The UK's Legal Response to Terrorist Communication in the 21st Century:

Striking the right balance between individual privacy and collective security in the digital age.

Simon Hale-Ross

A Thesis submitted to Liverpool John Moores University in partial fulfilment of the requirements for the degree of Doctorate of Philosophy

March 2017

TABLE OF CONTENTS

DECLARATION

This thesis is entirely my own work and has not been submitted in full or in part for the award of a higher degree at any other educational institute.

No sections of this thesis have been published.

ACKNOWLEDGMENTS

Firstly I would like to express my utmost and sincere gratitude to my Director of Studies Dr David Lowe for his continuous support throughout my undergraduate study, through to my PhD study. Dr Lowe has shown great patience and displayed immense knowledge, and has never failed to mentor and inspire me. I would also like to express my deepest thanks to Dr Bleddyn Davies for his support, particularly on the emotive side assisting me to push through and keep moving in a forward direction. Without my supervisors this work would not have been possible, nor would I have my career aspirations and I simply cannot thank them enough.

I would like to thank both my fiancée's parents and my parents, and my siblings for their support throughout my studies, my mother Alison in particular who understood the difficulties associated with completing postgraduate study. Their continued support is greatly appreciated, which has assisted in bringing about my choice of career. I am further blessed with very supportive friends, Richard Ridyard, Richard Sanderson and Danny Riley in particular.

Finally, this work would not have been possible without the emotional support provided by my fiancée Charlotte and my cousin Ian. Both have helped me to remain positive and balanced, particularly throughout my final year of writing.

ABSTRACT

The dynamics of private life have changed along with the vast advancements in 21st Century communications technology. Private conversations no longer simply take place in the citizens' home or through using a landline telephone, but rather online through the Internet, social media and through the ever-growing list of chat applications available on the smartphone that allows encryption. However, what often follows the legitimate use of technological advancements is criminal, or in this case terrorist exploitation. In the digital age it has become increasingly easy for terrorist groups to communicate their propaganda and for individual terrorists to communicate freely. This has served to create an investigatory capabilities gap thereby increasing the pressures on UK policing and security agencies', in fulfilling their task of protecting national security and protecting the citizens' right to life.

In response, the UK and the European Union (EU) have attempted to close the capabilities gap and thereby ensure collective security, by enacting new laws allowing the law enforcement agencies' to monitor electronic communications. The UK Government has recently enacted the Investigatory Powers Act 2016 (IPA) that introduces and preserves the ability to bulk collect, and retain electronic communications data, and to attain the operators' assistance in decryption. Although the IPA attempts to take a human rights approach, the main contentious elements in the Act are those in relation to the authorities' capabilities to intercept electronic communications data on mass, and to retain such data. Specifically, concerns currently surround the

introduction of 'backdoors' into encrypted online services, and bulk interception and equipment interference warrants, and bulk personal data sets, all of which serve to weaken the security and individual data protection and privacy rights of, potentially, the entire population.

The Court of Justice of the European Union (CJEU) has been the most influential judicial body in terms of individual data protection, and thereby on the UK's law making process, through its key judgements in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others, and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* (*Digital Rights Ireland*).[1] The CJEU has done this by asserting the EU's constitutional and legal prowess in protecting data protection, such as Article 8 of the Charter of Fundamental Rights and byway of two directives, namely the Data Protection Directive in 1995 and the e-Privacy Directive in 2002.[2]

In order to close the capabilities gap ensuring national security, the UK Government must ensure the law endures by safeguarding the cohesiveness with the jurisprudence of the CJEU and the European Court of Human Rights (ECtHR). The courts do focus on different elements, built around the Conventional rights, with the CJEU focused on data protection and the ECtHR

[1] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* delivered on 8th April 2014 and reported at [2015] QB 127. Referred to as *Digital Rights Ireland*

[2] European Union Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Also: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. See also *S and Marper v UK* [2008] 48 ECHR 1581, [66]-[67], the Court noted the concept of private life is a broad term not susceptible to exhaustive definition.

on Article 8 right to privacy. To solve the balance between individual privacy and collective security, a human rights focus is required with emphasis placed on the practical reality that one cannot assert privacy rights, if one's right to life is not fully protected in the first place. This focus must re-forge the UK's counterterrorism legal structure. Taken in conjunction with the UK's already broadly worded counterterrorism legal framework, particularly the lack of a freedom fighter exclusion within the legal definition of terrorism, the consequence is to almost criminalise any expression of a view that the armed resistance to a brutal or repressive anti-democratic regime, could in certain circumstances be justifiable, even where such resistance is directed away from non-combatant casualties'.

Although the current counterterrorism structure is broad, the UK and the EU must police the Internet and remove the safe places used by criminals and terrorists. The IPA fashions a way within which to achieve this, but because it can be aimed at the whole population, subject to authorisation safeguards, and following historical case law dealing with blanket policies that effect the innocent, it is likely to receive continual CJEU and ECtHR judicial scrutiny. Post the UK's exit from the EU however, the CJEU may become less important leaving the ECtHR to conduct the analysis. At present, the UK must follow CJEU rulings when the matter concerns EU law, whereas ECtHR decisions are merely recommendatory.

The thesis found that overall, the balance between collective security and individual data privacy rights in the UK are fairly stable because of the role

and importance of judicial review; judicial independence, and the over-arching scrutiny provided by commissioners and parliamentary committees. It is further argued that a blanket approach to retaining electronic communications data is necessary in finding the terrorist in the ever growing haystacks, because sometimes privacy rights and data protection must be curtailed to ensure the state can protect citizens' rights to life.

INTRODUCTION

> …terrorism is a generic concept covering a wide range of phenomena, with important political, philosophical, psychological, historical, ethical and legal dimensions.[3]

Whilst the majority of academic research approaches the subject of terrorism from a sociological perspective, this thesis approaches the subject from a legal black letter law doctrinal viewpoint, listed within Wilkinson's analogy.[4] The House of Lords decision in *A and others v Secretary of State for the Home Department*, kindled this perspective in Lord Hoffmann's judgement, illustrating the dichotomy between terrorism, the resulting restrictive laws and human rights:

> In my opinion, such a [counterterrorism] power in any form is not compatible with our constitution. *The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws such as these*. That is the true measure of what terrorism may achieve. It is for Parliament to decide whether to give the terrorists such a victory.[5] [My emphasis]

This statement inevitably prompted this postgraduate research. However, the research focus shifted from the controversial area of law highlighted by Hoffmann, to another increasingly controversial area, dealing with bulk electronic communications data surveillance, and bulk equipment interference. Rather than exploring counterterrorism measures that effect the few, these new measures are aimed at the population as a whole, and this is where the CJEU's decision in

---

[3] Wilkinson, P. cited in R. Jackson and S. J. Sinclair (2012) Contemporary Debates on Terrorism (Routledge) p.11

[4] *Ibid*

[5] [2004] UKHL 56, [97]bulk Although beyond the ambit of this thesis Hoffmann was referring to sections 21 and 23 of the Anti-Terrorism, Crime and Security Act 2001 (ATCSA) that allowed for the indefinite detention of foreign nationals, without having been formally charged or having gone through due process.

