The Ethical Implications of Encrypted Messaging Services: An investigation into the usage of WhatsApp

A dissertation submitted in partial fulfilment of the requirements for the degree of Bachelor of Science (Honours) in Business Information Systems

By Alexander John Bowler

Word Count: 11,429 (excluding references)

Ethical Standards Approval Code - 2016D5651
Declaration

I hereby declare that this dissertation entitled ‘Evaluation, development & testing of an educational support chatbot’ is entirely my own work, and it has never been submitted nor is it currently being submitted for any other degree.

Candidate: Alexander John Bowler

Signature:

Date:

Supervisor: Dr. Simon Thorne

Signature:

Date:
Abstract

Technology is now fully embedded into modern society and since the millennium we have all become more connected and our daily lives are moving online. The emergence of e-commerce has enable small businesses to thrive online and with new communication mediums being created each year, security is becoming a core issue in the industry. As the world becomes more digitally enabled and more reliant on electronic technologies, it also becomes more vulnerable to attack. Attack from rogue states to terrorist organisations worldwide. It is therefore crucial that government bodies implement policy and legislation to control the use of these technologies. However, this must be fair to the citizens of each nation and ensure transparency. The ethical issues that arise from the use of technology must be considered as part of this governance.
Acknowledgments

I would first like to thank Dr Simon Thorne for his excellent guidance and advice throughout the creation of this dissertation, his continued support has helped me create something I am very proud of.

Secondly, I need to thank Ellie Pagan for her kindness and motivation, she has helped me push myself further and always keeps me smiling.

Finally, I want to thank my parents for their dedication and support throughout my education, their motivation and drive has helped me succeed in many ways over the last 4 years.
## Contents

Abstract .................................................................................................................................................. 3  
Acknowledgments ............................................................................................................................... 4  
List of Figures ....................................................................................................................................... 7  
1. Introduction ....................................................................................................................................... 8  
   Motivation .......................................................................................................................................... 8  
   Outcome ............................................................................................................................................ 8  
   Aim, Research Questions and Objectives .......................................................................................... 9  
2. Literature Review ............................................................................................................................ 10  
   2.1 Introduction and Security ............................................................................................................ 10  
   2.2 IT Security .................................................................................................................................. 10  
   2.3 Privacy ...................................................................................................................................... 11  
   2.4 Mass Surveillance ...................................................................................................................... 12  
   2.5 Cloud Security ........................................................................................................................... 12  
   2.6 Mobile Device Security .............................................................................................................. 13  
   2.7 Mobile Applications .................................................................................................................. 14  
   2.8 Ethical Issues .............................................................................................................................. 16  
   2.9 Conclusion .................................................................................................................................. 18  
3. Methodology ..................................................................................................................................... 19  
   3.1 Introduction .................................................................................................................................. 19  
   3.2 Philosophy ................................................................................................................................... 19  
   3.3 Research Method ......................................................................................................................... 20  
   3.4 Strategy and Design .................................................................................................................... 21  
   3.5 Distribution and Process ............................................................................................................. 21  
   3.6 Analysis ...................................................................................................................................... 22  
   3.7 Ethical Considerations ................................................................................................................ 22  
   3.8 Bias Potential ............................................................................................................................. 22  
   3.9 Conclusion .................................................................................................................................. 23  
4. Results & Discussion .......................................................................................................................... 24  
   4.1 Introduction .................................................................................................................................. 24  
   4.2 Demographic Variables .............................................................................................................. 24  
   4.3 Knowledge of Technologies ....................................................................................................... 27  
   4.4 Security ...................................................................................................................................... 28
List of Figures

Figure 1 - Research Onion (Saunders, et al., 2009) ................................................................. 20
Figure 2 - Age of Participants .................................................................................................. 25
Figure 3 - Gender Distribution ............................................................................................... 26
Figure 4 – Results from Question 6: Out of the listed messaging services which do you use? .. 27
Figure 5 – Results from Question 8: Out of the listed messaging services, which do you believe are encrypted? ............................................................................................................. 28
Figure 6 - Results from Question 9: The security of your phone is important to you? .......... 29
Figure 7 - Results from Question 15: I am happy for the government to look at my personal data without my consent ........................................................................................................ 31
Figure 8 - Results from Question 16: Scenario 1 ................................................................. 32
Figure 9 - Results from Question 17: Scenario 2 .................................................................... 33
Figure 10 - Results from Question 18: Scenario 3 ............................................................... 34
Figure 11 - Results from Question 19: Scenario 4 ............................................................... 35
Figure 12 - Results from Question 19: Responses from those who are 25+ years of age........ 36
Figure 13 - Results from Question 20: Scenario 5 ............................................................... 37
Figure 14 - Results from Question 21 .................................................................................... 38
1. Introduction

Much of the world can communicate freely and the methods to do so are now wide ranging and differ in levels of security. From basic SMS messaging, to fully encrypted messaging, there are free and paid services in use by billions of people on a daily basis. These messaging services create many issues, some are ethically challenging. This paper will research the ethical issues of the highly encrypted services with a focus on WhatsApp, which uses end to end encryption to protect its user’s data.

Motivation
The motivation behind the research is to assess the ethical issues and the public’s opinion on the abilities of these encrypted services, especially when it comes to different levels of crime. To assess and define the core ethical issues is something that has not been done in detail before and this is the true inspiration behind this research. Being able to understand these complex issues will help drive better decision making by government and those looking to adopt new technology. Regarding existing research, a study by Caudill and Murphy (2000) looked at the basic ethical issues, but fails to discuss ethically challenging scenarios like those presented in this research. Also, Cohn-Gordon et al (2018) reports on the latest advances within group encrypted messaging but doesn’t consider, in detail, the ethical problems that arise from its use.

Outcome
The outcome of this research will present a clear overview of the ethical issues encrypted messaging services cause and the affect they have on the public. In this paper the researcher will be using a questionnaire to gather primary data alongside secondary research to generate a thorough analysis of the ethical issues behind this technology. The research sample will mainly consist of students, however there may be others who complete the questionnaire.
Aim, Research Questions and Objectives

Aim

- To assess and detail student’s response to the ethical issues created by encrypted messaging services, specifically WhatsApp
  o Should encrypted messaging services like WhatsApp be used openly by the public?
  o What ethical issues do these services create?

Objectives

1. Existing relevant academic literature will be reviewed and key findings will be documented.
2. Primary research will be conducted in the form of an online survey.
3. The results from both the primary and secondary research will be used to assess the ethical issues.
2. Literature Review

2.1 Introduction and Security

This chapter is going to be a review of relevant literature that concerns this field of study. Every section will discuss a different topic with the level of technicality increasing as the chapter progresses. Full references will be detailed in chapter 6.

Security is a major topic in 2018 as the world we live in becomes more digital, and the physical hardware to make systems and devices becomes cheaper. One of the definitions of Security is “The state of feeling safe, stable, and free from fear or anxiety.” (Oxford-Dictionary, 2018). Is this the way we feel about Information Technology (IT) Security? The model of being continually tracked and traceable is one which has found its way into today’s society. We all have the right to security in our lives, yet we are all exposed to vulnerabilities daily. As humans we try to avoid risk where possible, but there are those risks we cannot foresee. We must take precautions with technology in the same way we take precautions when we get into a car and put on our seatbelt.

2.2 IT Security

Most people now have smartphones and are welcoming technology into their homes through networked devices such as Hive and Amazon’s Alexa. But what most people don’t realise is the way they are making themselves more vulnerable to attack and surveillance like never before. Furnell and Thomson (2009) theorised that “security can be as much about people as it is technology” and how for it to be successful, we need to focus on “establishing the correct mindset”. As people are allowing more technology into their lives, are they really adjusting their mindset to compensate for the increased risk? The topic of terrorism and government access to data is an important one, the Financial Times reporting that “European countries and other developed nations suffered more deaths from terrorism in the past year than at any time since 2001” (Bond & Wisniewska, 2017), yet some people are still concerned about government monitoring.

Within the European Union (EU) there has been regulation introduced to try and govern the management and storage of personal data within the EU states. The General Data Protection Regulation (GDPR) 2016 acts as a reform on existing policy, the Data Protection Directive (DPD) 1995. Three major areas are addresses by GDPR; Legal standardisation across the European Union, Explicit consent for Processing and Lawful further use of data (Kotschy, 2014). As a regulation, GDPR aims to standardise control across the EU states, unlike the DPD which
was a guideline to create individual laws in each state. GDPR includes more specification on new technology and summarises the responsibility that an organisation has when collecting, storing and analysing personal information, specifically consent. There is further definition of ‘lawful use’ where organisations must delete personal data once it has been used for its consented purpose. This regulation is the biggest effort to control data use within the EU and should drive organisations to be more open and consumers/users to feel more confident when giving their information to a third party.

