A call for the prohibition of encryption; panacea or problem?

Graeme Horsman

School of Science, Engineering & Design,
Teesside University,
Middlesbrough,
North Yorkshire,
United Kingdom

Email: g.horsman@tees.ac.uk
Phone: 01642 738130

Abstract
Sadly, acts of terrorism are now more frequent worldwide. Following events in Europe and the United States, western civilisation is now facing the challenge of policing an evolved form of terror-attack, one which is suspected of being underpinned with communication and organisation across networked individuals online. It is suggested that such planning is taking place via covert, encrypted channels, beyond powers of interception by law enforcement. As a result, encryption usage is currently one of the most debated topics globally. In light of the attacks witnessed in Manchester and London in the United Kingdom during May and June of 2017, the UK Prime Minister Theresa May offered a renewed call to arms, seeking the prohibition of so called 'unbreakable' encrypted communication channels. This article provides a timely review of the challenges encryption provides in 2017 whilst considering the feasibility and issues surrounding its removal.

Keywords: Encryption; Communication; Internet; Terrorism; Crime; Criminal; Regulation

1 Introduction

To commence discussions, a chronological depiction of reported notable comments is offered regarding the use of encryption:-

> **Edward Snowden, June 2013:**- "*I don't want to live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity or love or friendship is recorded*".

> **Former FBI Director James Comey, October 2014:-** *"If the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place"*

> **Former Prime Minister David Cameron, January 2015**:- "*Do we want to allow a means of communication between two people which even in extemis with a signed warrant from the home secretary personally that we cannot read? ... My answer to that question is no, we must not. The first duty of any government is to keep our country and our people safe*".

Apple CEO Tim Cook, February 2016:- "*For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business*".

President Donald Trump, February 2016:- "*To think that Apple won't allow us to get into her cellphone? Who do they think they are?*"

Google CEO Sundar Pichai Backs, February, 2016:- "*Forcing companies to enable hacking could compromise users' privacy*".

Facebook CEO Mark Zuckerberg, February 2016:- "*We believe in encryption*".

Former US President Barack Obama, March 2016:- "*The question we now have to ask technologically is if it is possible to make an impenetrable device or system where the encryption is so strong that there is no key, how do we solve or disrupt a terrorist plot? ...There has to be some concession to the need to be able to get into that information somehow".*

Former Director of National Intelligence, James R. Clapper, April 2016:- "*As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years*".

US Attorney General Jefferson Beauregard Sessions III, January 2017: "*Encryption serves many valuable and important purposes……It is also critical, however, that national security and criminal investigators be able to overcome encryption, under lawful authority, when necessary to the furtherance of national security and criminal investigations*".

Home Secretary Amber Rudd, March 2017:- "*We need to make sure that organisations like WhatsApp, and there are plenty of others like that, don't provide a secret place for terrorists to communicate with each other*".

Prime Minister Theresa May, June 2017:- "*We cannot allow this ideology the safe space it needs to breed….Yet that is precisely what the internet and the big companies that provide internet-based services provide*".

Encryption has long been an area which evokes significant and often controversial debate, particularly with its suspected use during the planning and enacting of recent terrorist atrocities. Whilst 'unbreakable' encryption may frequently be used as a descriptor in news reports, further examination of this term is initially required to provide some clarity. Unbreakable infers a complete inability to decrypt content implying the use of information-theoretic security, yet such cryptographic schemes are not implemented in scenarios referred to by the media. Most existing encryption systems can be cracked given the time, resources, correct context or via the revelation or guessing of a key, allowing

subsequent encrypted content to be decrypted. Therefore instead, robust encryption may be argued as a preferable term where strong underpinning algorithms coupled with an effective implementation within a given context can prevent decryption and the surveillance of content using current investigative techniques. This is effectively the issue faced when references to encrypted communications via services such as Whatsapp are made.

