# Encryption: Should we put our privacy before our safety?

By Matthew Clutterbuck

**Research Review**

Squire's article examines the extent to which end-to-end encryption, used by WhatsApp, is effective. She explains, it is not actually the most effective method of securing messages sent through social media. Messages sent are *"most vulnerable- on our own devices"* (Squire 2017) and although end-to-end encryption is important, *"security experts have warned for years that the most vulnerable place for your data is not during transit from place to place, but rather when it's stored or displayed at one end or the other"*[1] (Squire 2017). It is easier to gain access to a device where data is stored rather than to intercept data in transit. Providing they have adequate cyber security knowledge, terrorists could exploit messaging apps, including WhatsApp, to provide them with a secure network to share extremist ideologies.

The documentary 'Crypto Wars: Behind the encryption debate' details the controversy surrounding end-to-end encryption and government involvement. The FBI claim they wanted to gain access to the shooter's device so that they could assess whether the San Bernardino shooters were part of a wider terrorist network. However, technology experts argue that the government are using this as an excuse to implement mass surveillance, whereby they can monitor citizens of America without their consent. The video explains that for years, the only way to send encrypted messages was using PGP (Pretty Good Privacy), however this technology is now outdated and is unsuitable for modern security requirements. Furthermore, the FBI claims that the rise in the use of encryption techniques has led to many cases, where the trail 'goes dark'[2]. The FBI explain that encryption is slowing down cases, using up more government resources, and is resulting in the prosecution of fewer criminals. This demonstrates the vicious circle of crime which cannot be broken without successful prosecutions.

'On ends-to-ends encryption' is a publication produced by academics from Oxford University, explaining the use of end-to-end encryption methods used in WhatsApp function. The document explains *"Sender keys are rotated whenever a participant is removed from a group but otherwise are never changed"*[3] *(Cohn-Gordon 2018),* therefore improving security of a group chat as removed members cannot regain access to the chat using the original sender key. This source is interesting as the data published is the result of years of extensive research, discovered by academics whom are experts in their field.

Additionally, encryption is prevalent throughout terrorist networks, demonstrated in a NBC News article, which discusses a helpdesk IS terrorists have created to enable their members worldwide to evade security. The helpdesk consists of a team of cyber security experts whom give advice on carrying out attacks undetected in the western world. The fact that Islamic State feel a need for this system shows that global governments are, to an extent providing adequate cyber security. This raises an important question: do we want to have a lower level of cyber security but be able to monitor terrorist activity or have a high level of

[1] End-to-end encryption isn't enough security for 'real people'. https://theconversation.com/end-to-end-encryption-isnt-enough-security-for-real-people-82054
[2] Crypto wars: Behind the encryption https://www.youtube.com/watch?v=j7VA4H8m4uk
[3] On Ends-to-ends Encryption https://eprint.iacr.org/2017/666.pdf

security which prevents terrorists communicating through mainstream channels but be unable to monitor their activities?

Furthermore, an article published in the Mirror contains the account of senior government officials in the wake of the London Bridge terror attack. It should be noted that whilst this source mainly focuses on the opinion of those condemning the attack, the opinion of opposing political parties (Labour and the Liberal Democrats) is also presented. We should however consider that their opinions may not be their own and may be representative of their parties' opinion. This would be particularly useful for Jeremy Corbyn, the leader of the Labour party, as he could be seen to be vying for the votes of those people whom would prefer their messages on WhatsApp to remain private using end-to-end encryption, contrary to Conservative opinion.

An article published on 'The Verge' details the actions the UK government have taken to access terrorist communications, simultaneously demonstrating the lack of progress achieved so far. This post is one-sided, as it does not account for successes by the government, instead only detailing their failings to persuade technology firms to provide access to personal messages. In addition, this article offers an insight into the enormity of the problem created by end-to-end encryption, with the source stating, *"Sky News reports that 80 percent of investigations into terrorism and serious crime are affected by encryption."*[4] (Ong 2017). This demonstrates that encryption is a major problem within terrorism investigations and so an appropriate solution must be sought.