Digital Rights Ireland became prevalent, given it repealed the EU's 2006 Directive and with parties concerned having successfully challenged the UK's Data Retention and Investigatory Powers Act 2014 (DRIPA).[6]

The research began by looking into UK's legal counterterrorism structure and examining other academic researchers' contributions. It quickly became clear that the terrorist threat faced is extraordinarily different from previous experiences, particularly following al-Qaeda's terrorist attack on the United States on the 11th September 2001.[7] The use of 21st Century communication technology by stateless terrorist organisations, such as al-Qaeda and more recently by the Islamic State, in influencing and recruiting others to their cause, illustrates the need for legislative measures.

The thesis examines a number of issues, from the legal perspective related to surveillance of electronic communications data including analysis of UK's counterterrorism legislation, and the impact of this on society. In order for the thesis to attempt to analyse the issues, the UK Governments approach to legislating for counterterrorism must be explored. Clearly, legislation must be aimed at combatting the 21st Century terrorist threat whilst ensuring human rights

---

[6] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* delivered on 8th April 2014 and reported at [2015] QB 127. Referred to as *Digital Rights Ireland*

[7] *Ibid*

protections.[8] What first became clear is that the UK's current counterterrorism structure has been built up, layer by layer over time, which significantly curtail human rights and civil liberties.[9] This led to the striking fact many of these counterterrorism laws lacked full and complete pre-legislative scrutiny, which has then led on to simply create a sometimes-abrasive relationship between the judiciary and the executive when conducting post-legislative scrutiny.[10] Compounding a controversial area of law with controversial legislation is certainly damaging on a number of fronts, not only to human rights but to legitimate law making and the reputation of the Government, and the UK Government appear to have recognised this fact given the recent passing of the Investigatory Powers Act 2016.

Focusing on the UK's counterterrorism legal framework the research highlighted the fact that the laws in this area are comprehensive and interlinked with other regulatory laws not entirely terrorism focused, such as the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA). It was around this time that the UK Government, introduced many broadly worded Acts, the reach of which have been merely moderated by unelected executive

[8] D. McKeever (2010) The Human Rights Act and anti-terrorism in the UK: one great leap forward by Parliament, but are the courts able to slow the steady retreat that has followed? *Public Law*, 110-139, 111

[9] *Ibid*

[10] The Anti-Terrorism, Crime and Security Act 2001 was enacted 33 days after the first reading in Parliament. See the Report on the Anti-Terrorism, Crime and Security Bill 2001 (2001-02 HC 351), & Reports on the Anti-Terrorism, Crime and Security Bill (2001-02 HL 37, HC 372) and (2001-02 HL 51, HC 420). Also the Prevention of Terrorism Act 2005 was enacted within 17 days of the first reading in Parliament. See the Joint Committee on Human Rights, Prevention of Terrorism Bill (2004-05) (2005) HL 68 Paragraph 1, 'The rapid progress of the Bill through Parliament has made it impossible for us to scrutinise the Bill comprehensively for human rights compatibility in time to inform debate in Parliament'.

departments, the Department of Public Prosecutions for example. This is an important point because these broadly worded Acts fashioned a repeated movement between the UK Government and the jurisprudence of the ECtHR, whereby the Government's conjoined reactionary attitude to law making evidently served to protract many different and repeated discussions surrounding individual human rights and civil liberties, and State powers.[11] The lack of pre-legislative scrutiny here simply serves to create further contention between Parliament and the judiciary as they effectively conduct post-legislative scrutiny. Changes in UK legislation only seem to happen when the judiciary decide against the Government. However, if the Government would implement recommendations made by others, such as their own various Parliamentary committees and appointed independent reviewer of anti-terrorism legislation, the situation could potentially be eased.

There has been an unprecedented amount of counterterrorism legislation enacted by the UK Government since the introduction of the Terrorism Act 2000, which re-defined an act of terrorism. The rationale behind this is that these have been aimed at policing the changing nature and methods of terrorism, thereby attempting to reduce the terrorist threat posed. Some of these legislative measures, such as the Prevention of Terrorism Act 2005 that was replaced by TPIMs, and particularly sections 1 and 2 of the Terrorism Act 2006 that have not

[11] For example sections 1 and 2 of the Terrorism Act 2006, enacted in a reactionary fashion to the 7th July 2005 terrorist attack on London serves to show an example. Another example is ATCSA that was presented to UK Parliament on the 12th November 2001 and enacted on the 14th December 2001, in response to the terrorist attack on the United States on 11th September 2001.

been as effective as the UK Government had hoped, have simply proved redundant in the face of the quickened speed of 21st Century technological growth. Using Islamic State as a case study, the research illustrates that current legislation remains ineffective; particularly since that overall the group's use of their digital communicational strategy has proved first class. The problem therefore remains: How can the UK's legal response to how terrorists communicate in the 21st Century balance individual privacy rights whilst ensuring collective security?

The thesis, being a doctrinal black letter law study, starts by conducting research into the restricted activity, important because of the impact these counterterrorism laws have, conferring special restrictions upon individual citizen's and providing special executive powers to the State. The activity in this instance is terrorist action of course, which is distinguishable from other forms of violent criminal aggression. This is because the deployment of this tactic, which ultimately results in the indiscriminate killing of innocent civilians, with whom the perpetrators have no relationship other than the fact they are there at the time, is motivated by the desire to gain publicity for their cause.[12] Used by groups and individuals, terrorist action has been described as triadic rather than dyadic in terms of the effectual relationship, reaching far beyond the immediate victims involving other

[12] *R v F* [2007] EWCA Crim 243, [29], the very nature of terrorism is indiscriminate. See also C. H. Simmons and J. R. Mitch (2001) Labelling Public Aggression: When Is It Terrorism? *The Journal of Social Psychology*, 125:2, 245-251, 245.

observers and the media.[13] Forming an integral part to the success of a terrorist attack is the placement of fear in the population, by effecting a spectacular event causing death and serious injury. Essentially aimed at undermining democracy, states are almost forced to take legislative action in seeking to prevent and pre-empt further episodes.