2.3 Privacy
As privacy is a core issue for many users of technology, it is important to consider the policies in place on social media. Many users just accept the default ‘open’ policy rather than spending time tailoring the privacy settings to something more suitable (Cheek & Shehab, 2012). Using the default settings for social media can expose user’s information, photographs and friends list, making it easier for criminals to steal this information and potentially sell it.

A prime example of social data harvesting was carried out through Facebook, by an organisation called Cambridge Analytica. They managed to collect “data of almost 87 million Facebook users” (Computing, 2018), a massive breach of privacy for millions of users. By using a legitimate application, the company managed to amass the names of user’s friends and their public profile. The users who had the default privacy settings, gave more information away to this organisation than those who had secured their profile.

The use of social media and the internet has created a ‘Privacy Paradox’, people want to feel secure and safe online, yet they will happily hand over private information to websites without question. The public want to be safe from snooping, yet don’t want to allow safe havens for criminals (Barnes, 2006). This just shows that the public, especially those who are younger and more naïve, really don’t understand the risks that sharing data creates. As the uptake of online social platforms increases, the risk of data being stolen increases as well, young people are enticed by the new technology and ignore any risk.

People’s perception of privacy is an important factor when considering the ethical issues with encryption. A comparative study carried out in Sweden by (Obradovac & Rodriguez, 2017) looked at the perception of Facebook privacy with a sample of both young and old adults. They found that 50% of the sample did not realise any risk to privacy whilst using Facebook. Furthermore, the group of young adult participants were less inclined to read a privacy policy and had less knowledge of the effects of social media on their privacy. It was only the older group within the sample, aged 36-70, who truly understood the way Facebook can affect their
privacy. If the current, younger, generation are not fully informed when making decisions online, they could not only risk the privacy of themselves, but also the privacy of their family and friends.

2.4 Mass Surveillance
Is terrorism used as an excuse by government for mass data collection and monitoring? The government can access our data secretly, if required, to combat crime, under the Investigatory Powers Act 2016. This act is designed to ensure the British security services and police have adequate electronic surveillance powers. But the original version of this act was hugely opposed due to concerns over privacy. With research finding that “Government intrusion concerns are positively related to privacy concerns” (Dinev, et al., 2008) it is no surprise people are becoming concerned with their online privacy. Metzger and Docter (2003) found “that while concern about privacy is high, few comprehensive policy options have been proposed” even with the introduction of the Investigatory Powers Act 2016, is this enough to protect users when online.

IT Security is of more significance nowadays as we all become more connected. Networked devices are now found in most organisations and public spaces, increasing the risk users face every-day. Beyond the increasing risk of compromised devices, there are also measures that must be taken to secure user’s data in the cloud and online, as people now integrate more freely with online storage and social media.

2.5 Cloud Security
The way people integrate with cloud computing is changing, for example, the amount of free cloud storage is increasing year on year and the public uptake of services such as these is huge. “The range of access device for the cloud has expanded in recent years. Home PCs, enterprise PCs, network computers, mobile phone devices, custom handheld devices and custom static devices (including refrigerators) are all online” (Mather, et al., 2009). There must be measures in place to ensure that there are no unnecessary vulnerabilities. Devices such as networked fridges and audio systems are at risk of hacks, which could see or hear into the user’s home.

A further area of risk that many people are unaware of, is internet browser security, one which has the potential to affect all of those users who don’t regularly update their computers. “It is essential for customers (the public) to maintain good browser hygiene. This means keeping the browser (e.g., Internet Explorer, Firefox, Safari) Patched and updated to mitigate threats related to browser vulnerabilities” (Mather, et al., 2009).
Beyond cloud security there are specific security methods adopted by companies to protect their user’s data. These methods can help deter those who want to steal a device physically or just its contents, which could be revealing personal information.

2.6 Mobile Device Security

The physical security of a mobile phone is an important factor for many people, with devices now costing more than £500. But what people take for granted is the security of the software and applications they use. With smartphones now able to hold hundreds of applications at once, there may be weakness in the security of that device. Whether it be photographs of your family at risk or the banking details which you save in your notes, security should not be over-looked.

Two Factor Authentication

“Authentication becomes much stronger by using a combination of both know and have factors” (Eide, 2015). These two factors make up the basis of ‘Two Factor Authentication’ or 2FA. An example given by Eide describes a user with a credit card making a payment, the card is the ‘Have’ factor and the PIN is the ‘Know’ factor. He goes on to state that for this security method to be compromised, the attacker would have to have both the card and the PIN code to utilize the card. As most people learn their PIN number and do not write it down it becomes difficult for an attacker to gain access to the card.

This method is also used within social media to confirm login authenticity, for example Facebook offers users the ability to enable 2FA as an added security measure. The user will attempt to login to Facebook from a new device, a laptop for example, and a code will be presented within the Facebook application on their mobile, this code is then required to enable a successful login.

Biometric Authentication

“Identification systems based on biometrics are capable of identifying persons on the basis of either physical or behavioural characteristics” (van der Putte & Keuning, 2000).

One of the most common forms of biometric authentication is fingerprint identification. Before a system can verify someone’s identity based on their biometric characteristics, a profile must be created in the system so it can compare against it for authentication. To ensure accuracy of people’s characteristics, fingerprints for example would be scanned multiple times (van der Putte & Keuning, 2000).
This form of authentication is now found in mobile devices across the world and offer a more secure platform, which is practical for the user. As well as fingerprint authentication, there are also amongst others, face, signature and voice recognition methods. Now mobile payment applications are becoming more popular and people are saving credit card information on their devices, security measures such as fingerprint authentication are a practical solution for adding extra security on top of standard four to eight-digit security codes (Yildirim & Varol, 2014). The most popular devices currently being sold by Apple and Samsung all offer fingerprint sensors for the added level of protection against theft.

This section has covered security and the main steps taken to protect user’s data and maintain the reputation of organisations. From the current UK and EU law that governs data management to the security techniques adopted by hardware manufactures to prevent data theft, there has been an extensive review. The next section will detail popular messaging applications, software and the vulnerabilities and security measures that exist.

2.7 Mobile Applications

Devices such as smartphones have enabled easier communication through online messaging services, these services are normally free and may offer video calling as well. The most popular messaging services used today are iMessage, Facebook Messenger and WhatsApp, the latter has 1.8 billion users in over 180 countries (Endeley, 2018). As we live in a security conscious world, where our data and messaging must be protected to secure our identity, these services now offer some level of encryption to maximize the protection of the user’s data.

iOS/Android

iOS is a very secure operating system, its API for controlling phone features such as SMS is limiting, forcing developers to ensure their GUI and instructions are clear and accurate. Having this reliance on the user to enter key information when authenticating applications such as WhatsApp, means there is little room for vulnerability unlike Android. Having a restricted API not only benefits Apple and their device integrity, but also the User, as their device and applications are less likely to be compromised. (Mueller, et al., 2014)

Android’s API is more flexible and allows a developer to take advantage of more advanced features of the operating system, unlike iOS. For example, when using a messaging application an Android application can "automatically extract the phone number and pre-populate the input field (although one could edit the number in all cases) and some even had a completely automated verification system" (Mueller, et al., 2014). However, enabling this level of
functionality in the API does open vulnerabilities and introduce some areas of concern. Application permissions within Android are very opaque in that they are offered to the user at the point of installation, but then stay in operation and can trigger functions without the user’s knowledge. An example of this would be the automatic capture and transmission of the phone’s contact list, which can be done without promoting the user, unlike iOS which would present a dialogue box to confirm this action (Mueller, et al., 2014).

**Encryption**

“In the past few years secure messaging has become mainstream, with over a billion active users of end-to-end encryption protocols through apps such as WhatsApp, Signal, Facebook Messenger, Google Allo, Wire and many more” (Cohn-Gordon, et al., 2018).