Online journal 'Business Insider' reports WhatsApp is fundamental in the fight against terrorism. 16 Belgium terrorists were arrested after messages sent on WhatsApp were intercepted by US authorities and passed on to Belgium authorities. Despite end-to-end encryption measures being implemented, government officials were still able to access messages. These are messages which WhatsApp assures its users are private. Answers are needed as to whether end-to-end encryption really maintains privacy or is it just another 'tick in a box' for Facebook, the owners of WhatsApp. The source continues that *"several of the suspects [were] released due to a lack of evidence"*[5] (Tani 2015), speculating the reason may have been that they might not have *"actually read the WhatsApp messages themselves"* (Tani 2015). Hence, this article shows the problems of a lack of valid evidence sourced from electronic devices, when prosecuting a terrorist case.

In 2016, the UK government introduced the 'Investigatory Powers Bill' containing amendments to the previous act, passed in 2000. This bill states *"obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data"*[6] (Investigatory Powers Bill 2016). This will significantly reduce the privacy of messages sent through WhatsApp and Telegram, also meaning Secretaries of State can access messages through legitimate enforcement of the law. Whilst end-to-end encryption prevents messages from being intercepted from hackers

[4] WhatsApp reportedly refused to build a backdoor for the UK government https://www.theverge.com/2017/9/20/16338128/whatsapp-reportedly-refused-request-uk-government-access-encrypted-messages

[5] WhatsApp chats may have gotten 16 people detained in a terrorism-related investigation http://uk.businessinsider.com/whatsapp-may-have-gotten-16-alleged-terrorists-busted-2015-6?r=US&IR=T

[6] Investigatory Powers Bill https://publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf

during transmission, it does also compromise public security, as it enables terror cells to operate undetected. This act has been published by the UK parliament, hence demonstrating its reliability and accuracy as the act was debated in both the House of Common and House of Lords prior to being passed in 2016.

An article published on '*theregister.co.uk*' explores the implications of the so-called 'Snoopers' charter' on technology firms operating within the UK. The significant concern with this act, is that there is no limit to the information, which the government can access. They are concerned by the morality of the government officials who will be able to access vast amounts of web data, without the need to obtain a warrant.

The Guardian explains sections of the 'Investigatory Powers Act' have been ruled unlawful by UK courts, sighting they are an invasion of privacy. Tom Watson, deputy Labour leader, has led the case, bringing to light the conflicting reasoning behind his opposition to the act, indicating it must therefore be politically motivated. The ruling by the court states that the government must amend the act with immediate effect. The judge overseeing this high-profile case also sighted that the act was "inconsistent with EU law"[7]. The UK is due to leave the EU in March 2019, so this ruling may be reviewed when this occurs. Ben Wallace, the security minister, explains that data collected in line with this act, has led to the successful prosecution of many terrorists and other criminals whom have left digital footprints.

Another article published in the Mirror, investigates the use of encrypted messaging apps by Islamic Extremists. US terror analyst Michael Smith discovered a message posted by a user on Telegram, questioning why police had not shot Darren Osborne (Finsbury Park terror attack suspect) after he committed a terrorist atrocity. The creator of the post believed this was representative of the unfair treatment of Muslims, recalling those involved in the London Bridge attacks were shot dead. Muslim extremists continue to use encrypted messaging apps to convey their radical view of Islam. The Telegram group this message was sent to contained 225 members, most of whom are likely to have read and shared this. This further emphasises the worrying increase in the use of end-to-end encrypted apps, as a tool to promote Islamic Fundamentalism.

The 2015 government departmental spending review produced by the House of Commons outlines the budget of each governmental department for the period 2015-2020. These statistics illustrate that funding for the Single Intelligence Account is set to increase at a rate of £100,000 a year. However, 69% of Governmental departments will see a decrease in their funding levels over this five-year period, showing the governments recognition of the significance of this department. The Single intelligence account is the fund for the Government Communication Headquarters (GCHQ), MI6 and MI5 (the security service). The government allocating a larger budget to this department is indicative of the imminent cyber threat and the funds will be used to increase their online presence to prevent terrorist material being shared.

