*, London: Portfolio Penguin.

Sekaran, U. and Bougie, R. (2013) *Research methods for business: a skill-building approach*, 6th ed., Chichester, West Sussex: Wiley.

Sloan, R. H. and Warner, R. (2014) 'Beyond Notice and Choice: Privacy, Norms, and Consent', 14(2), 370-414.

Smith, D. (2015) *Google Chairman: 'The Internet Will Disappear'* [online] Business Insider UK available:http://uk.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1?r=US&IR=T [accessed 19 February 2017].

Smith, H. J., Dinev, T. and Xu, H. (2011) 'Information privacy research: an interdisciplinary review', *MIS quarterly*, 35(4), 989-1016.

Srivastava, L. (2005) 'Mobile phones and the evolution of social behaviour', *Behaviour & Information Technology*, 24(2), 111-129.

Statista (2017a) *Worldwide smartphone unit sales 2013-2016 by region* [online] available: https://www.statista.com/statistics/412108/global-smartphone-shipments-global-region/ [accessed 19 February 2017].

Statista (2017b) *Number of apps available in leading app stores as of March 2017*, [online] available:https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ [accessed 18 April 2017].

Statista (2017c) *Digital Population Worldwide*, [online] available: https://www.statista.com/statistics/617136/digital-population-worldwide/ [accessed 18 May 2017].

Statista (2017d) *PC shipments worldwide from 2006 to 2016*, [online] available https://www.statista.com/statistics/267023/global-pc-shipments-since-2006-by-vendor/ [accessed 23 April 2017].

Statista (2017e) *Facebook Inc. Dominates the Social Media Landscape* [online] available*:* https://www.statista.com/chart/5194/active-users-of-social-networks-and-messaging-services/ [accessed 30 July 2017].

Telegraph (2016) iPhone 7: Fans queue at Apple Stores as sales begin amid supply shortage [online] available: http://www.telegraph.co.uk/technology/2016/09/16/iphone-7-huge-queues-at-apple-stores-as-sales-begin---live/ [accessed 23 April 2017]

Thomas, D. R. (2006) 'A General Inductive Approach for Analyzing Qualitative Evaluation Data', *American Journal of Evaluation*, 27(2), 237-246.

UN General Assembly. (1948). Universal declaration of human rights (217 [III] A). Paris.

Vodafone (2017) Smartphone Options [online] available: http://shop.vodafone.ie/shop/phones[accessed 12 April 2017]

Wang, T., Duong, T. D. and Chen, C. C. (2016) 'Intention to disclose personal information via mobile applications: A privacy calculus perspective', *International Journal of Information Management*, 36(4), 531-542.

Warren, S. V. and Brandeis, L. D. (1890) 'The right to privacy', *Harvard Law Review*, 4(5), 193-220.

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

Westin, A. F. (2003) 'Social and Political Dimensions of Privacy', *Journal of Social Issues*, 59(2), 431-453.

WhatsApp (2017) Connecting One Billion Users Every Day [online] available: https://blog.whatsapp.com/ [accessed 26 July 2017]

White, T.B. (2004) Consumer Disclosure and Disclosure Avoidance: A Motivational Framework, JOURNAL OF CONSUMER PSYCHOLOGY, 14(1&2), 41–51

World Economic Forum (2017) Valuing Personal Data [online] available: https://www.weforum.org/whitepapers/valuing-personal-data-and-rebuilding-trust
[accessed 23 April 2017]

Wu, T., Lu, Y., Gong, X. and Gupta, S. (2017) 'A study of active usage of mobile instant messaging application', *Information Development*, 33(2), 153-168.

Xu, H., Gupta, S., Rosson, M. B. and Carroll, J. M. (2012) 'Measuring mobile users' concerns for information privacy'.

Appendices

Appendix A. Ethics Application Documents

School of Computer Science & Statistics

Research Ethics Application

Part A

Project Title: An Exploration of User Understanding of Information Privacy Implications in the use of a Smartphone

Name of Lead Researcher (student in case of project work): ......Siobhán Foley ....

Name of Supervisor: ....PJ Wall...…........

TCD E-mail: ……foleys@tcd.ie.......…………….. Contact Tel ………………………..

Course Name and Code (if applicable): ……M.Sc Management of Information System…….

Estimated start date of survey/research: ………17th May 2017..................………….