Encryption is the procedure of encoding information with a method that only allows people with the correct decryption key to read it. It does not protect against the interception of the data, but it will be unreadable to those who intercept it (University of Michigan, 2018). “This allows for data between communicating parties to be secure, free from eavesdropping, and hard to crack... End-to-End Encryption provides an effective way to prevent these attacks, and if it had been implemented properly by Yahoo Inc., it could have prevented large-scale attacks like the one Yahoo suffered in 2016 and 2013, where almost 500 million, and more than 1 billion accounts were respectively compromised (Endeley, 2018)”. Encryption has been seen by many as the solution to their privacy concerns, it can “further conceal the identity, locale, gender, and personality of the messenger” (Cooper, 1998). There are many ethical issues with encryption which cause people harm and discomfort. Criminals use it to aid deception, marketers and online influencers may use encryption to cover up digital manipulation and false advertising. Crimes such as defamation and slander can be carried out more easily behind the anonymity of encryption (Cooper, 1998). Where does the accountability lie, with the encrypted service provider or the users?

**WhatsApp**

WhatsApp used the Signal Protocol to enable end to end encryption, it encrypts both messaging and calls using an asynchronous method under a shared key. This method allows plausible deniability for the users when it comes to the receiving messages, as the receiver can be sure where it originated from but cannot prove the identity of the sender, enabling deeper security and safety for the users. (Bryant, et al., 2017)
As well as end to end encryption, WhatsApp uses SMS to link an account to a device, this will “… prevent malicious users to impersonate somebody else using the victim’s number, a verification SMS containing a 4-digit PIN is sent to the phone… This process binds a WhatsApp user account (represented by the phone number) to a physical device” (Schrittwieser, et al., 2012). Using this method, a person cannot access the account of that user unless they have physical access to the device and/or can clone the sim card. This method of two factor authentication is used in many applications as it ensures the user is who they say they are.

**iMessage**

Apple’s iMessage service is used on iPhones, iPads and Macs across the world and handles over 2 Billion messages a day. (Coull & Dyer, 2014) This amount of usage generates large amounts of network traffic which can be viewed and any data leakage captured. Coull and Dyer researched this potential vulnerability and found that within the network data they could “reveal information about the device operating system, fine-grained user actions, the language of the messages, and even the approximate message length with accuracy exceeding 96%.” They also found that vulnerabilities such as this one are applicable to WhatsApp, Viber and Telegram. This is by no means a breach of encryption, nor does it allow access to the raw data, but does offer an insight into the user’s activities and allows the metadata to be viewed (Coull & Dyer, 2014).

Now that the technology has been defined and detailed the researcher will consider the ethical issues that surround these technologies.

### 2.8 Ethical Issues

Technology presents lots of ethical issues in the modern world, from large corporations collecting information on your activities, to governments having access to your private data. It is a huge area of concern. Security online is crucial to ensure customers and suppliers can work in harmony.

Take E-commerce for example, “individuals are tracked, and information is collected from purchasing transactions as they surf through Web site” (Caudill & Murphy, 2000). This damages trust, which is an important part of making a successful commercial transaction. It transpires into E-commerce as the customer must trust who they are buying from and believe the website is secure and safe to use. A website is faceless and therefore ensuring potential customers are aware of the security measures in place is important (Gajendra & Wang, 2014). Lots of websites track users through cookies and then adjust their marketing accordingly. This,
along with the fact that “many websites are poorly secured” (Kumar & Singh, 2014) make the process unethical and misleading for the customers.

Richard Mason in the 1980s theorized that there are four key ethical issues in the information age, which are Privacy, Accuracy, Property and Accessibility, these are still applicable today. Privacy relates to what and how, as users, we should reveal about ourselves online and what things we can keep private. Accuracy asks the question of responsibility, who is responsible for ensuring the accuracy and authenticity of information in the digital world. An example of this issue in the media currently is the idea of ‘Fake News’. Property issues are something that we face every day, who owns the information we use and integrate with. We must also ask who owns the media channels through which this ‘information’ is pushed to users. (Mason, 1986) Lastly, Mason discusses Accessibility “What information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards?” (Mason, 1986). This idea of access poses lots of questions today as we all have lots of personal information stored by various organisations around the world.

Big Data and Ethics

“Big Data combines information from diverse sources to create knowledge, make better predictions and tailor services” (Martin, 2015)

Currently, Big Data is used by businesses across the globe to tailor services and target marketing more accurately. They are collecting more and more personal data and even though some customers realize the benefit, some are worried about the impact this might have on their online experience (Rubinstein, 2013). Is every company being fully transparent with the way they are using customer’s data, something that is now being more regulated by the General Data Protection Regulation 2016. “Not only does big data pose a threat to traditional notions of privacy, but it also compromises socially shared information” (Hartzog & Selinger, 2013). Most of the information we share online should only be visible to those who we share this information with, and we have laws and procedures in place to protect us, however “big data threatens to erode these structural protections” (Hartzog & Selinger, 2013). The ethical issues this creates will no doubt influence law makers and the way organisations can use big data in the future. Now organisations can use big data to analyse information on a wider scale they can influence large groups of people more easily, sometimes for unethical reasons.
2.9 Conclusion
This section has discussed the core literature within the Information Technology and Ethics fields finding that there is a lack of investigation into the ethical issues encrypted messaging services create. There is however, extensive analysis of the security benefits with encryption such as that carried out by Endeley (2018) and Bryant et al (2017). To ensure the researcher is fully informed on the subject matter, this review of literature has covered a wide variety of topics these include; Cloud Security, Mobile Device Security, Encryption, Mobile Messaging Applications, Ethical Issues and Big Data. With the analysis of literature being focussed on how security and more importantly encryption aims to help protect users and their privacy. The researcher found many articles which eluded to users not fully understanding the technology they are using and therefore developing the incorrect mindset, this then adds to the complex ethical issues that have been discussed such as terrorism and crime.
3. Methodology

3.1 Introduction
This section of my dissertation will discuss the methodologies chosen for this paper. As part of this dissertation I have been conducting primary research, alongside the literature review that will act as my secondary research. A detailed study is required to fully understand the area of interest and allows me to critically analyse the topic in question. Covered below are the various methods chosen and the philosophy behind my choices.

The study will include the collection of primary data, original data collected for this study, and secondary data, data collected from another study and reused to assist with the analysis of findings. Once this study has been completed it could be published and my primary data will add to the library of academic data which would then become secondary data if used by another for research paper. Large data sets are collected and published by universities and research institutes to aid others with studies and critical analysis of many topics (Hox & Boeije, 2005).

3.2 Philosophy
There are many philosophies which you can base your critical thinking on, these are shown below in the Research Onion, which outlines the key areas of thought for research. Saunders created this onion to summarize the following areas, Philosophy, Research Approaches, Strategy, Method Choice, Time and Techniques (Saunders, et al., 2009).

The philosophy for this paper is positivism as I am using quantitative methods of data analysis. The survey will be distributed to a wide range of people to canvas various age groups and those at different stages in academia, from A-Level students through to recent Graduates. The topic of ethics affects everyone, so it is important to collect quantitative data which can be compared easily.

There is however an argument that interpretivism and qualitative research methods can be used within technology/Information Systems research. “Despite the dominance of positivism, there are signs that interpretivism is gaining ground, and the epistemological choice between interpretivism and positivism is an important issue for IS researchers” (Walsham, 1995).

Qualitative research is something that I considered for my dissertation but due to the intricate topic which has many nuances, especially around the issue of crime, I chose to stick with positivism. It will give me enough data to compare the difference in opinion and views and as I am using a larger sample of people it will make the process of distribution and analysis easier.
3.3 Research Method
The method of collection for this primary data will be quantitative as this applies to larger data sets where numerical data can be analysed and turned into information. I am using a quantitative method to collect data and then study the relationship of these data sets to one another. Through a questionnaire I will be using structured questions and this will present me with quantified conclusions that, depending on the sample, can be generalized (Bell & Waters, 2014). The chosen research method is quantitative and this will be used as I am looking to analyse a large sample of data collected through a questionnaire; the numerical output of which will be analysed to find any patterns and then compare responses based on different criteria such as age and background. The questionnaire will be made available online and will automatically collate the data for comparison. Using the qualitative method is the best fit for this Positivist philosophy, whereby I am aiming to make a conclusion based on numerical data, an inductive approach. I will be gathering raw data through which analysis will become functioning
information. I will then use this information to make an informed conclusion, this can be taken as a generalisation of the sample’s opinion as my sample will be large.