Another high-profile case hampered by encryption was the San Bernardino terrorism case, 2015. Published in the Guardian three months after the mass shooting, we learn that it took

[7] UK mass digital surveillance regime ruled unlawful https://www.theguardian.com/uk-news/2018/jan/30/uk-mass-digital-surveillance-regime-ruled-unlawful-appeal-ruling-snoopers-charter

nine weeks for the FBI to gain access to Farook's iPhone. The article provides evidence against the use of encryption, as it has created a barrier in a criminal prosecution. Whilst this case occurred in the United States, it is representative of issues faced by the UK government. It is also interesting to note that the government would not reveal the security flaw used to gain access to the device, to Apple. Apple would then have been able to patch this bug to prevent future exploitation.

Furthermore, Bill Gates (co-founder of Microsoft) proposes Apple should comply with the FBI's request and co-operate with their investigation. This comment however is not representative of the stance Microsoft, Google and Facebook have taken, who believe the government should not have access to this data. Consequently, this comment demonstrates that the argument surrounding encryption is not clear cut, as Bill Gates clearly agrees to an extent with both sides of the debate.

However, as published in the human rights act, *'Everyone has the right to respect for his private and family life, his home and his correspondence'*, and continues to say, *'there shall be no interference by a public authority [except] in the interests of national security, public safety, […] for the prevention of disorder or crime'*[8]. Therefore, the government have a moral responsibility to protect their citizens and as such, should have access to electronic devices to retrieve any potential intelligence. This publication outlines the grey area between security and the right to privacy. The organisation has a powerful influence over the criminal justice system and therefore endeavour to appeal a criminal case which does not meet their strict human rights act.

[8] Article 8: Respect for your private and family life https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life

**Abstract**

Encryption is one of the most powerful tools available in this technological era. It is a computational tool which has been designed with the sole purpose of maintaining our privacy and ensuring that third parties are unable to gain access to our messages. This discussion will examine encryption as a positive tool which is used to provide us with adequate privacy, through preventing others from accessing our personal data. The negative uses of encryption will also be explored, including its use as a tool which can facilitate crime, allowing criminals to communicate freely on messaging apps without government knowledge.

The purpose of this discussion is to examine real-life scenarios, primarily criminal prosecution cases, and assess whether encryption methods really have hampered efforts of a successful prosecution, or whether the UK government are using these cases as a reason to grant them unrestricted access to personal data. This approach will then be compared with the approach of the US government, to see whether the problem they face is similar. If this is the true, it will become evident that encryption is a problem and I will explore the alternatives to maintain the balance between privacy and security.

**Introduction**

The question which I will be analysing throughout this dissertation is: 'Encryption: Should we put our privacy before our safety?'. I have chosen this research question as I am currently studying Computer Science at A-Level and I would like to further develop my computing knowledge before I go on to study Computer Science at university. I am personally very interested in the topic of encryption, and it is also a very current topic, given the recent Cambridge Analytica Scandal and introduction of the GDPR (General Data Protection Regulation). In addition to this, encryption has proved to be a barrier in the prosecution cases against both Islamic State and the San Bernardino terror attack in 2015.

The main objective which I have whilst completing this project is to learn more about the methods of encryption companies such as Facebook and Apple are using to keep our data private. I will also assess whether this is morally correct or whether they should give the government access, so that they can protect us against physical threats. Going into this project, I have an open mind and am undecided about which argument I agree with. I hope that upon completion of this project, I will be able to produce a justified opinion on whether end-to-end encryption should be used to secure our messages, or whether it acts as a barrier for security services and hence prevents us from receiving full security offered to us by the government.

This extended project will enable me to evaluate the range of sources which are already available about encryption. I will then draw a conclusion to determine whether the UK government and other global organisations are doing enough to prevent illicit activity from occurring across internet connected devices.

The primary resource I will use for this dissertation is the internet, from which I will gather a variety sources which contain explanations about the way in which encryption works and news articles detailing recent terror events, including events where technology was considered to be a facilitator. It is important to note that whilst the internet contains lots of reliable information, it also contains vast amounts of inaccurate data. I will therefore ensure that data which I do collect is supported by other sources. Additionally, I will use my computer science textbooks which give in-depth information about the uses of encryption, the history of these methods and the laws which have been introduced to protect civilians.