Commencing with Charlie Hebdo in January 2015, 20 major terrorist incidents in Europe and North America have been reported resulting in the death of over 350 individuals[1]. In the aftermath of many of these events, attention has been drawn to the protection afforded by encrypted communication channels and their potential use **to plan and** coordinate terrorist events beyond the knowledge and regulation of law enforcement[2]. Few technologies have the power to impact society as significantly as that of encryption. Its use can be both positive and negative (as with any technology) where an evaluation of its deployment is often determined by assessing the underpinning motivations of those who implement it. World War II provides an informative example, with the well-documented challenges posed by cryptographic communications and the very act of breaking such encryption algorithms widely reported to have potentially shortened its length, saving countless lives[3]. Now in 2017, encryption has seamlessly encroached upon almost all aspects of society's digital lives resulting in many advantageous deployments, **with emerging areas such as Internet of Things devices posing additional practical and regulatory challenges**. Often unbeknownst to the non-technical user, and arguably taken for granted with regards to the safety it offers, it now protects a variety of online transactions. Its legitimate usage for safeguarding data provides the glue from which interconnected computing networks are now held together, allowing the safe transit of data between parties, protecting the individual. Arguably, its removal (albeit arguably impossible) would in itself likely cripple the Internet given the reliance on it from society and the inevitable widespread exploitation for criminal purposes which would ensue.

Despite its existence for hundreds of years, we are only now witnessing such severe condemnation of encryptions usage. Sustained criticism from government officials has often targeted encrypted communication channels, notably those of Whatsapp, Signal and Telegram (collectively reported to attract over 1 billion monthly users[4]) in conjunction with their inability to effectively examine and scrutinise this traffic. Encryption continues to polarize opinions surrounding its implementation as in an information-rich society, a protocol which permits content to be 'unintelligible' to everyone except those permitted to be involved in a transaction, carries with it an element of fear for those excluded. This scenario is currently being experienced by governments worldwide, where an unease is felt with regards to what actions are occurring beyond existing powers of surveillance and associated repercussions. Yet conversely, the very thought of mass surveillance invokes thoughts of George Orwell's '1984', simultaneously creating public unease.

This article provides an analysis of both sides of the debate surrounding the regulation of encryption, in light of sustained calls for the imposition of restrictions on the use of encryption with online communication platforms. To provide structure, discussions are divided into three areas, those of pro-encryption, anti-encryption and feasibility

considerations. Finally conclusions are drawn. The article will not stray into moral and legal debates, focusing on technological and regulatory issues stemming from these.

2 Pro-Encryption

To provide focus, discussions will remain on encryption of data transferred across a network/platform; coined in this article as 'transaction data'. To commence analysis, arguments in support of the sustained usage of encryption are provided. This stance has been offered by a number of influential organisations (see recent comments noted above from Apple, Google and Facebook), along with anti-surveillance activist Edward Snowden. The following pro-encryption moot-points are submitted:-

Privacy:- Arguably privacy is one of the main purposes of encryptions design and forms the founding argument for its sustained usage. Whether that be to prevent military and trade secret information, documented in the first usage of ciphertext in early Greek civilisations, or for the protection of financially or personally sensitive transaction content[2]. Privacy lies at the crux of justifications behind encryption, and arguably is the very thing which is under threat of erosion due to calls for its removal. A legal right to privacy provides significant difficulty with regards to determining to what extent privacy should be maintained, in what context, and how to ensure it is not compromised whilst protecting all involved. As a result, geographically, jurisdictional stances may differ (see for example the United Kingdom's Investigatory Powers Act 2016's data retention regulations and the Regulation of Investigatory Powers Act 2000 and its powers of surveillance and disclosure, contrast with the United States' Electronic Communications Privacy Act (18 U.S.C. §2510)). Encryption allows an individual to control their own dissemination of data to a greater extent whilst also protecting their own assets, regardless of overarching regulations. Essentially encryption offers an individual privacy and protection, regardless of overarching political regimes and motives, something which Madden and Rainie's[16] survey into Americans' perceptions of privacy indicates as important, with '93% of adult respondents stating that being in control of who can get information about them is important' and 10% having implemented encryption to enhance privacy. In addition, it removes reliance on third parties and services to protect and ethically utilize their data (where in light of recent reported breaches with organisations such as Verizon and Equifax, public confidence may be low, a consensus similarly noted in Madden and Rainie's[16] survey) as it often places it beyond their powers of control. The Tor Project[5] currently provides a prominent example of a privacy enhancing technology protecting individuals online via encryption processes, with organisations such as Google utilising HTTPS to protect email usage and online searching.