3.4 Strategy and Design
The design of the anonymous questionnaire will be simple. Using an online tool called Qualtrics, an online questionnaire is created. Using Qualtrics makes the creation of a visually appealing questionnaire easy, this tool also offers mobile support so it can be completed by those who aren’t near a computer. Another benefit of using an online automated platform is that “time-consuming data entry errors can be eliminated through automated data checking” (Schmidt, 1997). Using an automated process will ensure the time spent processing the data is kept to a minimum. Making the questionnaire anonymous means I am not collecting any personal information which helps when storing the data. Also, when using an anonymous survey, it may encourage respondents to answer more truthfully, especially when discussing topics such as terrorism and crime, as they won’t feel like there can be any repercussions due to their comments. The question format will begin with basic data collection, age, occupation etc, then move onto the rating of how security conscious they are. The second section is made up of scenarios which are aimed to show the difference in opinion one might have on encryption, the scenarios move from innocent users to those wishing harm and disruption to the wider population. Users will then be asked if, due to these scenarios, they opinion on the issue at hand has changed.

3.5 Distribution and Process
The sample aims to reach both Cardiff Metropolitan Students and the wider public, this should give me a balanced view of how a student’s view of these ethical issues differ from those of the public. Distributing the survey via email enables me to reach out to large groups of people quickly with minimal effort. Using social media to promote my survey is quick and may tempt more people to complete it as they are already on their smartphone or computer and connected to the internet browsing social media. As many people will be disinclined to complete a lengthy questionnaire, the number of questions is kept to 20 all on one page, as multiple pages may discourage people from completing the questionnaire.

A set process for distribution will be used to ensure people are offered the questionnaire in the same way each time. The same amount of information regarding the research will be presented to each potential candidate and they will be given the link freely for them to complete at their convenience. The recipients will not be given a time frame for when the survey needs to be completed by as this may rush them and lead them to give false answers. This process will also
help me to keep my message clear to users and not confuse those who are unsure of the meaning and reasoning behind my research.

3.6 Analysis
Qualtrics generates numerical data which can be used to calculate summary statistics. The research aims to collect over 120 responses with my survey to create a large enough pool of results to run accurate data analysis, which can be utilised pull a good conclusion from, any less and the summary statistics and findings will be unsubstantiated. This number of responses represents an adequate amount of granularity for the scope of the project. As there are only a maximum of 4 months for the data to be collected there can be only be so much data processed. Even though more responses would increase the granularity, it would be unfeasible to process this in the given time frame. As soon as more than the required amount of responses has been gathered, analysis can begin. The analysis will involve the visualisation of data and then a discussion based on the findings themselves, these will be grouped and any identified trends will be discussed.

3.7 Ethical Considerations
At the beginning of each questionnaire the participants will be made aware of the anonymous nature of the research. The researcher will ensure all users take part voluntarily and without any influence on their answers, doing this maintains the integrity of the research and its outcomes. As the topic covers security, there is a small risk some users may hold back on answering truthfully, therefore the questionnaire was made anonymous. Participants will also be given my, the researcher’s, contact information in case they have any queries regarding the research or the measures taken to protect their information. Throughout the data collection the email account will be checked daily, to ensure any queries are dealt with quickly. The questionnaire’s content has been pre-screened by the university ethics committee, this ensures that the questions will not upset or offend any participants. As the survey is open to a large audience, it is important that the researcher makes these ethical considerations, as the risk of causing offence increases with a higher number of participants.

3.8 Bias Potential
The risk of bias is always present within research; it is important that there is adequate representation across the whole target sample. The research will not be limited to just university students, but open to the wider population, so the sample has the potential to be large. To minimise any bias within the questionnaire itself, the participant will be given minimal context for each question. A detailed explanation of the context for the question may influence the
response given. There is also a limiting factor within this data source as it is quantitative, the researcher can only find the participants opinion, not why they think that way. A Quantitative survey does however give a good overall representation of a sample’s opinion, as opposed to a qualitative interview where body language and facial expressions may bias the response. Due to the size of the sample the researcher is only seeing an extract of full picture, something that will be taken into consideration during the analysis of the data.

3.9 Conclusion
In conclusion, the research paper works to the methods outlined in this section. Both primary and secondary research will be conducted to support the research questions, should encrypted messaging services like WhatsApp be used openly by the public? And, what ethical issues do these services create? A positivism philosophy will be used and underpinned by a quantitative research method which is designed in the form of an online questionnaire. This philosophy has been chosen as it best fits with the method chosen for this research and will help guide the researcher. Using an online questionnaire enables the collection of more data as the researcher can push it to more people, more easily and then automate the collation process. Using email to dispense the questionnaire simplifies the distribution process and saves the researcher time. Once data has been collated and processed using Qualtrics, a thorough analysis will take place, within this the data will be visualised and findings discussed.
4. Results & Discussion

4.1 Introduction
The aim of this paper is to assess the ethical implications of encrypted messaging services such as WhatsApp. This section will detail the results of the primary research completed within this research project, an online questionnaire. Students at Cardiff Metropolitan were given the opportunity to complete the questionnaire via an email. The wider public were offered it through social media and email. In total the questionnaire received 145 responses, more than the minimum requirement mandated by the researcher. The results of this questionnaire will be shown below, alongside a discussion of its relevance to the research questions. Any patterns or trends will be presented and then a comparison against secondary research will take place where relevant. This will allow the researcher to critically analyse both the gathered primary data results and any existing research. The participants were given a context then had to select how they felt based on a Likert scale.

4.2 Demographic Variables
Age and gender are the core demographic variables of the paper’s study which will be analysed. Demographics are an important factor of the questionnaire as age, for example, can be used to determine maturity. The variables below are shown to help underpin the following discussion as they must be considered regarding the sample’s overall value as a data source. This sample represents a snapshot of opinion for a mostly younger audience.

Age
As shown in Figure 2, below, most of the sample are aged between 18-24, this is due to the majority being university undergraduate students. The results would be more applicable for statistics if they included a wider range of ages. However, I can infer from this information that most of the participants are millennials who should have an adequate understanding of technology and should use some form of messaging service. Having this basic understanding of technology will mean they may have a more relevant opinion of the ethical issues, as they might come across them on a weekly, if not daily basis.
There are 25 participants who are over the age of 24, this is shown in Appendix 1, these participants may offer a different perspective on the ethical aspect of the questionnaire as they should have more life experience. This does indicate though that some participants may have less technical skills if they are from an older generation who have not been as exposed to new technology as the under 25s. Age was a defining factor for Obradovac and Rodriguez’s (2017) study in which they assessed the perception of privacy in both young adults and adults. Their age ranges for each group were 16-35 and 36-70. They found that age truly affected the way in which their sample responded to privacy issues on Facebook. All findings in the current study will be examined to see if there are any discrepancies when the results are filtered by age.
Gender Distribution

The results from the questionnaire show the researcher that over 70% of the sample are female, shown in figure 3, a large imbalance in gender within the participants. However, gender should not affect the validity of the results as there shouldn’t be a discrepancy between genders on ethical issues, unless they related to gender. Nevertheless, a study has shown that gender can affect the uptake of new technologies, for example in the study Venkatesh and Morris found men focus their utilisation on usefulness whereas women focus on the ease of use. This finding was made whilst considering prior experience with computers. (Venkatesh & Morris, 2000).

Within the results there was only one question which had a visible change if filtered by gender. Question 19: Scenario 4 asked the participants to use a Likert scale to agree or disagree with unconsented government access, for a terrorism investigation. The results showed that the female members of the sample answer more strongly when asked this question. This could indicate that when lives are at risk women are more compassionate and caring then the male members of the sample, who answered more weakly. However, there was no visible pattern across the results that indicate gender influenced any other responses. The researcher will consider the gender bias when concluding.

Figure 3 - Gender Distribution
Occupation

Results show that 93% of the respondents are students, with 6% holding other occupations. This shouldn’t affect the results as the aim is to understand the student’s perspective on ethical issues. The researcher had hoped to get more responses from those in other occupations, but this was difficult to achieve within the given timeframe. Appendix 2 shows the percentile split of the sample’s occupation.

4.3 Knowledge of Technologies

The sample showed a mixed understanding of the technologies presented to them. Some participants showed they used additional applications and others stated they used solely WhatsApp. This demonstrates a level of technical maturity within the sample, as the majority understood the question and could differentiate between the various messaging applications presented. More people in the sample use Facebook Messenger than WhatsApp, but only marginally. Figure 4 shows the messaging applications used by the sample. One participant did state that they used ‘Encrypted Facebook Messenger’ within the Other field, this shows that there is one participant who understands the capabilities of the application.