Whilst there is little international agreement on the accurate ascription of the terrorist label, the rule of law demands clarity and precision to enable the state to deal effectively with the problem.[14] The importance of the rule of law continued to push through the research, to which the legislature, the executive and law enforcement staff must all work within. Legal definitions must be precise and insofar as possible representative of the problems they are designed to address.[15] The difficulty found in trying to formulate a legal definition of terrorism, is the fact that the term 'terrorism' is subjective, pejorative and political, which is usually applied by one's enemies, rendering it as ambiguous as other terms such as democracy, freedom, justice and equality.[16] Internationally and domestically the terms use is entirely dependent on the legislators or definers' viewpoint and is

---

[13] F. J. Hacker (1980) Terror and Terrorism: Modern growth industry and mass entertainment, *Studies in Conflict and Terrorism*, 4, 143-159. Hacker argues most aggression is dyadic, involving the attacker and victim only, whereas acts of terrorism are described as triadic due to the dramatisation of the events, involving observers and the media. See also C. H. Simmons and J. R. Mitch (2001) Labelling Public Aggression: When Is It Terrorism? *The Journal of Social Psychology*, 125:2, 245-251, 246.

[14] *Ibid* as per C. H. Simmons and J. R. Mitch (2001) at 245

[15] Analysis drawn from Lord Carlile of Berriew Q.C. (2007) Independent Reviewer of Terrorism Legislation, The Definition of Terrorism, March 2007, CM7052, p.21

[16] B. Hoffman (2006) Inside Terrorism (2nd Edition, Columbia University Press) pp.1-44: The term 'terrorism' has changed from the revolutionary view in the 1970's, to the pejorative present day view implying moral and social judgment. This change in direction has been driven by political will. See also R. Jackson, L. Jarvis, J. Gunning and M. B. Smyth (2011) *Terrorism: A Critical Introduction* (Palgrave Macmillan) p.101

often ascribed opportunistically, rather than representing, factually, a description of a tactic.[17] Fashioning a 'one size fits all' legal definition of terrorism is extraordinarily difficult given that globally, there are a large number of groups labelled as terrorist, all with different grievances employing different tactics.[18]

An issue that repeatedly comes to light is the low threshold and broadly worded nature of the definition of terrorism under section 1 of the Terrorism Act 2000. All the independent reviewers of anti-terrorism legislation have recommended the threshold be raised, such as from 'influence' to 'intimidate', which unnecessarily expands the applicability of the terrorist label, yet the UK Government have failed to implement the changes. For Gale this is simply representative of the UK remaining in a permanent state of emergency, and as a result measures are increasingly encroaching upon UK citizens' rights, protected under the European Convention of Human Rights (ECHR) and, at least for the time being the European Union Charter of Fundamental Rights 2000 (CFR).[19] However, the definition serves its purpose well in practical terms, where law enforcement

---

[17] *Ibid*

[18] A. Martyn (2002) *The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September.* Australian Law and Bills Digest Group, Parliament of Australia Web Site http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/CIB/cib0102/02CIB08 accessed 2 September 2015

[19] C. J. S. Gale (2006) The UK Response to Terrorism: Human Rights and a Wider Perspective, *Working Paper Series*, No 06/01. See also J. Welch, and S. Chakrabarti (2010) The War on Terror without the Human Rights Act – what difference has it made? European Human Rights Law Review, (6), 593-600, 594. Measures include those such as sections 57 and 58 of the Terrorism Act 2000 that criminalise the collection of terrorist documentation, and section 59 covering incitement. The Terrorism Act 2006 was then enacted to attempt to fill the vacuum between phrases such as 'incitement' and 'encouragement', but all have been unsuccessful in preventing terrorist groups from spreading their propaganda through the Internet.

agencies' use it to determine if the activity they are investigating is terrorist. This has been particularly important when determining if the electronic communications data is terrorist or not. Overall the thesis found that technological advancements constantly evolve and progress, and it is therefore essential the UK legislature change its approach, from reactionary to progressive seeking to stay one step ahead, ensuring that law enforcement do not continue to suffer from the capabilities gap. In the attempt to remedy this, the UK has recently enacted the IPA that will introduce extremely wide state discretionary powers of electronic data surveillance.

The thesis found that the use of the Internet is continually expanding, as is the growth and use of commercially available encrypted direct messaging applications, largely used legitimately and extensively by smart phone users. Given that the average age of the IS recruit is 24; the subsequent growth in the use of this technology by terrorists is not entirely unexpected. Most 24 year olds have grown up with the Internet and smart technology, and are therefore proficient in its use. Cyber-crime has vastly escalated along with the use of the darker side to the Internet, coincidentally named the 'Darknet'. The capabilities presented to a potential terrorist by the darknet are perhaps the most concerning and startling, allowing those who mean to do serious harm anonymity and access to weaponry, including firearms, ammunition and explosives.

The IPA is an essential element in forming part of the UK Governments approach, in order they may determine which members of the public are friend or foe. The proliferation of terrorist communication through the Internet and social media means that the Internet must be monitored, if they are to avert the dangerous and destructive nature of a terrorist attack. This is a controversial area of law, where the IPA seeks to focus on surveillance powers, bringing many powers under one statute and repealing others, and is aimed at far more than the gathering of bulk data. In addition to the bulk electronic data collection and retention powers, the IPA introduces the ability to decrypt messages sent through instant messaging applications, such as Whatsapp.[20] The possible outcome of increased state presence online, which may result in a sudden growth of the availability of anonymity software and services, seems to have been pre-empted by the Government. Section 253 of the IPA offers such pre-emption, allowing the Secretary of State to issue an operator a technical capability notice, requesting all assistance in the removal of electronic protection. It may however prove difficult to police given the international nature of the Internet, and of course the locality of service and application providers.