I confirm that I will (where relevant):

- *Familiarize myself with the Data Protection Act and the College Good Research Practice guidelines http://www.tcd.ie/info_compliance/dp/legislation.php*
- *Tell participants that any recordings, e.g. audio/video/photographs, will not be identifiable unless prior written permission has been given. I will obtain permission for specific reuse (in papers, talks, etc.)*
- *Provide participants with an information sheet (or web-page for web-based experiments) that describes the main procedures (a copy of the information sheet must be included with this application)*
- *Obtain informed consent for participation (a copy of the informed consent form must be included with this application)*
- *Should the research be observational, ask participants for their consent to be observed*
- *Tell participants that their participation is voluntary*
- *Tell participants that they may withdraw at any time and for any reason without penalty*
- *Give participants the option of omitting questions they do not wish to answer if a questionnaire is used*
- *Tell participants that their data will be treated with full confidentiality and that, if published, it will not be identified as theirs*
- *On request, debrief participants at the end of their participation (i.e. give them a brief explanation of the study)*
- *Verify that participants are 18 years or older and competent to supply consent.*
- *If the study involves participants viewing video displays then I will verify that they understand that if they or anyone in their family has a history of epilepsy then the participant is proceeding at their own risk*
- *Declare any potential conflict of interest to participants.*
- *Inform participants that in the extremely unlikely event that illicit activity is reported to me during the study I will be obliged to report it to appropriate authorities.*
- *Act in accordance with the information provided (i.e. if I tell participants I will not do something, then I will not do it).*

Siobhán Foley

Signed:..Date:...............2/5/2017.................................
Lead Researcher/student in case of project work

Part B

Please answer the following questions.		**Yes/No**
Has this research application or any application of a similar nature connected to this research project been refused ethical approval by another review committee of the College (or at the institutions of any collaborators)?		No
Will your project involve photographing participants or electronic audio or video recordings?		Yes
Will your project deliberately involve misleading participants in any way?		No
Does this study contain commercially sensitive material?		No
Is there a risk of participants experiencing either physical or psychological distress or discomfort? If yes, *Give details on a separate sheet and state what you will tell them to do if they should experience any such problems (e.g. who they can contact for help).*		No
Does your study involve any of the following?	*Children (under 18 years of age)*	No
	People with intellectual or communication difficulties	No
	Patients	No

Details of the Research Project Proposal must be submitted as a separate document to include the following information:

1. *Title of project*
2. *Purpose of project including academic rationale*
3. *Brief description of methods and measurements to be used*
4. *Participants - recruitment methods, number, age, gender, exclusion/inclusion criteria, including statistical justification for numbers of participants*
5. *Debriefing arrangements*
6. *A clear concise statement of the ethical considerations raised by the project and how you intend to deal with them*
7. *Cite any relevant legislation relevant to the project with the method of compliance e.g. Data Protection Act etc.*

Part C

I confirm that the materials I have submitted provided a complete and accurate account of the research I propose to conduct in this context, including my assessment of the ethical ramifications.

Siobhan Foley

Signed: ....Date: ....2/5/2017.............................
Lead Researcher/student in case of project work

There is an obligation on the lead researcher to bring to the attention of the SCSS Research Ethics Committee any issues with ethical implications not clearly covered above.

Part D

If external or other TCD Ethics Committee approval has been received, please complete below.

External/TCD ethical approval has been received and no further ethical approval is required from the School's Research Ethical Committee. I have attached a copy of the external ethical approval for the School's Research Unit.

Signed: ....Date: ....

Lead Researcher/student in case of project work

Part E

If the research is proposed by an undergraduate or postgraduate student, please have the below section completed.

I confirm, as an academic supervisor of this proposed research that the documents at hand are complete (i.e. each item on the submission checklist is accounted for) and are in a form that is suitable for review by the SCSS Research Ethics Committee.

PJ WALL

Signed: ....Date: ....6th April 2017....................
Supervisor

Appendix B. Participant Information Sheet

Research Title:

An Exploration of User Understanding of Information Privacy Implications in the use of a Smartphone.

Background to the research:

The proliferation and functionality of smartphones has grown dramatically since their introduction about ten years ago. A confluence of technologies in the smartphone ecosystem: faster processors, increased memory, Global Positioning Systems and faster mobile network speeds have allowed the range of services that can be provided to expand greatly. This combined with reducing hardware and communication costs has aided smartphone adoption. As well as being an intelligent device in their own rights, smartphones are acting as a broker or control point for a range of other smart devices like fitness trackers and intelligent home devices. The range of services offered provides the user with a good experience and convenience in completing routine tasks like shopping, web browsing and consuming media on the move. As the services used have expanded so too has the volume of information being captured, shared and stored. This raises the following questions

Are users aware of what information they have agreed to share?