![Figure 4](image)

*Figure 4 – Results from Question 6: Out of the listed messaging services which do you use?*

However, many participants don’t realise that there is a device to device encryption in the other messaging services shown. This is shown in figure 5, where a huge majority of people selected WhatsApp as the only encrypted services out of the list of the 5 major encrypted services. Evidently WhatsApp has made it clear to their users that the service now uses end to end encryption, unlike services such as iMessage. As Cooper (1998) found there are many ethical
issues that surround messaging services such as these and the users may not be aware of the capabilities. A revelation is that 28% of the sample state they do not know what encryption is at this point of the questionnaire. The lack of understanding may affect their answers later in the questionnaire, that is why the researcher chose to give a detailed context before the scenarios, which explained the capabilities of WhatsApp’s Encryption. Within the section discussing these scenarios, I will compare how this 28% respond to the scenarios and how their opinion varies to those who have a ‘more detailed’ understanding of what encryption is.

Figure 5 – Results from Question 8: Out of the listed messaging services, which do you believe are encrypted?

4.4 Security

Security is presented as a core issue, with 72% of the sample stating that the security of their phone is important to them, shown in figure 6. This shows most of the people sampled believe there is a risk, both physically and electronically to their device. The researcher believes that if they are concerned with the physical security that means both the electronic contents and financial value of the device are important to the user. Mobile phones are becoming more expensive, which means they are now more of a security concern to users. Furnell and Thomson (2009) believe that people are at the core of technology and that unless the correct mindset, i.e. one that fully understands the risks, is created technology will cause more issues
than solutions. The sample show that they at least have, at minimum, an understanding of the material value of their electronic devices and hopefully some understanding of the risk of using an online messaging service. On the next question, 10, an even larger 77% of the sample believe that their laptop/computer’s security is hugely important to them, showing that security really is at the forefront of people’s minds. Results from question 10 are shown in appendix 3. The researcher now believes that, overall, the participants have a real concern for security, this should drive them to answer more truthfully when presented with ethically difficult scenarios in the second section.

Figure 6 - Results from Question 9: The security of your phone is important to you?

Enderley (2018) found that end to end encryption could be the digital security solution that stops the concern within the general population. Data breaches such as Yahoo could have been easily prevented if encryption was correctly implemented. The sample shows that even though there are many methods of digital security available, many people are either not taking advantage of them or are unaware of the methods available to them. If greater emphasis was put into warning users of the risk, not just the benefits of the many applications and websites offered to them, then maybe people would approach technology with a more positive and enlightened mindset.

4.5 Government Access and Privacy
The threat of terrorism is a fear that many people sense and since 9/11 there has been heightened tension in large cities and at big events such as the Olympics. In light of this, the amount of government surveillance has increased, which in the eyes of some people is an
issue. The results show that 97% of people who completed the questionnaire Agree or Strongly Agree that they should be able to contact friends and family securely. Results from question 11 shown in appendix 4. Everyone has the right to their privacy yet should this come before the safety of others. WhatsApp’s use of encryption adds an extra level of complexity to this issue as even the government cannot crack encryption, therefore even those using the service innocently are driving a privacy uprising.

The results from question 15 show that only 30% of the participants are Neutral, Agree or Strongly Agree with unconsented Government access to personal information. This is however without context, as the scenario questions regarding government access with context, present different results. Alongside potential unconsented government access, Hartzog (2013) found that big data is already eroding the protection we have of our data, now more of it is being shared with third parties. But this 30% still believe there is valid reason for government access, some of whom may have been victims of crime or terrorism, so are happy to waive their right to privacy, in a hope that it may protect others. The other 70% of the sample disagree with government access, this is the norm as most people feel they have a right to privacy even in the digital age. Even this 70% may be sharing data with multiple organisations freely without any concern about privacy, nor the validity of the data security procedures in place. The use of encryption reduces the risk of personal information being stolen, as most of the time even the company operating the service has no access to the information. Figure 7 shows the results from question 15.
The results from the scenarios in the questionnaire present some interesting outcomes, there is a big push towards neutrality on ethically difficult questions. However, there are stronger feelings on questions which involve privacy and terrorism. This section of the findings will discuss the results from the scenarios and how they change based on targeted filtering.

Question 16 is the first scenario the researcher used within the questionnaire. Scenario 1: A group of students are using WhatsApp to communicate in a group chat, discussing their modules and timetable. "I believe these students should be allowed this level of security and protection."

**Question 16**

Results from question 16 show that most participants agree with students using encrypted messaging for the discussion of university matters. The context is very clear ethically as there is nothing malicious or illegal occurring whilst the encrypted messaging service is being used, this is shown in the result as 116 respondents, 80%, agree this should be allowed. This gives the
researcher a base for comparison as the participants allow for ‘innocent’ use of encryption but may not for more ethically challenging situations. Figure 8 shows the results from question 16.

![Figure 8 - Results from Question 16: Scenario 1](image)

**Question 17**

Question 17 is the second scenario given to the participants and is designed to help show the contrast between an ethically sound situation as shown in question 16 and one which is more challenging. In this scenario they were given a context containing terrorism, ‘A terrorist cell operating in the UK are using WhatsApp to plan an attack, discussing timings and locations.’, they were then again asked if they believe encryption should be allowed in this scenario. As shown in figure 9, the response is highly negative and when compared with Figure 8 above, shows a huge contrast. The sample are very clear about these two topics, students can use encryption, but not terrorists, this presents an issue, should encryption therefore be banned. As a society we can either be allowed to freely use encrypted messaging services or encryption could be banned for public use, there is no middle ground with this technology. But as Mason (1986) states, privacy is one of four key ethical issues within the information age, with encryption seen by many as the solution, so a ban on encrypted messaging services could impact the privacy of millions of people.
There was however, an interesting finding when the results are filtered to show only those who did not know what encryption was at the beginning of the questionnaire. The results from this section of the sample show that there is still a lack of understanding when asked this question as there is a 7% increase in the selection of ‘Strongly Agree’ on the Likert Scale. This result makes the ethical issue of terrorism more shocking as there are people within the sample that, even after a detailed explanation, still don’t fully understand the consequences of encrypted messaging. It is the harrowing acts which terrorists have planned over WhatsApp that make encryption for the masses a huge issue. Results for this finding are found in appendix 6.

**Question 18**

Question 18 was designed to address a more ethically difficult scenario, where the act being carried out is morally correct but illegal. The context was a person who struggles with chronic pain after an accident buys marijuana from a drug dealer using WhatsApp. They find that marijuana is much more effective than off the shelf drugs at managing their pain. This issue is in a very grey area, they are using WhatsApp for illegal purposes but, as the results show, people are more neutral towards this use case as it helps make a person’s life easier. Participants do not want to condone illegal drug usage, but they also don’t want to deprive the person of something that helps them managed their chronic pain. The fact that marijuana is a Class B drug and has been glamorized in music might make it more acceptable then so called ‘hard’ drugs like cocaine and methamphetamine. This doesn’t however detract from the fact that there
is a glaring contrast in responses compared to the previous scenario, terrorism, which is seen by many as a reason for the removal of encryption from messaging services. Figure 10 shows the amount of neutrality within the sample for question 18.

![Figure 10 - Results from Question 18: Scenario 3](image)

**Question 19**

Scenario 4 is designed to capture the sample’s opinion on government access to their information. Since the *Investigator Powers Act 2016* was introduced there has been great discussion about the invasion of privacy by the government. The scenario’s context describes that the government needs to access personal information secretly to potentially capture a terrorist cell, who are planning an imminent attack in the local area. Participants are then asked would they be happy for the Security Service (MI5) to look at their communications even if they haven’t committed a crime themselves. As figure 11 shows, the majority have selected to agree, and would be happy for the government to access their information. This reveals they are willing to give up their right to privacy in a hope that it could save the life or lives of others. An interesting result, as without context 70% of the sample stated they would not be happy with the government accessing their information on question 15. Clearly, once the core ethical issue has been made apparent, in this case fighting crime, the sample become more acceptable towards government access to their data. If there was the ability to opt-in to government access the problem could be more controlled, but with encryption there is no option. If a messaging service
created a so called ‘back-door’ into a user’s encrypted data it would only become a target for hackers and therefore generate risk which most users would not want to accept.