In order to reassure and gain public support for this legal initiative, a human rights and civil libertarian approach must be taken with an infusion of open and honest Governance, aimed at building trust. Utilising the CJEU's jurisprudence, the

[20] Investigatory Powers Act 2016, Part 6 for Bulk Powers, and s 253(5)(c): The Secretary of State may impose an obligation on the service provider to remove electronic protection, i.e. Encryption.

thesis has developed a new criterion from the *Digital Rights* case, from which to test the IPA, which is that:

1. Primary legislation must lay down clear and precise rules governing the scope and application of the measure;
2. Minimum safeguards must be imposed sufficiently reducing the risk of abuse or unlawful access to the data;
3. Access to the data must be expressly provided for, limiting the number of persons authorised to have such access and restricted to the purpose of preventing and detecting precisely defined serious criminal offences;
4. Access to the data will only be granted after a prior assessment has been made by an independent administrative body or court, with the primary focus on human rights and proportionality of the measure;
5. Retained data will be deleted after 12 months unless an independent administrative body or court decides otherwise, having weighed the evidence and conducted a proportionality test.[21]

The passing of this test and the focus on the building of trust is crucial given that the IPA has passed through the UK Parliament, resulting in the public's belief that they are being constantly subjected to bulk electronic communications data collection and retention, effectively removing the majority of available online privacy. Human rights groups such as Liberty, who use over-exaggerating flamboyant language to gain support in challenging UK State powers, perpetuate this belief.[22] Of course, in practical terms nothing could be further from the truth for two reasons.

---

[21] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others,* delivered on 8th April 2014 and reported at [2015] QB 127. Referred to as *Digital Rights Ireland*

[22] See https://www.liberty-human-rights.org.uk accessed 30 December 2016

Firstly, law enforcement agencies' have finite resources and simply cannot physically conduct surveillance on the entire population.[23] This has been made apparent where they have even struggled to keep careful watch of targeted individuals, such as the killers of Fusilier Lee Rigby.[24] Although the IPA allows for the retention of electronic communications data to be stored for 12 months, and legislative pre-emptive measures that criminalise neutral behaviour are littered thought the UK's counterterrorism framework, the thesis will argue that neither affect individual privacy rights in the way portrayed by Liberty. The doctrinal methodology will highlight that mass data retention does not equate to mass data surveillance, and pre-emptive measures are not 'pre-crime' measures. They are in fact, criminal offences.

Secondly, the Home Secretary must first sanction the use of bulk powers, which is then subject to independent judicial approval, and reviewable by the Independent Investigatory Powers Commissioner.[25] This 'double lock' system provides a new proactively pervaded human rights agenda. With this in mind, the thesis will argue that the balance in the UK between collective security and individual data privacy is reasonably steady because of the role and importance of judicial

[23] First sitting Committee Debate Session 2015-16, Investigatory Powers Bill, Publications on the Internet, Column 23, 24 March 2016 available at http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160324/am/160324s01.htm accessed 30 August 2016

[24] The Rt. Hon. Sir Malcolm Rifkind MP, Report on the intelligence relating to the murder of Fusilier Lee Rigby, Intelligence and Security Committee of Parliament, HC 795, 2014 at p.81

[25] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473744/Factsheet-Investigatory_Powers_Commission.pdf accessed 2 December 2016

review; judicial independence, and the over-arching scrutiny provided by commissioners and parliamentary committees.

THESIS OUTLINE

The information presented in this thesis is correct as at the 30th December 2016. The thesis contains five chapters, plus the Introduction, Methodology and Conclusion. As explained in the Introduction the hypothesis to be tested throughout the thesis is: How can the UK's legal response to how terrorists communicate in the 21st Century balance individual privacy rights whilst ensuring collective security?

Chapter One opens the thesis by outlining the UK's current legal definition of terrorism. It discusses several elements to the definition position, such as the undefined phrases used and resulting breadth of capture. The impact on the rule of law is considered along with a focus on human rights infringements. The Chapter focuses on the legal definition of terrorism because it is the definition used by law enforcement agencies', and applied by the UK courts to activities related to surveillance of electronic communication data. Chapter Two then moves on to consider how terrorist groups and individual terrorists communicate in the 21st Century. It highlights the growth in technology and how, using the Islamic State as a case study, they have used this to fashion an extraordinary threat level whereby law enforcement have difficulty in recognising friend from foe.

Arguing the law enacted that is aimed towards protecting national security and the lives of UK citizens' is not used effectively, Chapter Three is introduced showing the UK latest efforts to close the technological capabilities gap. Taken in conjunction with the counterterrorism framework, this new law will provide the State with exceptional powers of online electronic communications data surveillance. Illustrating the implications for human rights and the rule of law, Chapter Four is where the original contribution comes to fruition, where the chapter discusses the Court of Justice of the European Union's jurisprudence in the area of individual data protection, developing a new criterion to test the Investigatory Powers Act 2016. This criterion is again used to test international intelligence exchange between the EU and the United States of America covered under Chapter Five, that then goes on to look at the potential relationship between the EU and the UK following the UK's exit from the EU, estimated to take place in 2019. Looking forward and highlighting some potential stumbling blocks to successful negotiation, the situation appears to not be as worse as first thought.

METHODOLOGY

In order to answer the research question overall, it is essential that the methodology used is able to stand up to scrutiny. The thesis takes a doctrinal, black letter law approach, which is perhaps the most traditional methodology for a legal study. Significantly analytical and interdisciplinary, it provides a legalistic approach to concentrate on the letter of the law. The primary aim of this method is to collate the legal rules surrounding a research question and critically analyse existing normative rules and the laws effectiveness. Being a black letter law study, the thesis is an amalgamation of doctrinal and non-doctrinal research. Doctrinal research naturally marginalises political, ethical, moral and societal impact discussions, and may be described as narrow:

> 'All [non-doctrinal] legal research can be generally grouped within three categories: problem, policy and law reform based research...They can be considered together because of the often-occurring link between them. In fact, all four categories of research, doctrinal, problem, policy and law reform, could be part of a large-scale research project. A researcher, for example, could begin by determining the existing law in a particular area (doctrinal). This may then be followed by a consideration of the problems currently affecting the law and the policy underpinning the existing law, highlighting, for example, the flaws in such policy. This in turn may lead the researcher to propose changes to the law (law reform)'.[26]

The thesis therefore reflects the great tradition of legal scholarship and uses mainly primary sources of data, such as legislation found in UK statute books and case law, which is reported. This approach fits within the broader picture of

[26] I. Dobinson and F. Johns, (2007) Qualitative Legal Research, in M. McConville and W. Chong Hui (eds), Research Methods for Law (Edinburgh University Press) pp19-20.

social science theory and methodologies, and whilst a substantial amount of secondary data is relied upon, it remains empirical:

> '[E]mpirical research, as natural and social scientists recognise, is far broader than these [normally] suggest[ed]. The word "empirical" denotes evidence about the world based on observation or experience. That evidence can be numerical (quantitative) or non-numerical (qualitative); What makes research empirical is that it is based on observations of the world...These facts may be historical or contemporary, or based on legislation or case law, the results of interviews or surveys, or the outcomes of secondary archival research or primary data collection'.[27]

The thesis will therefore make empirical observations and offer original critical analysis on the UK's current counterterrorism and surveillance law structure, focusing on those dealing within the ambit of the research question. Given the UK's legislative interdependency on European Union law, specifically with regards to data protection, the thesis will further critique relevant EU Treaty law, regulations, directives and framework decisions, and the relevant articles from the Charter of Fundamental Rights and Freedoms 2000.