The main areas my research will span include the use of end-to-end encryption in messaging apps, which provides a high level of privacy for all messages, thus preventing the government access. This could lead to a serious crime going undetected. Additionally, I will examine the levels of funding which are received by UK government departments, to discuss whether money is a factor in the level of security which we receive. I will also examine the introduction of the Investigatory Powers Bill (2016) and the General Data Protection Regulation (2018), as the government attempt to reduce the freedom which global corporations and individuals have whilst using personal data and the internet, so that they can prevent criminal activity from occurring before it becomes a larger threat. Additionally, throughout this discussion, I will refer to the Human Rights Act. This outlines the boundaries to which the government can be involved in our personal lives. This dissertation is more of an ethical argument than it is factual, and as such lends itself excellently to a discussion.

This project will primarily focus on the use of end-to-end encryption, a form of encryption for messages, which *"ensures only you and the person you're communicating with can read what's sent, and nobody in between"*[9] (WhatsApp, 2018). In addition to this, *"every message you send has an unique lock and key"*[10] (WhatsApp, 2018) which adds an additional layer of security to each message which is sent, so that if the device fell into the wrong hands, they would not be able to decrypt and read any of the messages which you have sent or received. However, as stated above, no-one, not even WhatsApp can view the content of these messages, and so this has created a large problem for the UK government, who monitor the activity of their citizens for security reasons.

Additionally, I will also examine some of the key events which have sparked much controversy over the use of encryption technologies across social media applications. The main events which this discussion will cover include the 2015 San Bernardino terror attack, the 2017 Westminster Bridge attack and the 2017 Finsbury Park Mosque attack. These are all events which have caused much governmental discussion, to determine whether current cyber security measures are justified.

[9] WhatsApp FAQ- End-to-end encryption https://faq.whatsapp.com/en/android/28030015/
[10] WhatsApp FAQ- End-to-end encryption https://faq.whatsapp.com/en/android/28030015/

**Discussion**

Encryption has long been one of the most controversial topics in the study of computing and security. The use of encryption has grown exponentially since Julius Caesar first introduced the secure messaging method in 100 B.C., the Caesar Cipher, to hide secret messages; today encryption is prevalent throughout messaging applications to ensure that third parties cannot intercept our messages. Cohn-Gordon (2018), an academic at the University of Oxford, further explains the flaws in the use of modern encryption technology in his publication, stating, *"Sender keys are only rotated when a participant is removed from a group, but otherwise are never changed"*[11]. This therefore demonstrates that security could be compromised if the sender key were to be intercepted. This type of encryption is known as end-to-end encryption and is widely used in messaging applications such as WhatsApp.

To an extent, end-to-end encryption provides adequate security for electronic messages as government organisations in both Europe and America are unable to access any messages that are sent through these applications. This therefore demonstrates the effectiveness and impenetrability of end-to-end encryption. This effectiveness is also evident in many high-profile cases, including the San Bernardino terror atrocity (2015) and the London Bridge terror attack (2017). Both criminal cases were severely hampered by a lack of evidence, which could not be accessed due to security restrictions imposed on the attackers' mobile devices. In addition, both events remained undetected by law enforcement officers prior to the events occurring, even though they both communicated with other individuals through social media applications, discussing their ideologies and plans.

In an interview on the Andrew Marr show in March 2017, the then Home Secretary Amber Rudd demanded more should be done to prevent terrorists from being able to freely communicate with each other through the internet. The problem, she had with the encryption methods tech companies were using, is that they prevent government security officials from monitoring communications, and as such, atrocities such as the Westminster Bridge Attack went undetected by law enforcement.

Furthermore, in the wake of this car attack, Rudd felt that it was time to severely clamp down on terrorists, and that technology companies should no longer be able to offer their users an environment where they can message each other freely. She called for an environment where the government could effectively 'snoop' on people without their knowledge or consent. It seemed however, that technology companies such as Facebook were not willing to share data on their customers with the UK government, and so the government had to find a way to get around this. To overcome this issue, the UK government introduced the Investigatory Powers Bill on the 29th of November 2016.