When the results from this question are filtered to people over the age of 25, an interesting change is visible as the strength with which the sample answered increases, shown in figure 12. Age and therefore maturity can be viewed as having an impact on the results, as the older members of the sample feel more confident when answering on this ethically difficult scenario. Those over 25 will have more life experience than the younger members of the sample and consequently will have come across issues such as this before and may have been affected. The data also shows a slight reduction in neutrality when the under 25s are taken out of the results, showing that due to their lack of life experience they may feel unable to answer strongly.
Question 20

The 5th and final scenario that was presented to the participants considers a protestor’s use of WhatsApp for the disruption of a politician’s work. The subject is ethically difficult as the act is not illegal but some would believe that disrupting the work of a politician is not the correct way to enact change, even if the politician has made incorrect decisions in the past. The results support this view as 40% of the respondents were Neutral towards the subject, with the next biggest group being Disagree at 26%, presented in figure 13. Once the age range is again changed to those aged 25+ there is, again, more strength in the responses and less neutrality as the older group of participants should have more experience with politics. The results from scenario 5 filtered to only show responses from those who are 25+ years of age is shown in appendix 5.
Figure 13 - Results from Question 20: Scenario 5

4.7 Perception of WhatsApp & Encryption

The final question that the sample were given asked: “After considering these scenarios, has your perception of WhatsApp, its encryption and data security changed?” The results show that over 44% of the people who completed the questionnaire are neutral when asked if their perception has changed. 39% of the sample agree that their perception has changed and this shows that by presenting ethically challenging scenarios and situations to people they are inspired to really consider the issues at hand.

The neutrality of the consensus informs the researcher that there is still a real problem with the way that people are using encryption so freely, if the young sample are unwilling to address the issue in detail, these ethical problems may continue to cause issues. If these difficulties are not confronted does this drive the government to take drastic action to resolve the issue or will we have to accept that encryption for the masses isn’t the perfect solution for privacy.

Similar to the study that Furnell and Thomson (2009) carried out, the mindset of the sample has an effect on the way they approach the technology. It is important to consider the mindset of the sample when looking at perception as they may not be ready to contemplate the bigger issues that WhatsApp and encryption has on the public. The results from this question show a similar trend to those found by Obradovac and Rodriguez’s (2017) study, those who are younger tend to be less aware of the privacy issues caused by the use of social media. If this is the case, and the younger members of the sample are not informed enough of the consequences of their
social media and messaging use, this could lead to a future generation who are not risk aware and do not consider the privacy risks of the internet.

Figure 14 - Results from Question 21

4.8 Discussion
Throughout the results there has been a noticeable focus on privacy and how the sample are highly concerned with privacy yet will immediately give up that right to help protect others. This brings the researcher to look at the necessity for a technology such as encryption for public use, why do people believe we need it when the risk is relatively low. The idea of the Privacy Paradox (Barnes, 2006) is one which has been discussed in chapter 1 and can be related to the researcher's findings above. With the usage of social media increasing people are becoming less concerned with how secure they are.

Social networks for example normally offer their users a customisable privacy policy, which can be adjusted to either open access or lock it down to a few close friends. As most people normally just accept the standard permissive policy there is a high risk of information leakage (Cheek & Shehab, 2012). This still stands within encrypted messaging services, normally users just accept the standard settings and begin usage. If they are willing to take this risk, why do they need encryption at all, only some users will configure their privacy settings in detail. The sample state that privacy is of the upmost importance, yet only a small percentage of them could identify an encrypted messaging service, even though a large percentage of them are
being used by the sample themselves. If they are not aware of the security measures in place, this shows that deep down they are not as concerned with privacy as they first stated.

4.9 Conclusion
In summary, the research has found that there are many ethical issues that are created using encrypted messaging services. The sample which took part in the online questionnaire had a mixed understanding of the technology and therefore there was a diverse response to the ethical issues when they were presented to them. Within the results, age and therefore maturity was shown to influence the way people responded to questions. When the sample was filtered to those over 25 years of age, there was a visible increase in the strength of answering across the entire questionnaire. The younger members of the sample being visibility more neutral, unwilling to truly confront the issues at hand. The sample showed that they use a variety of messaging services, all of which are encrypted. They presented a dedication to security and a fondness of encryption as it helps protect against hacks or unconsented government access, the latter being opposed by nearly 70% of the sample.

The scenarios offered an insight into the ethical issues and how they are received when contrasted with ethically sound use cases. Issues such as government access and crime are opposed and seen as unethical, until the sample are presented with an ethically challenging scenario and then these become ethical. It only takes one difficult subject and the opinion of the sample can change drastically, but this itself is the main issue. Encryption is either allowed and anonymity ensues, or there is a ban on encryption and privacy is risked. In such a situation, criminals would need to find alternative methods to remain anonymous. As a large proportion of the sample stated, they are unaware of which applications are encrypted yet they still use them. This has informed the researcher that the participants are not using these applications for their encryption, it is more likely they only use them due to convenience and their popularity. Therefore, their use of these services should not be affected if the encryption was removed, some users might find other means of securing their devices, but the research doubts that it would cause a major issue.
5. Conclusion and Evaluation

The aim of this research paper was to assess the ethical implications of encrypted messaging services. To reach this aim, objectives were set and research questions were posed to ensure the study was carried out with a clear mandate. The three objectives for this study are shown below.

1. Existing relevant academic literature will be reviewed and key findings will be documented.
2. Primary research will be conducted in the form of an online survey.
3. The results from both the primary and secondary research will be used to assess the ethical issues.

All objectives were completed by the researcher without fault. Objective one is completed through chapter two in the literature review, where there is an analysis of existing literature pertinent to this study. Objective two was detailed in the third chapter, where a methodology was completed. It was then completed easily using Qualtrics and a sample of 145 people was generated. The final objective was completed within section four where the results from the questionnaire were used to detail and review the ethical issues generated through the use of WhatsApp. The relevant literature found within the literature review was then used to compare and contrast the results and identify and patterns or similarities.

Research Questions

Alongside the aim of this study there were two research questions posed, these were used to ensure that two lines of inquiry could be created within the research. These helped guide the researcher when creating the survey, analysing results and writing this conclusion. The two research questions are shown below and answered based on the findings of this research:

1. Should encrypted messaging services like WhatsApp be used openly by the public?

The first research question was posed due to the increasing ethical issues that are being created through the use of encrypted messaging services, specifically WhatsApp. From petty crime and drug dealing to high profile terrorism investigations, these messaging services have always had a negative press. However, the sample found that overall, privacy was extremely important, and they felt that they should be able to message in private, away from government surveillance and safe from the risk of criminals wishing to steal their data. But does this necessity for privacy outweigh the bearing it is having on the execution of criminal activities?
The use of these services by criminals is just another hurdle for law enforcement services to jump over. This is a major issue; one which governments worldwide are debating, therefore an answer to this question has to be balanced. Encryption is regarded by some as a right, enabling anonymity and free speech to the masses, and an invisibility cloak to criminals. Should these services be openly used by the public? The researcher believes yes, they should be allowed, for two key reasons. Firstly, encryption not only protects users, it enables freedom of expression, there are more people using these services with good intentions than bad, so there is not enough of a precedent for it to be banned. Secondly, criminals have and will, find ways of avoiding capture, if the use of encrypted messaging was banned for public use, these criminals would only find another way of evading law enforcement.

2. What ethical issues do these services create?

The second research question aims to define the main ethical issues that encrypted messaging services create. The first issue, and one that was reacted to strongly by the sample, is responsibility this comes from the need for privacy in this digital age which is a right to all but drives companies to introduce encryption. Having encryption removes the responsibility that companies have, if they cannot see what their users are sharing and saying through their networks they have plausible deniability. Removing responsibility means no organisation is accountable for the actions of their users, even if there are heinous crimes being committed. Responsibility then becomes an issue for the police and other law enforcement agencies, who do they hold accountable, those that facilitate these services or just the criminals.

Secondly, some say encryption does more harm than good but the argument stands that the police have multiple ways of detecting and tracking criminals yet the general public have limited means to safeguard their privacy. The public have the right to their privacy so surely that outweighs the small percentage of those who use it for crime. There would be a public outcry if the government banned these services, as they would if door locks where banned, the public want to feel secure and safe. To summarise, both legal responsibility and privacy are key ethical issues created by the use of services such as WhatsApp.
Limitations

Whilst completing the research, some limitations were found due to various constraints, this section will review these limitations. Firstly, the sample size was adequate for the purpose of this research paper but if increased, it would add more detail and statistical significance. Having the questionnaire targeted at mainly students rather than the wider public narrows the pool of opinion that could be collected. To counteract this the researcher would review and redesign the questionnaire to collect more detailed responses. Some questions would be made more direct and the addition of interviews would help generate a more rounded understanding of the sample’s opinion. A questionnaire can only inform the researcher what a person believes not why they believe it, an interview gives a more comprehensive overview of their opinion. The extra detail gathered from a revised questionnaire and the addition of interviews will help create a more innovative discussion which can be more critical of the issues at hand. If the topic was more focussed on the legal implications of encrypted messaging services a more detailed analysis could be completed as the law regarding data protection has recently been overhauled.