Contribution to Research

The significance of the approach taken in this thesis naturally allows for a certain degree of originality in so far as interpretation of primary and secondary sources. Chapter One provides a good example of the merits of this approach, where the legal definition of terrorism is heavily critiqued and compared to other jurisdictions. In doing so, the Chapter develops a new legal definition, which provides a higher level of legislative certainty and in turn, some protection from

[27] L. Epstein and G. King (2002) The Rules of Inference, 69 U. Chi. L Rev. 1, 2-3

the current remarkably low thresholds set. Chapter One proves essential to the research question, given that law enforcement and the courts in assessing whether or not the action is deemed to be terrorist use the current definition.

Chapter Two considers how terrorist groups and individual terrorists' communicate in the 21st Century, critically analysing the current digital problems fashioned. The doctrinal approach then assists Chapter Three in examining the UK's latest efforts, in attempting to close the capabilities gap faced by law enforcements, as discussed in Chapter Two. Analysing the UK's current legal surveillance framework, the Chapter offers original critique to the newly enacted Investigatory Powers Act 2016 (IPA).

Highlighting the implications for human rights and the rule of law, the uniqueness and the advancement of the doctrinal methodology used enables Chapter Four to develop a human rights based criterion, called the Digital Rights Criterion, from which to test the IPA, and potentially future counterterrorism laws, ensuring compatibility with the jurisprudence of the CJEU and the ECtHR. Utilising the doctrinal approach, the Chapter challenges the terms 'pre-crime' and 'mass surveillance', illustrating the effectiveness of the method used. It is concluded that particularly since the enactment of the IPA, the UK has managed to correctly balance collective security with individual data privacy.

The doctrinal methodology is then utilised in Chapter Five in order to illustrate international intelligence exchange. The current PNR agreement between the EU and the USA is used as a case study, to explore the potential relationship between the EU and UK, for when the UK becomes a third country in 2019. The Digital Rights Criterion is then used to test potential future international intelligence exchange post the UK's exit, ensuring this continues in line with current agreements, thereby maintaining law enforcements' capabilities.

CHAPTER ONE. THE UNITED KINGDOM'S LEGAL DEFINITION OF TERRORISM

INTRODUCTION

Terrorism is distinguishable from other forms of criminal activity and aggression, by the indiscriminate killing of innocent civilians and the lack of nexus between the victims and perpetrators, and by the motivational aspect to gain publicity.[28] The substantive risk posed by terrorism to national security and to the public in the 21st Century, are so serious in consequence and so complex to investigate as to justify specialist counterterrorism legislative powers, and increased powers of electronic communications data surveillance.[29]

This chapter is important to the thesis title because it outlines the 21st Century understanding of the concept of terrorism, illustrating the need for specialist permanent counterterrorism legislation. UK law enforcement and the courts use the legal definition of terrorism in order to ascertain if the crime being investigated is in fact, terrorist related. It legally defines what actions amount to terrorism and introduces an extra-jurisdictional provision illustrating the international nature of the threat. By considering certain prominent cases, this

---

[28] *R v F* [2007] EWCA Crim 243, [29]. See also C. H. Simmons and J. R. Mitch (2001) Labelling Public Aggression: When Is It Terrorism? *The Journal of Social Psychology*, 125:2, 245-251, 245.

[29] D. Anderson (2014) The Terrorism Acts in 2013, London: The Stationary Office p.84

chapter reveals that the UK's legal definition of terrorism presents numerous shortcoming, such as the relative lack of resolute definitions for certain phrases used, which has led to malleable judicial application. These undefined phrases have also resulted in rather low thresholds, thereby expanding the term 'terrorism' beyond international comparisons. Discussion will then be introduced on what this clear and evident lack of legislative uncertainty means for the rule of law.[30] The alternative options to the phrases used will be analysed, revealing this would be a better choice for the UK's definition, ultimately resulting in greater understanding and fairness, having been brought into line with international law.

The aim of this chapter is not to offer a full and comprehensive exploration of the historical changes surrounding the term 'terrorism', rather to focus on the legal definition of terrorism and to present the research findings concerning the phrases used within the legislation. These inconsistencies can be described as a legislative failure due to the higher currency fixed to the political value of terrorism. In reality, it is not feasible to entirely remove this political value simply because UK Parliamentarians create law, and terrorism is after all a political crime. This chapter therefore advocates for a permanent definition of terrorism that is as free as possible from ambiguous phrasing, focusing on the wrongful nature in line with international law.

[30] Legal terms must be clear and precise, analysis drawn from Lord Carlile of Berriew Q.C. (2007) Independent Reviewer of Terrorism Legislation, The Definition of Terrorism, March 2007, CM7052, p.21

Terrorism: The Concept

Before considering the law in this area, it is fundamental to briefly highlight the concept of terrorism and illustrate the need for specialist legislation. Without a doubt terrorism is characteristically a unique from of criminality, whereby the high risk posed to national security and to the public, are so serious in consequence, often resulting in the indiscriminate killing of innocent civilians, and are increasingly complex to investigate, as to justify specialist legislative powers.[31] Put plainly, the nature of the 21st Century terrorist threat has augmented whereby terrorists' capabilities have increased, particularly in the digital age, which has allowed them to remain unknown to the policing and security services until the moment of attack.[32] Although debatable, the description of terrorism was provided by Wilkinson as:

> …coercive intimidation or more fully as the systematic use of murder, injury, and destruction or threat of same to create a climate of terror, to publicise a cause, and to coerce a wider target into submitting to its aims.[33]

It is clear that 'without being noticed terrorism would not exist', meaning the act of killing alone fails to create a terrorist act.[34] The acts to which are assigned to the terrorist label are deliberate terrifying events, but without its horrified