The Investigatory Powers Bill (2016) contains amendments to the previous bill, which passed in 2000. This update enables government officials and security experts to demand social media companies give them access to any data that they want, upon official request. This is different from the previous standing where the government could only hope that the company would reply to their request. The act is problematic however as there are no regulations to justify the reasoning for accessing personal data, and as such I feel that this

[11] On Ends-to-ends Encryption https://eprint.iacr.org/2017/666.pdf

power could be open to exploitation from senior government officials. Whilst I feel it is important that the government should be able to monitor the activities of anyone whom they suspect of committing terrorist activity, I also believe there should be a need for a clearer justification when accessing the data.

Owing to the large ethical concerns over the introduction of this act, it was inevitable that a case would be bought upon the UK government to challenge the amendment act. At the end of 2017, the Investigatory Powers Act was ruled unlawful in part, meaning the government must amend sections of the Act with immediate effect. Consequently, they had to install tighter restrictions surrounding the approval required by senior police officials to access personal data and communications, meaning that these officers could no longer access materials without requesting permission. Whilst these improvements were met with a positive response, many high-profile campaigners, including Labour's Tom Watson were not wholly satisfied with the government's response.

Whilst the critical response to this act, led by Tom Watson, is perfectly valid in demanding greater privacy for UK citizens from the so-called 'Snooper's Charter', it is simply impractical to allow everyone to have free, unrestricted access to the internet without government monitoring. Monitoring of communications by US officials lead to the arrest of 16 Belgium terrorists, who were sharing extremist propaganda, highlighting the use of messaging applications such as WhatsApp by terrorists. Communications monitoring, therefore prevented these terrorists, who may have potentially gone on to commit terrorist attacks which could have resulted in many innocent lives being lost. Whilst it should be noted that this case did not directly involve UK citizens, there have been many arrests linked to the sharing of extremist propaganda in the UK. However, if the proposals made by Tom Watson, were to exist, the security services may not have intercepted these messages. This would mean that terrorists would be able to operate freely and as such, could lead to a sharp rise in the amount of terrorist activity in the UK.

It is evident though, that despite there being a call for a decrease in the amount of government monitoring, there is still an even greater need for government monitoring to protect UK citizens and to prevent terrorist activities and serious crime from being committed. In the weeks following the Finsbury Park van attack, Michael Smith, a US terror analyst discovered a message in a large group on messaging app 'Telegram', promoting terrorist activities. Muslim extremists from across the world agreed with the message which questioned why the van attacker at Finsbury Park had not been shot dead, unlike the terrorists in the London Bridge attack. They were spreading widespread hate views against those who they felt were treating Muslims unfairly and promoting their fellow terrorists to carry out attacks against the Western Allies. Most of the 225 members in this terror cell had read this message, and there is the possibility that these ideologies had been further spread to other radicalised individuals in other social media groups. This again demonstrates the use of social media applications by extremists to promote their twisted view of Islam, without the need to travel long distances to spread hatred.

Whilst rapid developments in computing technology since 2001 have made it easier for terrorists to communicate, tighter security restrictions have made it harder for them to remain undetected on the internet. It has however been reported that to combat these

difficulties, Islamic State created a 'helpdesk'. This consists of a small number of radicalised technology experts who advise their members on methods to avoid government detection and commit terrorist attacks in their own countries. The use of end-to-end encryption and site monitoring has meant that it is now more difficult for extremists to operate undetected. This raises the important question: surely if increases in screening technology at airports have prevented terrorists from attempting to bring down aeroplanes in the sky, measures can be put in place on the internet to deter extremists from even attempting to communicate with each other?

Pretty Good Privacy (PGP) had long been the best method of securing messages using symmetric encryption, which involved using a public key to encrypt data and a private key to decrypt data. The receiver must have a copy of the private key to able to access the data. This method of privacy was initially released in the early 1990's, marking the introduction of modern encryption technologies. This encryption technology was not exploited for criminal activities when it was first introduced. Therefore, it did not cause a problem for the government, however globalisation and increases in the use of technology has meant that criminals are now smarter and are able to use technology as an aid to crime, to enable them to operate almost completely undetected. It is therefore appropriate that as secure technology changes, the security measures surrounding these should also adapt.