Despite the fact that 'privacy enhances protection', a phrase potentially invoking sinister undertones, consideration must also be given to the need to invoke privacy for everyday 'harmless' acts. For example, a conversation between individuals who simply do not wish to have the content publicly available or arguments of legitimate pornography usage. Were such data to become publically available, embarrassment to parties may ensue but no legal ramifications (to the individual) are at stake, i.e. communications were personal as opposed to criminal. Many of the Internet's users pursue innocent yet potentially controversial (to some) actions online (see discussion below regarding free movement and speech). A leaked communication of this type may in itself be harmful due to the level of embarrassment or

apprehension suffered due to the knowledge that such communications are publically available, potentially resulting in psychological harm. The question remains as to whether such actions have a right to be privatised and whether the privacy afforded by encryption actually stands to protect the physical health of an individual, where its removal increases their vulnerability. In cases where encryption is removed and data is subsequently compromised, determining who would be liable for any damage resulting from such a breach poses an issue for debate.

Promotes freedom of speech and movement online:- Perhaps a controversial sentiment, but the removal of encryption may limit the ability to move freely online which may stunt societal development. Privacy promotes autonomy[6], and in absence of, individuals become vulnerable to over regulation and behavioural control. The protection afforded from encryption offering anonymity may prevent individuals from exploring ideas which are not popular, but need to be explored for the health or wellbeing of a country or set of individuals, and to further knowledge without experience of prejudice. In absence of encryption, a shadow over the right to freedom of speech is arguably cast, knowing that surveillance of content is a possibility and potential regulatory repercussions may result. Lets not forget, a right to discuss all topics exists, free of discrimination, regardless of how controversial within the limits of existing laws. In doing so, societal benefits include increased knowledge, education and awareness. Organisations such as the Electronic Frontier Foundation champion encryption usage for the protection it can afford an individual, particularly for the benefit of free expression and knowledge access and gathering. Removal of encryption arguably limits such debate due to fears of discrimination.

Crime & information security:- It is now acknowledged globally that acts of cyber-crime are widespread, causing significant regulatory problems[7]. Arguably, the removal of encryption would seek to exacerbate this issue. Whilst it may reveal content-based offences (hate crime etc.) or evidence of those involved in criminal acts, in removing the protection provided by encryption individuals are left potentially exposed to those seeking to intercept and abuse their personal information. Although no protocol provides complete security, configurations can be set to ensure the decryption of encrypted content is impractical where time-to-crack periods are too great, leaving the use of any decrypted content redundant. It remains easy to focus on the impact on an individual, particularly given the sentiment of recent governmental calls. Yet, prohibiting secure communication is likely to also stunt commercial growth due to a lack of reliable methods of transferring data without risk (for example, financial transactions). Organisations must offer a reliable and safe service in order to attract, sustain and grow a customer-base. Communication with customers must be secure, with reliance placed on encrypted channels, where removing this option directly contrevenants existing information security standards. The removal of encryption would also place a greater burden on commercial organisations to protect customer information, a task which would normally utilise encryption protocols. As a result, its removal would likely see data transferred across a network unprotected, arguably at its most vulnerable point, permitting surveillance and potential malicious interception, before being locally stored by an organisation at an endpoint. Such security models are unfavourable to both the commercial organisation and its users. The removal of encryption for data in transit would arguably inevitably lead to an

increase in the volume of cybercrime, with potentially significant financial implications and concerns for almost all parties involved in any form of asset or monetary exchange.