Future Work

While this research has detailed the ethical issues with encrypted messaging services there is room for expansion as the topic is vast and ever developing. Below there is a summary of the potential areas for expansion and development beyond the completed research.

- Encrypted Messaging and Crime

Developing from this report’s findings an anonymous survey which would investigate the criminal use of encrypted messaging services within a university setting, would give further insight into services such as WhatsApp. There is limited research in this field due to the ethical implications of people admitting to crime yet this could generate a snapshot of the amount of illegal activity on these secure and anonymous services. From these findings a thorough discussion can be had about the current legislation in place and its ability to prevent crime and capture criminals who use this medium.

- The Perception of Privacy and it’s Necessity

In addition to the example above, another area which could be assessed in detail is the perception of privacy in the modern world and how necessary it really is. This review could use a comparison of two groups from different demographics and see if things such as background or wealth affect their perception. There may be instances where those who are more privileged have a different view on privacy and take a stronger stance on the issue than those who are of a
lesser income. This view may stem from an increased exposure to technology through their childhood and may offer a thought-provoking set of results.

- Technical limitations of mobile security

A detailed analysis of the technical capabilities and vulnerabilities of mobile devices such as the Apple iPhone and Samsung Galaxy range. There is intense discussion on the weaknesses of both company’s mobile security, with the FBI paying a firm to hack into an iPhone for a terrorism investigation. There could be security suggestions that can be made based on an analysis of the major smartphone’s capabilities.

- Encryption and Responsibility

An analysis of past legal cases that concern responsibly for encrypted data across the world is an interesting topic especially as the findings can be compared with the latest General Data Protection Regulation 2016 legislation. There are multiple instances of companies being held accountable for customer’s data even though they are not aware of the customer’s actions. A thorough study of these cases and the relevant legislation worldwide would create a wide-ranging summary of research that could be used as reference for governments worldwide.

These areas are all expansions of the topic of this thesis and present a framework for future work which may be completed.

Final Conclusion

This final chapter has summarised the findings of this thesis, answered the research questions and looked at how this topic can be expanded on in future research. This research has found that encryption causes a multitude of issues both ethically and legally, due to the multifaceted uses of this technology. It is important to consider the huge impact that a technology such as this has on the public, it offers both anonymity and deniability. Two things which are both highly important and must be considered in detail when both lobbyists and members of parliament discuss the control of technologies such as this. The findings have shown there many people are concerned with privacy yet don't fully understand the extreme capabilities of encryption and ethical issues it creates. These issues are here to stay and as people purchase more and more networked devices, security and privacy are going to become even more of an issue as people expose themselves to more risk. Encryption is only the beginning, soon people will be able to anonymise the majority of their actions but this may be offset by advances in criminal detection.
6. References


Bond, D. & Wisniewska, A., 2017. Terror attacks on developed nations hit 16-year high. [Online] Available at: https://www.ft.com/content/3c258898-c95c-11e7-ab18-7a9fb7d6163e [Accessed 05 April 2018].


7. Appendices

### Appendix 1 - Age of all participants

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Percentage</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 18</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>16-24</td>
<td>71.11%</td>
<td>64</td>
</tr>
<tr>
<td>25-34</td>
<td>14.44%</td>
<td>13</td>
</tr>
<tr>
<td>35-44</td>
<td>6.67%</td>
<td>6</td>
</tr>
<tr>
<td>45-54</td>
<td>9.56%</td>
<td>5</td>
</tr>
<tr>
<td>55+</td>
<td>1.11%</td>
<td>1</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>1.11%</td>
<td>1</td>
</tr>
</tbody>
</table>

### Appendix 2 - Occupation of all participants

<table>
<thead>
<tr>
<th>Occupation</th>
<th>Percentage</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student</td>
<td>92.10%</td>
<td>135</td>
</tr>
<tr>
<td>Other</td>
<td>6.90%</td>
<td>10</td>
</tr>
</tbody>
</table>

### Appendix 3 - Results from Question 10: The security of your laptop/computer is important to you?

```plaintext
Strongly Agree
Strongly Disagree
Disagree
Neutral
Agree
```

Appendix 3 - Results from Question 10: The security of your laptop/computer is important to you?
Appendix 4 - Results from Question 11: I should be able to message friends and family securely

Appendix 5 - Results from Question 20: Scenario 5 Responses from those who are 25+ years of age
Appendix 6 - Results from Question 17: Scenario 2 - Filtered to only show those who have stated they do not know what encryption is.
How old are you?

- Less than 18
- 18-24
- 25-34
- 35-44
- 45-54
- 55+
- Prefer not to say

What is your gender?

- Male
- Female
- Unspecified
- Prefer not to say

What is your nationality?

[Textbox]

What is the highest level of education currently achieved?

- GCSE or Equivalent
- A-Level or Equivalent
- Undergraduate Degree
- Other (Please State)

Appendix 7 - Questionnaire Section 1
What is your occupation?

- Student
- Other

Out of the listed messaging services, which do you use?

- iMessage
- WhatsApp
- Facebook Messenger
- Signal
- Viber
- Other (Please List)

Out of the listed messaging services, which do believe are encrypted?

- iMessage
- WhatsApp
- Facebook Messenger
- Signal
- Viber
- I don’t know what encryption is.

*Appendix 8 - Questionnaire Section 2*
"The security of your phone is important to you"
(Please select how you feel about this statement)

○ Strongly Agree
○ Agree
○ Neutral
○ Disagree
○ Strongly Disagree

"The security of your Laptop/Computer is important to you"
(Please select how you feel about this statement)

○ Strongly Agree
○ Agree
○ Neutral
○ Disagree
○ Strongly Disagree

"My privacy is important to me, I should be able to message friends and family securely"
(Please select how you feel about this statement)

○ Strongly Agree
○ Agree
○ Neutral
○ Disagree
○ Strongly Disagree

Appendix 9 - Questionnaire Section 3
"I am happy for the government to look at my personal data without my consent"
(Please select how you feel about this statement)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

WhatsApp is a messaging application that uses a highly advanced encryption method, meaning that the messages are unreadable, even to the Government and Police. This next set of questions are scenarios based on the use of WhatsApp.

Scenario 1:
A group of students are using WhatsApp to communicate in a group chat, discussing their modules and timetable.

"I believe these students should be allowed this level of security and protection."
(Please select how you feel about the statement above)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Appendix 10 - Questionnaire Section 4
Scenario 2:
A terrorist cell operating in the UK are using Whatsapp to plan an attack, discussing timings and locations.

"I believe encryption should be allowed in this scenario."
(Please select how you feel about the statement above)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Scenario 3:
A person was severely injured in a car accident, they now live with chronic pain. They have found that smoking Marijuana, helps relieve that pain much more effectively than mainstream drugs.

"In the scenario above, would you be happy for this person to communicate with a drug dealer on WhatsApp to purchase Marijuana? Even though doing so is illegal."
(Please select how you feel about the statement above)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Appendix 11 - Questionnaire Section 5
Scenario 4:
The Security Service (MI5) are investigating a potential terrorist group in your local area, they believe that an attack is imminent. As part of their investigation they need to rule out suspects without informing them, to maintain the investigation’s integrity and security. To rule out these suspects they need to access their personal data.

"In this situation would you be happy for the security service to look at your communications, without informing you, even if you haven’t committed a crime."
(Please select how you feel about the statement above)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Scenario 5:
Mr Brown is a political activist who has made it their personal duty to protest a senior politician’s failings recently. Mr Brown uses WhatsApp to organise protests and rallies wherever the politician goes to disrupt their work. He uses this disruption as payback for the politician’s failings.

"In this scenario would you be happy for this activist to communicate securely, disrupting the politicians day to day business?"
(Please select how you feel about the statement above)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Appendix 12 - Questionnaire Section 6
After considering these scenarios, has your perception of WhatsApp, its encryption and data security changed?
(Please select how you feel about the statement above)

- [ ] Strongly Agree
- [ ] Agree
- [ ] Neutral
- [ ] Disagree
- [ ] Strongly Disagree

Thank you for taking your time to complete this questionnaire. I hope it has helped you consider the ethical issues with encryption and the problems that arise from its use.