Improvements in cyber security measures in large part, are down to the increase in the budget available to police officers and security services, meaning they can recruit more staff and install equipment to monitor criminal activity. The 2015 government departmental spending review released by the House of Commons shows the Single Intelligence Account's budget (GCHQ, MI5 and MI6) is increasing at a significant rate of approximately £100,000 each year over the next three years. This is different to a large proportion of other government departments, with nearly 70% these facing a decrease in the amount of funding which they will receive in the period 2015 to 2020. Several large departments who will see a decrease in funding include Education, Home Office, Local Governments and Justice. Given that the budget for this department is set to increase shows the importance of cyber security, which is hardly surprising given the sharp increase in cyber terrorism.

Introduced on the 25th May 2018, the 'General Data Protection Regulation (GDPR)' was implemented by the UK government in collaboration with other European governments. Facilitated by the increase in funds available in the Single Intelligence Account, this act aims to increase user awareness of how their data is being used and encourages greater transparency between the customer and business. The introduction of this act illustrates a better understanding of Human Rights which are available to us, as consumers have the right to be told what information is held about them. The business must disclose this information when requested by the customer.

Also, in 2018, an updated 'Data Protection Act' was published, replacing the existing 1998 Act which had not been updated in 20 years, with an aim of keeping up with modern technology standards. This act explains that organisations who hold personal data must keep it up to date and secure. To keep personal data secure, organisations must either encrypt the data or apply a hash function to it. Encryption works by applying either a private or public key to encrypt data and then another key to decrypt the data, meaning only those

with the correct key will be able to decipher the data. If data is hashed however, it has undergone a one-way function, meaning that the data cannot be deciphered without matching the plaintext by hashing the new data and comparing them to see if they match. The use of these two methods demonstrate the strong data security which is provided by encryption, and thus shows the importance of encryption methods when storing personal data, to prevent identity fraud or false impersonation.

However, as explained in a blog article published on 'theregister.co.uk', many people are not concerned with the government's desire to implement new security measures but are concerned at the extent to which the 'Investigatory Powers Act' will grant senior police officers and security service personnel access to any information about anyone at any time. However, I believe it is hard to see how this is a problem for most people, as if you have nothing to hide, then the government will not be interested in any data which you share? For most people however, I believe it is merely the fact that they disagree with this act providing the UK government with even more power than it already has. This could then lead to greater restrictions on other aspects of daily life such as freedom of speech and right to will.

The high-profile San Bernardino terror case was severely delayed due to a lack of evidence available to prosecutors, caused by restrictions on the shooter's Apple iPhone. This prevented law enforcement officers from accessing the killer's device. Again, encryption methods are preventing justice from being served, with the FBI announcing that the increase in the number of encryption methods has led to an increase in the number of cases which have gone 'dark'. Whilst it is important for Apple to have excellent security measures to prevent hackers from gaining access to their users' devices, I believe that they should have granted the US government access to the device when requested, as it was necessary for all evidence to be disclosed and so that justice could be fully served.

Further controversy in this case erupted when Bill Gates, co-founder of Microsoft, suggested Apple should work with the US government to retrieve data from the iPhone. It is interesting that Gates suggested this idea as he has previously voiced an opinion against government involvement and the interception of communications. Hence, it can be deduced that this argument is not clear-cut, as individuals who have previously expressed one opinion are now expressing the opposing opinion. This shows that current methods of encryption are doing an acceptable job of protecting us, however there is still more that could be done by large corporations to make encryption a more effective method of security.

In addition to this, the Human Rights Act states that a government has a responsibility to protect its citizens, through any means necessary. Therefore, it could be argued that governments should have access to any data required, including personal data from mobile devices, so that they can ensure the safety and security of their citizens. This is in line with the opinion of many senior government officials who believe that the government should have a right to access any personal data which is sent through a mobile device. This does however contradict the opinion of Labour's Tom Watson who believes citizens should have access to privacy and does not agree with the amendments to the Investigatory Powers Bill 2016. This raises the interesting point that even members of the UK government have a

differing opinion to that which is laid out in the Human Rights Act, which is the basis for many decisions which are made by the government.