Destabilization of data protection:- Encryption is a well established principle, embedded into many current technological systems and data transfer methods and protocols in existence (for example, HTTPS). Its removal would seek to cause significant disruption, undermining the existence of functionality of many current services, potentially affecting the financial stability of organisations and countries. Many systems are designed around encryption standards and would cease to exist or function satisfactorily in their absence. Any government decision enforcing the decryption of encrypted content would create a ripple-effect, destabilising current systems and structures, whilst also creating a grey area of liability stemming from breaches involving unencrypted data. Legal uncertainty would ensue, where existing legislation for the purpose of data protection would be arguably undermined (see for example discussions surrounding the General Data Protection Regulation in Europe). Further, if encryption usage was to be banned within specific geographical regions, their engagement with other non-encryption regulated jurisdictions would likely be reduced or cease, with significant commercial impact.

3 Anti-Encryption

Political figures including the United Kingdom's Prime Minister Theresa May have called for the removal of encryption which is used with popular communication platforms. Such acts would potentially allow for the mass surveillance of communication data where it is perceived by law enforcement that interception of terrorist plotting and criminal activity would be possible, subsequently increasing public safety. The following anti-encryption arguments are offered:-

Surveillance, control and prohibiting terrorist communication:- The current primary argument stemming from those seeking to withdraw or restrict the use encryption **stems** from its suspected use in the communication and organisation of acts of terrorism and serious crime. Effective encryption standards and their implementation in many communication platforms can prohibit the regulation of data transferred across a network. As a result, government officials are fearful that encryption is screening the actions of those involved in terrorism, allowing the planning and implementation of these acts. Concerns are also extended to an inability to intervene where such acts are occurring, allowing ideologies free to grow, facilitating radicalisation. In theory, the regulation of encryption stands to afford public protection, potentially facilitating the interception of communications of those currently on a course to plan and commit acts of terror. Arguments are forwarded that an ethical government should be able to eavesdrop to protect health and safety of both a country and its citizens, providing that such information is used in a suitable manner and where applicable data protection measures are implemented, with investigatory measures both transparent and accountable. Such theories link to the concept '*if you have done nothing wrong, you should have nothing to hide*', although in reality, this notion is an oversimplification, raising complex ethical concerns.

A barrier to justice:- The application of justice requires the need for both sufficient facts surrounding the suspected criminal act coupled with the ability to identify those accountable.

Encryption can prevent both. Whilst supporting anonymity, it can (and most likely has already) facilitate the commission of criminal acts beyond the detection of law enforcement[6]. Encryption may not just prevent the delivery of justice, it may also prevent a criminal act from being detected in the first instance. In allowing surveillance, encryptions removal increases both transparency online and potential accountability for one's actions. Further, the absence of encryption may in itself act as a deterrent to those who have abused or intend to abuse this technology, due to fear of being caught. In addition, where content remains encrypted, cooperation may be needed by a specific technology vendor in order to potentially seek access to it (if it is possible - see discussion in sections 4). In absence of their assistance, criminal investigations may stall, creating a potential barrier to justice; see the recent difficulties encountered by law enforcement when liaising with Amazon over stored Echo data during a murder investigation[8].

Regulatory Costs:- Coupled with a barrier to justice, encryption increases regulatory costs. For example, where a suspect has been identified, decrypting content maintains a price in terms of time and resources. One notable instance is that of former Lostprophets singer Ian Watkins, where specialist expertise was required from the Government Communications Headquarters (GCHQ) to gain access to a laptop device[9]. Although this instance surrounds localised encryption methods, it provides an informative example, where the costs associated to the use of such services is arguably neither sustainable or feasible for use on mass. As a result, the removal of encryption may decrease targeted investigation costs and complexity.