Who is the information being shared with?

Do users think they have the skills to control how and what information they share?

The procedures relevant to the participant within this particular study:

As a person who currently uses a smartphone I would like to invite you to participate in this study. Should you agree to participate, your involvement would consist of a 40-60 minute interview with the lead researcher.

The topics covered in the interview will relate to the use of your smartphone. Areas of interest will include a description of the activities you use your smartphone for, your understanding of privacy settings and information sharing permissions, any concerns you have about information privacy and any positive or negative experiences you have had from sharing information. All questions asked during the interview are optional.

The interview will be electronically recorded. If you do not wish to be electronically recorded you will not be interviewed and will withdraw fully from this process. If you agree to be electronically recorded you may stop electronic recording at any time, and may at any time, even subsequent to participation in this research have the audio recordings destroyed.

In some cases, you may be asked to participate in a short follow up interview. This will only occur where there is a need to confirm prior findings and/or identify any changes that may have taken place since the initial interview. If the case arises that you are re-interviewed, the same consent form and Participant Information Sheet will apply.

Declaration of conflicts of interest:

The lead researcher declares that she has no conflicts of interest of any sort in connection with this research.

How Participants have been selected to Participate in this Research:

As a smartphone user you are being asked to participate in this research.

The voluntary nature of the participation:

Your participation in this research is voluntary, and without prejudice to your legal and ethical rights. You have the right to withdraw at any time without penalty. You have the right to decline to answer individual questions without penalty.

Anticipated risks/benefits of participation:

There are no anticipated risks to your participation in this research. However, please be aware that if you make illicit activities known, these will be reported to appropriate authorities.

The provisions for debriefing after participation:

If requested, you will be fully de-briefed at the end of your participation in this research. If you so wish, you will also be given a brief explanation of the study.

Dissemination of the Research, and Publications arising from the Research:

Results, data and findings from this research will be published as part of the final thesis of Siobhán Foley. Additionally, results, data and findings from this research may be published in one or more peer-reviewed journals, conference proceedings, and a variety of other research publications and conferences.

By participating in this research, you agree that this data may be used for such scientific purposes, and that you have no objection that the data is published in research and scientific publications in a way that does not reveal your specific identity.

At all times your data will be treated with full confidentiality. Any results, data and findings will be fully anonymous and no personal details about you will be revealed or identified as yours.

There will be provision for verifying direct quotations and their contextual appropriateness. If any direct quote from you is to be used, you will be contacted in advance and asked to give permission for the use of the quote. You will also be asked if the use of the quote is contextually appropriate and otherwise accurate. If you decline to give permission, the quote will not be used.

Electronic recordings made will not be made available to anyone other than the lead researcher and research supervisor. The electronic recordings will not be replayed in any public forum or as part of the presentation of the research. You may stop electronic recording at any time, and you may at any time, even subsequent to your participation in this interview have the audio recordings destroyed. At no time will any electronic recording of you be identifiable unless you give prior written permission.

All electronic recording devices are password protected and have encryption software installed. They will be kept secure and in the possession of the lead researcher while any recorded audio or other data is on the device.

Following interview recordings, the sound recording will be transferred from the electronic recording device to an encrypted hard drive. No electronically recorded data of any sort will be uploaded to the cloud or backed up online at any time. All passwords and encryption keys will be kept by the lead researcher and will be made available to the research supervisor upon request. No one else will have access to the passwords and encryption keys.

The lead researcher will, at all times, act in accordance with all information provided in this and other documents and the Data Protection Act 1988 and 2003.

Ethical Approval:

The lead researcher has obtained ethical approval for this research from the School of Computer Science and Statistics, Trinity College Dublin.

Declaration:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and a consent form. I have had the opportunities to ask questions and all of my questions have been answered to my satisfaction and I understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in research and scientific publications in a way that does not reveal my specific identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation, have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the lead researcher and research supervisor.
- I freely and voluntarily agree to be part of this research study, through without prejudice to my legal and ethical rights.

- I understand that I may refuse to answer any questions and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

Appendix C. Participant Informed Consent Sheet

Research Title:

An Exploration of User Understanding of Information Privacy Implications in the use of a Smartphone.