*Appendix 13 - Questionnaire Section 7*
When undertaking a research or enterprise project, Cardiff Met staff and students are obliged to complete this form in order that the ethics implications of that project may be considered.

If the project requires ethics approval from an external agency (e.g., NHS), you will not need to seek additional ethics approval from Cardiff Met. You should however complete Part One of this form and attach a copy of your ethics letter(s) of approval in order that your School has a record of the project.

The document Ethics application guidance notes will help you complete this form. It is available from the Cardiff Met website. The School or Unit in which you are based may also have produced some guidance documents, please consult your supervisor or School Ethics Coordinator.

Once you have completed the form, sign the declaration and forward to the appropriate person(s) in your School or Unit.

Participant recruitment or data collection MUST NOT commence until ethics approval has been obtained.

PART ONE

<p>| Name of applicant:                  | Alexander John Bowler          |
| Supervisor (if student project):    | Dr Simon Thorne                |
| School / Unit:                      | School of Management           |
| Student number (if applicable):     | ST20056379                     |
| Programme enrolled on (if applicable): | Business Information Systems     |
| Project Title:                     | The Ethical Implications of Encrypted Messaging Services: An Investigation into WhatsApp |
| Expected start date of data collection: | 15/01/2018                   |
| Approximate duration of data collection: | 6 Weeks                      |
| Funding Body (if applicable):       | Click here to enter text.      |
| Other researcher(s) working on the project: | If your collaborators are external to Cardiff Met, include details of the organisation they represent. |
| Will the study involve NHS patients or staff? | No                            |</p>
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will the study involve taking samples of human origin from participants?</td>
<td>No</td>
</tr>
</tbody>
</table>

| Does your project fall entirely within one of the following categories: |
|------------------------------------------------------------------------|--------|
| Paper based, involving only documents in the public domain             | No     |
| Laboratory based, not involving human participants or human tissue samples | No     |
| Practice based not involving human participants (e.g., curatorial, practice audit) | No     |
| Compulsory projects in professional practice (e.g., Initial Teacher Education) | No     |
| A project for which external approval has been obtained (e.g., NHS)     | No     |

If you have answered YES to any of these questions, expand on your answer in the non-technical summary. No further information regarding your project is required.

If you have answered NO to all of these questions, you must complete Part 2 of this form.

In no more than 150 words, give a non-technical summary of the project:

This project is going to consider the ethics of modern messaging services. My primary research will look at the opinion of the public and how their opinion may change when shown the extreme scenarios surrounding these messaging services. Encryption is becoming more and more common in the modern world, and my secondary research will look at IT security and how encryption is effecting the ethics behind it.

DECLARATION:

I confirm that this project conforms with the Cardiff Met Research Governance Framework.

I confirm that I will abide by the Cardiff Met requirements regarding confidentiality and anonymity when conducting this project.

STUDENTS: I confirm that I will not disclose any information about this project without the prior approval of my supervisor.

Signature of the applicant: ____________________________ Date: _____________

FOR STUDENT PROJECTS ONLY

Name of supervisor: ____________________________ Date: _____________

Signature of supervisor: ____________________________
**PART TWO** only to be completed if primary research is to be undertaken

<table>
<thead>
<tr>
<th>A RESEARCH DESIGN</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 Will you be using an approved protocol in your project?</td>
</tr>
<tr>
<td>A2 If yes, please state the name and code of the approved protocol to be used</td>
</tr>
<tr>
<td>A3 Describe the research design to be used in your project</td>
</tr>
</tbody>
</table>

The design of the research will be centred around a questionnaire, summarised below.
- The researcher aims to get around 90+ questionnaires completed to ensure the data collected is valid and they have enough data to see any trends.
- The questionnaire itself should only take 5-7 minutes to complete.
- Questionnaires will be delivered both physically and electronically to the public as well as students at Cardiff Metropolitan University.
- The electronic version will be created using Qualtrics.
- An example of the questionnaire is attached below.

The sample type is described below.
- It is open to the public and is therefore random in nature.
- The researcher is estimating it to be roughly 90 people in size however this is only an approximation and there may be less or more people questioned.
- This number of participants should help the researcher created a detailed opinion on the subject and fully understand what people’s views are.
- The sample will be chosen by offering people the opportunity to complete the questionnaire at random, both online and physically.

---

1 An Approved Protocol is one which has been approved by Cardiff Met to be used under supervision of designated members of staff; a list of approved protocols can be found on the Cardiff Met website here
- Online questionnaires will be offered on social media.
- Results will be anonymous and the sample will be made aware how their confidentiality will be protected.

<table>
<thead>
<tr>
<th>A4 Will the project involve deceptive or covert research?</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5 If yes, give a rationale for the use of deceptive or covert research</td>
<td>N/A</td>
</tr>
<tr>
<td>A6 Will the project have security sensitive implications?</td>
<td>No</td>
</tr>
<tr>
<td>A7 If yes, please explain what they are and the measures that are proposed to address them</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**B PREVIOUS EXPERIENCE**

<table>
<thead>
<tr>
<th>B1 What previous experience of research involving human participants relevant to this project do you have?</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>B2 Student project only</strong></td>
<td>What previous experience of research involving human participants relevant to this project does your supervisor have?</td>
</tr>
</tbody>
</table>

**C POTENTIAL RISKS**

<table>
<thead>
<tr>
<th>C1 What potential risks do you foresee?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risks with Questionnaires</strong></td>
</tr>
<tr>
<td>- Participants may feel pressured into choosing an answer even if they don’t have a detailed understanding of the topic.</td>
</tr>
<tr>
<td>- Participants may also be rushed and not answer truthfully when completing the questionnaire.</td>
</tr>
<tr>
<td>- If a person feels shy or threatened by research into security they may try and answer in a way which aims to please the researcher.</td>
</tr>
<tr>
<td>- As the data collected will be anonymous the results are not at risk of compromising a participant’s confidentiality.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C2 How will you deal with the potential risks?</th>
</tr>
</thead>
<tbody>
<tr>
<td>There will be a summary of technical terms within the questionnaire to stop a participant becoming confused and answering by guessing.</td>
</tr>
<tr>
<td>Ensuring participants have the time to complete the questionnaire without feeling rushed will mitigate against untruthful answers.</td>
</tr>
<tr>
<td>The researcher will give a detailed overview of the research and ensure the participant feels comfortable taking part, again, ensuring that answers are truthful. As part of this overview they will be made aware that the data is collected anonymously.</td>
</tr>
</tbody>
</table>
PARTICIPANT INFORMATION SHEET

Evaluation, development & testing of an educational support chatbot

Cardiff Metropolitan University Protocol Number: (if applicable)

Project summary

The purpose of this research project is to research the ethical implications of encrypted messaging services.

Why have you been asked to participate?

You have been asked to participate because the researcher wishes to collect information from students and the public at random.

Project risks

The research involves the completion of a questionnaire. We are not seeking to collect any sensitive or personal data on you; this study is only concerned with your knowledge surrounding messaging services and other information surrounding this technology. We do not think that there are any significant risks associated with this study. However, if you do feel that any of the questions are inappropriate then you can stop at any time. Furthermore, you can change your mind and withdraw from the study at any time – we will completely respect your decision.

How we protect your privacy

All the information you provide will be held in confidence. As the questionnaire is anonymous you are not at risk of being personally identified. Your signature on the consent form will be kept in a secure location by the research team. When we have finished the study and analysed all the information, the documentation used to gather the raw data will be destroyed except your signed consent form which will be held securely for 5 years.

YOU WILL BE OFFERED A COPY OF THIS INFORMATION SHEET TO KEEP

If you require any further information about this project then please contact:

Simon Thorne, Cardiff Metropolitan University

Cardiff Metropolitan University email: SThorne@cardiffmet.ac.uk
PARTICIPANT CONSENT FORM

Cardiff Metropolitan University Ethics Reference Number: 2016D5651
Study ID Number:
Title of Project: The Ethical Implications of Encrypted Messaging Services
Name of Researcher: Mr Alexander John Bowler

Participant to complete this section: Please initial each box.

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. [ ] [ ]

2. I understand that my participation is voluntary, anonymous and that I am free to withdraw at any time, without giving any reason. [ ] [ ]

3. I agree to take part in the above study. [ ] [ ]
   Yes No

_______________________________________  ___________________  
Signature of Participant                      Date

_______________________________________  ___________________
Name of person taking consent                 Date

_______________________________________
Signature of person taking consent