4 Feasibility considerations

It is key to note that up to now, this article has arbitrarily treat the debate surrounding the regulation of encryption as binary. In reality, this is an oversimplification of the challenges, where encryption usage cannot be simply turned on and off. Encryption is embedded deep into society's technology and functionality, requiring strategic evaluation of its impact with the feasibility of encryption regulation providing a third categorisation of considerations.

You cannot just 'un-invent' encryption:- Like it or not, encryption is here to stay, regardless of the words of politicians and those in support of its removal or regulation. It is simply not possible to 'un-invent the wheel', not forgetting that encryption has existed (albeit in varying degrees of complexity) for hundreds of years. Removal of its presence from modern day technology is likely to at best stunt the use of it from within certain platforms, triggering the development of others. A go-to example in many instances is 'Tor' and its browsing protocols facilitating online anonymity and those migrating to it following the declarations made by Edward Snowden in 2013 regarding governmental mass surveillance programs. This platform has now existed for over 15 years, successfully protecting online transactions. Whilst offering law enforcement the chance to 'window-shop', and passively observe illicit activity[6], often they remain powerless to act. Encryption is not a tangible object which can be restricted or removed from consumption. It is simply knowledge of the application of mathematical principles applied to data, providing interchangeable states of intelligible data and ciphertext. Encryption algorithms can be designed (albeit it with varying degrees of complexity) by anyone, meaning that where regulation or restriction is placed upon a specific platform, it is only a matter of time before another is developed and adopted.

Blanket or Targeted?:- To even consider a blanket encryption ban is naive, in fact, such considerations are unlikely to have been contemplated. Encryption is heavily embedded into our digital society, where its complete removal would seek to pick-away at the very functionality of many mission critical systems and services, consequentially impacting many commercial ventures. Arguably nothing more needs to be said on any such proposal, leaving only considerations for targeted-decryption. Targeted attempts appear to be the method called for by many commentators, with platforms such as Whatsapp, Signal Messenger and Telegram bearing the brunt of much recent critical commentary. Yet as many would have likely considered before, the compromising of one platform would only seek to encourage the development of another which meets an individual's security needs, or the migration to one which already does. As a result, knowledge for the development of new encryption platforms will always be available.

Targeted encryption is also faced with addressing an impossible task - identifying only those communications in need of decryption in order to limit the unnecessary erosion of privacy. This can occur at both the 'platform level' and 'transaction level'. At a platform level, specific platforms can be targeted for decryption such as Whatsapp. Enforcing any encryption banning law on such an organisation would not be straightforward, requiring cross-jurisdictional compliance given many companies exist beyond the shores of the United Kingdom. Yet even this may not be enough, where any organisation itself must be willing to comply, an issue already demonstrated with the San Bernardino iPhone case[10]. Singling out platforms also poses a risk of retaliatory legal action aimed at governments who publically align their platform with terrorist usage, particularly where there may be limited evidence of such acts. Public declarations may result in damage suffered to reputation and operating costs, which may lead to compensation being sought. At a transaction level, targeting only those communications which are evidentially relevant to law enforcement is arguably impossible, with attempts inevitably leading to the collateral intrusion of the communications of those not involved in illegal acts.

Commercial acceptance & incentive:- Banning encryption provides limited commercial incentive in an industry where technology organisation rule. Multibillion pound organisations built upon reputations of consumer trust and reliance are unlikely to offer compliance to an order to offer an unprotected service to their clients. We have already seen this with Cook's open letter[11] regarding Apple's stance on this matter and the subsequent support offered by Facebook and Google. The San Bernardino iPhone case also suggested that governments may even see defiance from technology companies in regards to compliance with legislative command, where we are arguably approaching a situation where these organisations may become unregulatable.