Encryption is prevalent all around us; all data sent across the internet is encrypted for security, and methods of encryption are improving all the time. Encryption has become such an important aspect of cyber security that the UK government have begun several schemes whereby they wish to attract more young people to pursue a career in the cyber security industry. They see this as being one of the largest industries which will grow within the next decade. The threat from cyber-crime has increased dramatically in recent years, which has led to the introduction of dedicated cyber police teams in each police force across the UK. In the period March 2015-2016, there were a total of 2006 cyber-crime across England and Wales, which included computer misuse, spreading viruses and hacking. In the following period of March 2016-2017, there were 3591 incidents of this type, an increase of 1585 in one year. This exponential increase demonstrates the greater demand which is now required of the security service, to deal with a new type of threat which developed rapidly over the last 15 years.

As it is today, the UK government already have a difficult challenge when accessing private messages that have been encrypted, however large technology firms are always finding new ways to secure messages which are sent across their services. The introduction of these new privacy methods comes with an even greater challenge for the UK government than already exists. This challenge will require more employees, more computing power and more knowledge. Therefore, the cost of running the UK security service will increase and so there will be a greater demand for money in the Single Intelligence Account. This in turn will bring an even greater challenge for the government whom are already struggling to provide each department with the funding which is required and therefore, the UK government looks set for a challenging future.

## Conclusion

Overall, there are both benefits and drawbacks for the use of encryption technology. The positive uses are primarily for personal privacy and to prevent third parties from intercepting our messages or important data such as bank details or passwords. There are also drawbacks of this technology; the main reason being that the technology is so good it cannot be broken, meaning the government are unable to intercept and decipher any of the messages which are sent across end-to-end encrypted networks. This is a problem as many terrorist organisations and criminal gangs are aware of this and exploit the technology to remain undetected by law enforcement. This is therefore ironic as whilst encryption was implemented to make the internet safer, it has in turn made it easier for crime to be facilitated and hence makes the world a more dangerous place.

I was particularly surprised to discover the wide number of instances where encryption prevented justice from being fully served as there was a lack of evidence to make a successful prosecution. Whilst these cases were predominantly high-profile, I am sure there are many other smaller cases where evidence is not fully disclosed as police officers cannot gain access to an assailant's mobile device. This is a big problem when messages are stored using end-to-end encryption as the messages can only be accessed from the device, as they are not stored elsewhere. This makes it even more important that law enforcement officers can gain access to the device.

Based upon this, I believe that encryption is a necessary tool to prevent the disclosure of sensitive information, but I also believe there is a long way to go until the balance between privacy and security is appropriate. Whilst I feel that we have the right to not have our messages read by a third party, I do believe that the government should be able to monitor messages sent through social media networks to monitor extremism and prevent serious crime from being committed. In addition, it is unlikely that your messages will be flagged and monitored if you haven't done anything wrong. This would therefore mean most people would be unaffected by any new acts which were implemented.

I have thoroughly enjoyed working through my extended project as it has enabled me to develop my analytical skills, through my detailed analysis of the many sources which I used throughout this dissertation. This has been particularly useful as it has enabled me to improve my test scores in computer science on extended response questions where there are more marks available for the analysis of a problem. Similarly, there were some challenges which I faced during this project, the main one being inserting references for each quote which I use, as this is a skill which I have not used before. However, after completing some research on referencing methods, I was successfully able to record every source I used. This new skill will be particularly useful for me when writing dissertations at university.

**Bibliography**

**Websites**

EU GDPR Portal. 2018. EU GDPR Information Portal. [online] Available at: https://www.eugdpr.org/ [Accessed 10 May 2018]

HM Government. 2018. Cyber Discovery. Joincyberdiscovery.com [online] Available at: https://joincyberdiscovery.com/ [Accessed 18 May 2018]

McCarthy, K. 2016. UK's new Snoopers' Charter just passed an encryption backdoor law by the backdoor. The Register [online] 30 November 2016. Available at: https://www.theregister.co.uk/2016/11/30/investigatory_powers_act_backdoors/ [Accessed 2 November 2017]

Meyer, J. 2015. ISIS had help desk for terrorists staffed around the clock. NBC News [online] 16 November 2015. Available at: https://www.nbcnews.com/storyline/paris-terror-attacks/isis-has-help-desk-terrorists-staffed-around-clock-n464391 [Accessed 12 October 2017]