Background to the Research:

The proliferation and functionality of smartphones has grown dramatically since their introduction about ten years ago. A confluence of technologies in the smartphone ecosystem: faster processors, increased memory, Global Positioning Systems and faster mobile network speeds have allowed the range of services that can be provided to expand greatly. This combined with reducing hardware and communication costs has aided smartphone adoption. As well as being an intelligent device in their own rights, smartphones are acting as a broker or control point for a range of other smart devices like fitness trackers and intelligent home devices. The range of services offered provides the user with a good experience and convenience in completing routine tasks like shopping, web browsing and consuming media on the move. As the services used have expanded so too has the volume of information being captured, shared and stored. This raises the following questions

Are users aware of what information they have agreed to share?

Who is the information being shared with?

Do users think they have the skills to control how and what information they share?

Procedures to this Research:

As outlined this research will investigate the level of understanding users have of information privacy implications when using their smartphones. The proposed research method is semi-structured interviews with a selection of participants. As a person who currently uses a smartphone I would like to invite you to participate in this study. Should you agree to participate, your involvement would consist of a 40-60 minute interview with the lead researcher.

The interview questions will relate to the use of your smartphone. Areas of interest will include a description of the activities you use your smartphone for, your understanding of privacy settings and information sharing permissions, any concerns you have about information privacy and any positive or negative experiences you have had from sharing information. All questions during the interview are optional.

In some cases, you may be asked to participate in a short follow up interview. This will only occur where there is a need to confirm prior findings and/or identify any changes that may have taken place since the initial interview. If the case arises that you are re-interviewed, the same consent form and Participant Information Sheet will apply.

The interview will be electronically recorded on the lead researcher’s smartphone which has encryption software installed. You will have an opportunity to review the interview and make amendments or clarifications. You may stop recording at any time and withdraw from the process. You may also request recordings be destroyed after the interview process has completed. Following interview, the sound recording will be transferred to an encrypted hard drive for analysis. At no time will the recording be shared beyond the lead researcher and project supervisor. Your identity will be kept confidential. Following submission and final marking of the thesis, all recordings will be destroyed.

There are no anticipated risks to your participation in this research. However, please be aware that if you make illicit activities known, these will be reported to appropriate authorities.

Publications from this Research:

Results, data and findings from this research will be published as the final thesis of Siobhán Foley. Additionally, results, data and findings from this research may be published in one or more peer-reviewed journals, conference proceedings, and a variety of other research publications and conferences.

By participating in this research, you agree that this data may be used for such scientific purposes, and that you have no objection that the data is published in research and scientific publications. At all times your identity will be kept confidential.

Declaration:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunities to ask questions and all of my questions have been answered to my satisfaction and I understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in research and scientific publications in a way that does not reveal my specific identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation, have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the lead researcher and research supervisor.
- I freely and voluntarily agree to be part of this research study, through without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any questions and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

Appendix D. Schedule of Interview Questions

General questions

What are your general IT skills?

Do you have an interest in information privacy?

Do you think information privacy is important or necessary?

How long have you being a smartphone user?

What type of smartphone do you have?

Do you have a password on your phone?

Does it auto lock?

On disposal of a phone in the past have you deleted all your information – how?

Do you have the ability to track / remotely wipe your device?

Does it have encryption and or malware software installed?

Do you apply system updates when you are advised to?

Do you have a separate phone for work?

Online Activities

What type of activities do you use your phone for?

Voice/Video Calls	Email
Online shopping/banking	Social Media
Satellite Navigation	Photographs
Web Browsing	Media Consumption
Playing music	Mobile Payments
Instant Messaging	Voice Activated assistant

Do you use social network platforms?

Can you tell me which ones?

How often do you use them?

Are there social media platforms that you deliberately don’t use? / Why?

Do you read privacy policies when displayed?

Do you read the cookie statements that appear when using the internet?

What functions are generally enabled on your phone?

How do you typically connect to the internet?

Mobile Apps

Have you installed additional apps on your smartphone?

How many?

How do you decide to install an app?

Where do you download the apps from?

Do you read the terms of service?

Do the permissions requested make sense?

Have you ever uninstalled apps?

Why?

Are you happy to share your information in order to receive a reward/improve experience?

Are there any restrictions on the type of information you would share?

Storage

What types of information is stored on your device?

Do you keep passwords/credit card details on your smartphone?

Does your smartphone back up your information?

How?

Do you know where the backed up information is stored?

Is there a cost?

How do feel about deleting something and it may remain on cloud storage?

Does your smartphone link to other devices?

Privacy

Are you confident you know what information you have shared on your smartphone?

Do you feel you have control over how and where your information is shared?

Do you think about privacy or information loss when you are using your smartphone?

Have you ever lost your smartphone?

Are you aware of your information ever being compromised?