The Backdoor 'argument':- The imposition of a backdoor was a focal point of discussions and allegedly a proposal made to Apple from the FBI during the San Bernardino iPhone case. The problem here remains that a backdoor fundamentally compromises a system undermining any existing security. As a result, whilst making a system potentially accessible to law enforcement, all users of a given system are vulnerable to unauthorised individuals with the requisite knowledge also exploiting such an access point. Backdoor arguments

undermine principles of information security, and risks causing an increase in acts of cyber crime stemming from the exploitation of the system defect. Arguably they are a non-viable solution to the encryption conundrum and have been reportedly condemned by many technology companies including Apple.

What happens if nothing is inside?:- Consideration must be given to the fact that once the hypothetical 'encrypted box' is open, what happens if there is nothing inside? There remains a real risk that in calling for the removal of encryption, officials may still fail to detect instances of terrorist communication. In addition, analysis may reveal that identified platforms are not in fact used to plan or engage in acts of terror. At this point, it arguably remains merely a supposition that extremist views are being consistently disseminated on platforms such as Whatsapp, Signal, Telegram. Although isolated incidents have lead to heightened suspicions, law enforcement are unlikely to know for certain that the removal of encryption will result in increased detection. As a result, governments are faced with a 'chicken and egg' scenario where calls to regulation encryptions need to be based on substantive evidence. Yet to acquire this data, examination of unencrypted content must be undertaken. There are no easy solutions, and a decision to remove encryption would be at best, a calculated risk, based on assumption.

Any decision to remove encryption also risks the loss of societal trust in government structures, where arguably any move to regulate encryption would require a government to justify their decision. This would require documenting the impact that being able to analyse communication data has had on increasing public safety and identifying terrorist activity. To do this requires a government establishing a measurement of success or the impact of their decision which is not straightforward. There is no benchmark from which to measure success of this type, and the correctness of their decision would likely be arbitrarily judged against a reduction in the number of terror events post-decision against those which have been witnessed in recent times.

Better the devil we know?:- Consideration must be given to the impact that removing encryption may have on the actions of those currently using such platforms. There remains a tangible risk that such acts drive terrorist and criminal communications underground, to undocumented and unknown platforms beyond contemplation of law enforcement. Removing encryption may also see a movement towards older or non-digital means of communication for planning purposes. Such circumstances would take time for governments to detect and redirect resources in other areas to support investigations, potentially increasing public risk during this period of adaptation. In addition, methods which increase surveillance, potentially exacerbate those currently relying on it, forming a catalyst for the development of more sophisticated off-the-grid methods of communication. Increasing attention towards encryption debates indirectly educates those currently relying upon it allowing them to make an informed decision for protecting their communication practices. Therefore by drawing attention to the issues in media reports, we may also be indirectly exacerbating the issue.

Cost:- All policing involves cost in terms of the allocation of resources and acquisition of suitable equipment. The removal of encryption potentially seeks to increase the volume of

decipherable content (likely millions of transactions) in need of analysis and therefore additional resources are needed to effectively examine it. Whilst automated methods may offer some use (for example, triage or targeted processes like image recovery and automatic grading for cases of illegal imagery, or, targeting specific terminology usage), in many cases surveillance would likely require man power and the subjective interpretation of any potential illegal actions in order to accurately respond to any perceived threat. Effective processing would require additional manpower which comes at a cost, and arguably it would need to be footed given the significant compromises to privacy suffered by society if encryption were to be removed. Government officials must evaluate whether such costs are first feasible and sustainable before even considering a decision which would allow access to this content, as ineffective analysis strategies would likely lead to public outrage. In addition, decisions must be made as to who will take the burden of these costs. Accessing transaction data following the prohibition of encryption is only valuable if it can be effectively processed. A risk remains that officials cannot handle the volume of data received both in terms of processing and its safe storage within applicable jurisdictional data protection legislation.