---

[31] *Supra* as per D. Anderson (2014) p.84

[32] J. Klausen (2009) British Counter-Terrorism After 7/7: Adapting Community Policing to the Fight Against Domestic Terrorism *Journal of Ethnic and Migration Studies*, Vol. 35, No. 3, March, 403-420, 404. See also *Supra* as per The RT Hon Lord Lloyd of Berwick (1996) paragraph 1.7

[33] P. Wilkinson (2006) *Terrorism versus Democracy: The Liberal State Response* (2nd Edition, Routledge,) pp.20-21. Professor Paul Wilkinson is the former chairman of the Centre for the Study of Terrorism and Political Violence at St Andrews University

[34] *Ibid*

witnesses, it would be rendered as 'pointless as a play without an audience'.[35] For Wilkinson, the general public understanding of terrorism in the 21st Century includes bombing campaigns, shootings and hostage takings, hijackings and threats of carrying out these actions, aimed at the civilian population.[36] Conceptually and empirically, terrorism can be distinguished from other violent crimes by following characteristics such as:

- Premeditated and designed to create a climate of extreme fear;
- Directed at a wider target than the immediate victims;
- Inherently involves attacks on random or symbolic targets, including civilians;
- Considered by the society in which it occurs as 'extra-normal', that is, in the literal sense that it violates the norms regulating disputes, protest and dissent;
- Used primarily, though not exclusively, to influence the political behaviour of governments, communities or specific social groups.[37]

Because terrorism is directed towards a wider target than the immediate victims, the effectual relationship is different from the normal ideas on violent criminal behaviour. Normally one would know one's victim, and simply aim the violent criminal aggression towards that person. Hacker recognises this and described the terrorist relationship as 'triadic', reaching far beyond the immediate victims involving other observers and the media, with normal criminal activity being 'dyadic' in nature, meaning that the aggression is limited involving only the

---

[35] M. Juergensmeyer (2000) Terror in the Mind of God: The Global Rise of Religious Violence (University of California Press) p.139

[36] *Supra* as per P. Wilkinson (2006) p.1

[37] *Ibid*

attacker and the victim.[38] The placement of fear in the population forms an integral part to the success of a terrorist attack. Essentially aimed at undermining democracy, states are almost forced to take legislative action in seeking to prevent and pre-empt further episodes by providing policing and security agencies sufficient powers.

This was recognised by the UK's former Home Secretary Jack Straw in 1999 where he defended to the UK Parliament why special powers and restrictions were desirable, stating:

> 'Terrorism differs from crime motivated solely by greed in that it is directed at undermining the foundations of government'.[39]

This statement goes to the heart of the rationale behind the introduction of the Terrorism Act 2000 and within this context, epitomises the key mischief of terrorism that is its danger to democracy.[40] An effective political response, adopting specialist terrorist offences rather than relying on the normal criminal law is required, especially when having regard to the international nature of terrorism and the UK's obligations under international law.[41]

The UK Government's independent reviewer of anti-terrorism legislation, David Anderson QC, supports this contradictory view that terrorist violence is not

---

[38] F. J. Hacker (1980) Terror and Terrorism: Modern growth industry and mass entertainment, *Studies in Conflict and Terrorism*, 4, 143-159. See also C. H. Simmons and J. R. Mitch (2001) Labelling Public Aggression: When Is It Terrorism? *The Journal of Social Psychology*, 125:2, 245-251, 246.

[39] Jack Straw MP, the then Home Secretary, The Terrorism Bill, Second Reading HC 14 December 1999, col 152

[40] C. Walker (2009) *Blackstone's Guide to The Anti-Terrorism Legislation*, (2nd Edition, Oxford University Press) p.10

[41] *Supra* as per The RT Hon Lord Lloyd of Berwick (1996) Chapter 2 paragraph 2.2 and 2.3

necessarily worse than ordinary crime, and has therefore recommended a review of criminal law specifically in the area of national security, focused primarily on the necessary extent in supplementing ordinary rules and procedures.[42] He seems to advocate this position due to the amount of counterterrorism legislation that is aimed at early intervention, enacted whilst being drawn to focus on the worst-case scenario. This is an important point given that should law enforcement, through the use of electronic communications data surveillance determine a person has been disseminating terrorist publications through the Internet, the current counterterrorism structure criminalises this conduct, which would have otherwise fallen short of a prosecutable offence under the ordinary criminal law of inchoate offences.[43] McKeever takes this argument further and confirms that action captured by counterterrorism laws is well below the standard required by ordinary UK criminal law, whereby 'only that action which goes beyond mere preparation for the commission of the offence, is criminalised as attempt'.[44] The threshold for attempt is extremely high where the suspect must only have the actual crime left to commit.[45] Given the potential devastating nature of a successful terrorist attack, law enforcement and the courts must be able to intervene before this point. Simply waiting for example, until the suspect has his finger hovering over the trigger is not a viable option. This is why it is argued that Anderson is potentially

---

[42] *Supra* as per D. Anderson (2014) p.83

[43] Terrorism Act 2006, ss1, 2

[44] *Supra* as per D. McKeever (2010) 119

[45] Criminal Attempts Act 1981 s 4(3)

incorrect in advocating that counterterrorism laws must be closely associated with ordinary criminal law.[46]

It is further pertinent to note, that the serious implications of being convicted and labelled a terrorist remain with that person for the rest of their lives. This is because the term has become increasingly pejorative, particularly in the 21st Century, where the terrorist label almost dehumanises the person convicted. This could potentially be due to the inhuman behaviour committed by terrorist groups, such as al-Qaeda and IS, depicted in the graphic and disturbing media released by the group, showing the beheading of non-combatant western citizens' and combatant captives. Justice Collins pointed out the pejorative nature of the label in *R (CC) v Commissioner of Police of the Metropolis and another*, stating:

> …once a terrorist always a terrorist whether or not the person in question has renounced his past or circumstances have changed (for example where the acts of terrorism occurred in a country whose government, perhaps because dictatorial and oppressive, has since been overthrown). Indeed, the terrorist may have become a respected and respectable member or even leader of the new government of that country. Nevertheless, he is still a terrorist within the meaning of the [Terrorism Act] 2000.[47]

[46] *Supra* as per D. Anderson (2014) p.83

[47] [2011] EWHC 3316, [5]

THE LAW IN THE UNITED KINGDOM: THE TERRORISM ACT 2000

The foundation stone to the UK's current specialist legislative counterterrorism framework is the Terrorism Act 2000. Simply, it legally defines what actions amount to an act of terrorism and is used by UK law enforcement and the courts to determine if the criminal action is terrorist related.[48] Under section 1 of the Terrorism Act 2000, in order for an action to be deemed as terrorist, three collective elements are required, the action or threat of action, the target and the causes.[49] The use or threat of action must involve,[50] serious violence against a person[51] or serious damage to property,[52] or endanger a person's life[53] or create a serious risk to the health and safety of the public or a section of the public,[54] or be designed to seriously interfere with or seriously to disrupt an electronic system.[55] The use or threat must be designed to influence the government or an international organisation,[56] or to intimidate the public or section of the public.[57] The second element is expressly made redundant by way of an exclusory provision however, when such action or threat of action involves the use of

---

[48] It has also been described as a lynch pin in *R v F* [2007] EWCA Crim 243, [962], a corner stone at [963], and central to counterterrorism legislation at [967].