Ong, T. 2017. WhatsApp reportedly refused to build a backdoor for the UK government. The Verge [online] 20 September 2017. Available at: https://www.theverge.com/2017/9/20/16338128/whatsapp-reportedly-refused-request-uk-government-access-encrypted-messages [Accessed 12 October 2017]

Tani, M. 2015. WhatsApp chats may have gotten 16 people detained in a terrorism-related investigation. Business Insider UK [online] 8 June 2015. Available at: http://uk.businessinsider.com/whatsapp-may-have-gotten-16-alleged-terrorists-busted-2015-6?r=US&IR=T [Accessed 2 November 2017]

WhatsApp. 2018. WhatsApp FAQ- End-to-end encryption. whatsapp.com [online] Available at: https://faq.whatsapp.com/en/android/28030015/ [Accessed 4 May 2018]

**Newspaper Articles**

Blanchard, J. 2017. Government eyes new laws for clampdown on encryption of WhatsApp messages in wake of London terror attack. Mirror [online] 27 March 2017. Available at: http://www.mirror.co.uk/news/politics/government-eyes-new-laws-clampdown-10105142 [Accessed 2 November 2017]

Bullen, J. 2017. Twisted WhatsApp message shows ISIS fanatics using Finsbury Park terror attack to urge further atrocities against the West. Mirror [online] 20 June 2017. Available at: https://www.mirror.co.uk/news/world-news/twisted-whatsapp-message-shows-isis-10650579 [Accessed 2 November 2017]

Hern, A. 2016. Bill Gates backs FBI in battle with Apple over San Bernardino killer's phone. The Guardian [online] 23 February 2016. Available at:

https://www.theguardian.com/technology/2016/feb/23/bill-gates-fbi-apple-san-bernardino-killer-phone [Accessed 14 December 2017]

Travis, A. 2018. UK mass digital surveillance regime ruled unlawful. The Guardian [online] 30 January 2018. Available at: https://www.theguardian.com/uk-news/2018/jan/30/uk-mass-digital-surveillance-regime-ruled-unlawful-appeal-ruling-snoopers-charter [Accessed 23 February 2018]

Yadron, D. 2016. San Bernardino iPhone: US ends Apple case after accessing data without assistance. The Guardian [online] 29 March 2016. Available at: https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone [Accessed 8 December 2017]

**Books**

Cohn-Gordon, K and others. 2018. On Ends-to-ends Encryption. [online] 18 January 2018. Available at: https://eprint.iacr.org/2017/666.pdf [Accessed 8 February 2018]

Naeem Akram, R. 2014. End-to-end Secure and Privacy Preserving Mobile Chat Application. [online] 1 June 2014. Available at: https://pure.royalholloway.ac.uk/portal/files/23295486/Paper.pdf [Accessed 2 November 2017]

**Blogs**

Squire, M. 2017. End-to-end encryption isn't enough security for 'real people'. theconversation.com [online] 14 August 2017. Available at: https://theconversation.com/end-to-end-encryption-isnt-enough-security-for-real-people-82054 [Accessed 8 February 2018]

**Videos**

2016. Crypto wars: Behind the encryption debate | Fault Lines. youtube.com [online] 25 October 2016. Available at: https://www.youtube.com/watch?v=j7VA4H8m4uk [Accessed 8 February 2018]

**Corporate Publications**

Equality and Human Rights Commission. 2016. Article 8: Respect for your private and family life. Equalityhumanrights.com [online] 4 May 2016. Available at: https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life [Accessed 8 December 2017]

House of Commons Library Statistics. 2015. UK Spending Review 2015: Departmental Budgets. public.tableau.com [online] 26 November 2015. Available at: https://public.tableau.com/profile/house.of.commons.library.statistics#!/vizhome/SpendingReview2015/TotalDEL [Accessed 10 November 2017]

Office for National Statistics. 2018. Crime in England and Wales: Additional tables on fraud and cybercrime. ons.gov.uk [online] 19 July 2018 Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables [Accessed 19 July 2018]

Parliament Publications. 2016. Investigatory Powers Bill. publications.parliament.uk [online] 29 November 2016. Available at: https://publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf [Accessed 10 November 2017]