5 Some concluding thoughts

The encryption debate will almost certainly continue to feature in the agendas of politicians should future acts of terrorism be witnessed. The diverging opinions of law enforcement and technology providers means that regardless any solution chosen during future decision making processes, each party will likely oppose the views of the other. An accurate assessment of what is driving calls for the regulation of encryption must be made, questioning whether encryption is currently being made a scapegoat following recently witnessed terror events, or whether greater underpinning problems lie with resourcing and policing strategies.

It is key to note that reports following the attacks on London bridge on 3rd June 2017 and Manchester Arena on 22nd May 2017, suggest that some assailants were known to police[12,13]. Therefore law enforcement cannot claim to be solely reliant on the decryption of encrypted content in order to identify potential terrorists. The ability to survey online communications which are currently encrypted may or may not have supported a potential intervention method for preventing both attacks. Questions must be raised as to whether changes first need to occur to procedures for dealing with intelligence received in the first instance and the development of a viable effective response. This opens up a larger debate regarding the effectiveness of current counter terrorism regulation, beyond the scope of this article. An evaluation of these measures must take place to make sure that privacy is not unnecessarily compromised.

The removal of encryption is arguably a decision which should involve not only expert knowledge and opinion, but also the opinions of the general public, arguably those greatest effected by privacy violations. A referendum may provide such a measurement of public consensus. Particularly, it is necessary to identify whether society would be willing to sacrifice privacy in return for an assumed greater potential for safety and protection against planned acts of terrorism as the encryption debate is one of risk and reward, where a measurement of worth needs to be placed on each element.

To ban the use of encryption requires a leap of faith, which given the consequences to personal and commercial security may be too great a one to take. Any decision as important and impactful as encryption regulation should be underpinned with clear evidence of a need. A concern exists at present that a lack of empirical evidence of the need prohibit online encrypted communications leaves only a hope that it will improve current rates of detecting and preventing terrorism acts. Arguably this is not sufficient reasoning.

One scenario would require the acquisition of a sample of decrypted traffic for a defined period of time, i.e. remove encryption for a period of time, sample transaction data and analyse the findings. This approach would allow definitive data to be captured from which to build a suitable case for the prevention of encryption on a permanent basis. However given that it is likely that relevant terrorist communication exists as a significant minority of the total volume of online communication transactions taking place, sampling approaches are unlikely to lead to conclusive results. Further, defining a suitable timeframe from which to remove encryption and sample content would be troublesome where removing encryption from particular communication platforms maintains two hurdles to overcome. First, compliance from the provider to do such a sample and secondly, those using the platform but are aware of the sampling process may simply withdraw communication until the period is over (covertly carrying out the sampling process would raise significant ethical and legal considerations). Sampling without disclosing to users would arguably be needed to encourage 'normal' communication behaviour.

The debate also raises the question as to whether society has a right to total digital privacy, or whether this right is partial, where law enforcement and associated individuals are permitted to review content under certain circumstances. The latter appears to be the favourable view of former President, Barack Obama who offered the following opinion at South by Southwest (SXSW), Austin, Texas in regards to tackling encryption in 2016[14]:-

> "*I suspect the answer is going to come down to how do we create a system where the encryption is as strong as possible, the key is as secure as possible, it is accessible by the smallest number of people possible for a subset of issues that we agree are important*."

Many communication/social media companies have previously operated on this basis, where disclosure or access to some content is possible under the correct circumstances **(for** example, emergency requests linked to a risk of death or serious harm) given the correct procedures are properly followed[15]. It is only relatively recently that a shift towards systems offering technology companies potential plausible deniability is being witnessed, where passphrase/decryption information is no longer held server-side but on each customer's local device (see for example, Whatsapp- https://www.whatsapp.com/security/). Arguably a compromise would be to have decryption capability being held by each vendor, where suitable access is provided in cases of need, where requests can be subject to objective scrutiny and regulation. For such an approach to exist law enforcement would need to begin with looking to build better relationships with technology organisations (which may have been tarnished due to recent data-disclosure requests) and acquire their support for sustained information disclosure in the right scenarios[15]. Although cooperation and

disclosure may not be sought in all circumstances (see Horsman[15] for an analysis of disclosure procedures and regulation), arguably in cases of definitive need, compliance could hopefully be sought. This places emphasis on ensuring a valid need for data-disclosure before asking for it. However, the problem with this issue, is that it does not facilitate real-time surveillance of communications, only providing retrospective access to content.