[49] *Supra* as per D. Anderson (2014) p.75

[50] Terrorism Act 2000, s 1(1)(a)

[51] *Ibid* s1 (2)(a)

[52] *Ibid* s1 (2)(b)

[53] *Ibid* s1 (2)(c)

[54] *Ibid* s1 (2)(d)

[55] *Ibid* s1 (2)(e)

[56] International organisation was added to section 1 of the Terrorism Act 2000 by an amendment brought in by the Terrorism Act 2006, s 34(a)

[57] Terrorism Act 2000, s1 (1)(b)

firearms or explosives.[58] In satisfying the causes element, the use or threat must be made for the purpose of advancing a political, religious, racial[59] or ideological cause.[60]

Comparatively, overall the international perspective is not very different in terms of the words used to define an act of terrorism.[61] Although the international community have not entirely succeeded in defining terrorism, the United Nations (UN) Member States have adopted a series of conventions, which attempt to define and criminalise terrorist activities.[62] In 1994 the UN General Assembly condemned terrorist acts as:

> Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.[63]

Similar to the international situation, the UK legal definition of terrorism is essential in condemning violations of human rights by other citizens' and to ensure adequate protection of both the state and its citizens'.[64] It is also argued that 'without a definition of terrorism it is impossible to formulate or enforce

---

[58] *Ibid* s1 (3)

[59] The racial element was added to section 1 of the Terrorism Act 2000 by an amendment brought in by the Counter-Terrorism Act 2008, s 75(1)

[60] Terrorism Act 2000, s 1(1)(c)

[61] *Al-Sirri v Secretary of State for the Home Department (United Nations High Comr for Refugees intervening) DD (Afghanistan) v Same (Same intervening)* [2012] UKSC 54 [25G]

[62] *Supra* as per A. Martyn (2002)

[63] United Nations General Assembly resolution 49/60 (1994) 'Declaration on Measures to Eliminate International Terrorism' A/Res/60/49

[64] B. Saul (2008) Defining "Terrorism" to Protect Human Rights, *Sydney Law School Legal Studies Research Paper* No. 08-125, p.1. See also, R. Jackson (2008) An Argument for Terrorism, *Perspectives on Terrorism* Vol. 2, No. 2, 1-12, 1

international agreements against terrorism'.[65] This is representative of the fact that terrorism is no longer simply a local problem, but an international issue requiring an international unified response. An example of the need to define terrorism, in line with other nation states, concerns the extradition of terrorists. For Ganor, extradition for political purposes is often expressly forbidden as per the many bilateral and multilateral agreements however; this can be achieved for the committing of a crime.[66] Whilst these are important aims, in practical terms the UK legal definition does nothing more than to clarify what actions and causes must be met for the UK executive to use in determining if an individual's actions amount to terrorism, and thereby seek prosecution, and the judiciary to then interpret and determine if the case before them amounts to terrorism.

The Terrorism Act 2000 was enacted specifically to provide some permanence to the counterterrorism structure and in order to combat the emerging international Islamist terror threat. This was identified by the research carried out by Lord Lloyd of Berwick working with an inquiry team, where the threat was highlighted as directly affecting the UK, given that many Islamist supporters were permitted direct entry into the UK through the means of asylum in the late 1980's and 90's.[67] Governmental scrutiny of applications was lacking at this time, simply

---

[65] B. Ganor (2002) Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? *Police Practice and Research: An International Journal*, 3:4, 287-304, 300

[66] B. Ganor, (2014) *Defining Terrorism: Is One Mans Terrorist Another Mans Freedom Fighter*? In D. Lowe, A. Turk, and D. K. Das, *Examining Political Violence: Studies of Terrorism, Counterterrorism and Internal War*, (CRC Press) pp18-19

[67] G. Joffe (2008) The European Union, Democracy and Counter-Terrorism in the Maghreb, *Journal of Common Market Studies* 46(1), 147-171, 155

because the UK's primary focus was directed towards Irish related terrorism.[68] Internationally, it became a well-known fact that Islamist supporters were free to openly fundraise for international terrorist groups and causes, which inevitably led French Intelligence to describe London as 'Londonistan', the international jihadist/Islamist hub.[69]

In addition to this emerging threat, the UK and the EU had fashioned multilateral agreements in a joint effort to combat it, recognising an international threat required an international response, and co-operation.[70] Commonwealth countries and the EU have all provided similar definitions of terrorism within their own legislative frameworks, highlighting this fact. Canada and Australia for example have the same causes, reflecting the international nature and response required to combat the terrorist threats. Although the UK's Terrorism Act 2000 is easily understood by policing and security agencies and the executive, and therefore could be said to serve its purpose well, it has been criticised for being too broad with terms undefined.[71] The words threat and influence, and the proliferation of potential causes represent the main contentious issues.