There are no simple solutions to this somewhat recently emerging issue. Arguably, the removal of encryption and subsequent surveillance will not provide a solution to terrorism, where at best it may provide a solution to its reduction. Yet despite persistent calls for encryptions removal from communication protocols online, issues of feasibility and compliance would suggest that government officials are unlikely to act and successfully enforce any measures of this type.

References

1. Singman, Brooke (2017) 'Timeline of recent terror attacks against the West' Available at: http://www.foxnews.com/world/2017/06/05/timeline-recent-terror-attacks-against-west.html (Accessed: 7 June 2017)
2. Schulz, Wolfgang & Hoboken, Joris van (2016) Human rights and encryption, UNESCO Publishing
3. Bauer, Craig P., (2013) 'Secret History: The Story of Cryptology' CRC Press
4. Statista (2017) 'Most popular mobile messaging apps worldwide as of January 2017, based on number of monthly active users (in millions)' Available at: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (Accessed: 7 June 2017)
5. Tor Project (2017) 'Home' Available at: https://www.torproject.org/index.html.en (Accessed: 7 June 2017)
6. Moore, D. and Rid, T.,(2016) Cryptopolitik and the Darknet. Survival, 58(1), pp.7-38.
7. National Crime Agency (2016) 'NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016' Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file (Accessed: 10 June 2017)
8. BBC News (2017a) 'Amazon resists Echo murder evidence call' Available at: http://www.bbc.co.uk/news/technology-39063113 (Accessed: 10 June 2017)
9. ITV (2013) 'GCHQ cracked Ian Watkins' laptop password' Available at: http://www.itv.com/news/story/2013-12-18/lostprophets-singer-ian-watkins-sentenced/ (Accessed: 7 June 2017)
10. Bay, M., 2017. The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. *First Monday*, *22*(2).
11. Apple, (2016) 'A Message to Our Customers' Available at: https://www.apple.com/customer-letter/ (Accessed: 7 June 2017)
12. BBC News (2017b) 'Manchester attack: What we know so far' Available at:http://www.bbc.co.uk/news/uk-england-manchester-40008389 (Accessed: 10 June 2017)

13. BBC News (2017c) ‘London attack: UK was warned about third attacker’ Available at: http://www.bbc.co.uk/news/uk-40183147 (Accessed: 10 June 2017)
14. Carson, Biz (2016) ‘OBAMA: If government can't access phones, 'everybody is walking around with a Swiss Bank account in their pocket'' http://uk.businessinsider.com/obama-comments-on-encryption-at-sxsw-2016-3?r=UK&IR=T (Accessed: 7 June 2017)
15. Horsman, G., 2017. A survey of current social network and online communication provision policies to support law enforcement identify offenders. *Digital Investigation*
16. *Mary Madden, Lee Rainie. Pew Research Center, May 20, “Americans’ Attitudes About Privacy, Security and Surveillance.” Available at: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/* (Accessed: 3rd November 2017)

Biography

Graeme Horsman is a lecturer in computing at Teesside University, specializing in digital forensics. He has a BSc (Hons) degree in Computer Forensics, a PhD, graduate diploma in law and Masters of Jurisprudence. His research focuses on digital forensic examination techniques, methods for forensically investigating mobile devices, and knowledge-based systems for improving digital forensic examinations and evidence identification. Sub-topics include the use of so-called anonymous communication services and the potential detection of users and legislation surrounding the possession, distribution and creation of illegal imagery.