---

[68] R. S. Leiken (2005) Europe's Mujahideen: Where Mass Immigration Meets Global Terrorism, April 2005, *Center for Immigration Studies*, available at http://cis.org/EuropeMujahideen-ImmigrationTerrorism accessed 11th January 2016. See also Legislation Against Terrorism, A consultation paper (1998) The Stationary Office Cm 4178 at paragraph 4

[69] *Supra* as per R. Pantucci (2010) 253, and see also *Supra* as per S. Hewitt (2011) p.33

[70] A. Kaczorowska (2013) *European Union Law* (3rd Edition, Routledge) pp.17-21

[71] Lord Carlile of Berriew Q.C. (2007) Independent Reviewer of Terrorism Legislation, *The Definition of Terrorism,* March 2007, CM7052, p.22

The Causes

Dealing with the causes first, the idea of introducing more potential causes was fashioned by Lord Lloyd in his 1996 report titled 'Inquiry into Legislation Against Terrorism', commissioned by the UK Government of the time.[72] Lloyd's mandate was to assess the potential types of terrorist threats moving forward into the future, and to assess whether permanent counterterrorism legislation would be required, following at the time the potential peace settlement in Northern Ireland. Lloyd's research findings led him to conclude that as the Northern Ireland threat would decrease, a new emerging international Islamist threat would increase, rendering the then legal definition under section 20(1) of the Prevention of Terrorism (Temporary Provisions) Act 1989, inadequate. This definition read:

> …"terrorism" means the use of violence for political ends and includes any use of violence for the purpose of putting the public or any section of the public in fear.[73]

For Lloyd this definition was aimed solely towards dealing with the Irish related threat, and would therefore prove to be unsatisfactory, should a terrorist type act be carried out for a single-issue religious or ideological cause, rather than a straightforward political cause.[74] Ensuring that the legal definition of terrorism captures all terrorist activities, and taking inspiration from the US Federal Bureau of Investigations (FBI) definition of terrorism, Lloyd recommended social and

---

[72] The RT Hon Lord Lloyd of Berwick (1996) Inquiry into Legislation Against Terrorism, Volume One, The Stationary Office Cm3420, Chapter 5, paragraph 5.21

[73] Prevention of Terrorism (Temporary Provisions) Act 1989 and the Prevention of Terrorism (Additional Powers) Act 1996

[74] *Supra* as per The RT Hon Lord Lloyd of Berwick (1996) Chapter 5, paragraph 5.21, and Chapter 6, paragraph 6.13

ideological causes be introduced, in addition to a political cause.[75] The UK Government of the time largely agreed, but declined his recommendation for the inclusion of a social cause, opting for a religious cause instead, due to the breadth of non-terrorist style crimes it could capture, such as blackmail or extortion.[76] Conversely, the UK Government's response here is confusing for two reasons. Firstly it seems to imply a generalised terrorist crime exists despite there being no such general criminal offence of terrorism *per se*, and secondly why then include an ideological cause if a social cause was seen as too broad. After all there appears to be very little difference between the two terms. The impact of the proliferation of these causes is to broaden the definition of terrorism and ultimately serves to cast the net wider, encapsulating a broad range of behaviours.

Specifying the use or threat of action must be for a political, religious, racial or an ideological cause is not a unique approach to the UK. Countries within the Commonwealth have taken a similar approach. Canada for example covers the same causes apart from racial.[77] This is also seen in Australia where the Criminal Code 1995 was amended by the Security Legislation Amendment (Terrorism) Act 2002, meaning that the action must be taken for advancing a political, religious or ideological cause, aimed at influencing or intimidating a government, Australian

---

[75] *Ibid* at Appendix E Part 1

[76] *Supra* as per Legislation Against Terrorism (1998) 3.16 and 3.17

[77] See the Canadian Criminal Code R.S.C.1985, c. C-46, s83.01(1)(a) and (b)(i)(A) and (B). Code can be viewed http://laws-lois.justice.gc.ca/eng/acts/c-46/page-12.html#h-26

or foreign, or intimidating the public or a section of the public.[78] What is interesting is that the EU's approach differs from the UK and other Commonwealth nations, insofar as it does not include potential causes in their legal definition of terrorism, whereby specific types of actions that must be fulfilled to be determined as terrorist:

> …attacks upon a person's life which may cause death, attacks upon the physical integrity of a person, kidnapping or hostage taking, causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss, seizure of aircraft, ships or other means of public or goods transport, [the] manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons, release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life, interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life.[79]

It cannot be denied however, that the causes are a 'useful way of categorising non-state terrorist movements or group is by their political motivation: ethno-nationalist groups, for example Euzkadi Ta Askatasuna (ETA) in Spain, or ideological motivation, for example the Red Brigades in Germany whose aim was of creating a neo-communist state and socio-economic system'.[80] Wilkinson goes somewhat further than the law provides, submitting a more detailed academic typology of terrorism to encompass five types:

- Nationalist;
- Ideological;
- Religiopolitical;

---

[78] Criminal Code 1995, s 100.1(b) and (c)(i) and (c)(ii)

[79] *Ibid*

[80] *Supra* as per P. Wilkinson (2006) p.4

- Single-issue;
- State-sponsored and state-supported.[81]

Definition of causes

What does not help however, is the fact that the UK Government failed to offer an explicit definition of what these new causes actually mean, despite the fact that legal discourse and the rule of law demands clarity in order to ensure denotations are not used or interpreted interchangeably, thereby providing a safe and secure legal framework. It could be argued the causes were not defined for the very reason that it allows for the interpretation to change over time, allowing law enforcement and the UK courts a degree of flexibility when applying the law. Either way questions regarding the differences between religious and political, racial and ideological can therefore be legitimately raised.[82] As a direct result, the judiciary, applying normal rules of statutory interpretation have been afforded the task of providing a definition that for Walker has in turn occasioned malleable application. Rightly so it would appear dissemination by the courts turns on the practicality and evidence put forward, where the terrorist group is in essence placed into a category dependent upon the predominate cause.[83]

The Political Cause

An example of predominantly political terrorist groups are the various denotations and factions of the Irish Republican Army, who carried out many terrorist attacks

---

[81] P. Wilkinson (2000) Terrorism versus Democracy: The Liberal State Response (London: Frank Cass) pp. 19-21

[82] Nicholas Ryder (2007) A false sense of security? An analysis of legislative approaches towards the prevention of terrorist finance in the United States and the United Kingdom, *Journal of Business Law*, November, 821-850, 824

[83] *Supra* as per C. Walker (2009) p.10

on the British mainland during the Irish Troubles (1969-1997). Their aim was, and still is, to have the British Government relinquish their control over the six northern counties to the Dial in Dublin, unifying Ireland's 32 counties. The threat posed by republican dissident groups remains set at 'severe' in Northern Ireland, and 'substantial' for the UK mainland. The political cause element remained dominant, despite recorded religious intolerance and therefore proved adequate within the old definition of terrorism under the Prevention of Terrorism Act 1974 (PTA).[84] The political meaning has not been expressly altered by Parliament under section 1 of the Terrorism Act 2000, and as a result it appears that neither have the judicial approach to the term. It could be argued therefore, the judiciary could potentially widen the term rendering the additional causes redundant. This would serve to bring the law into line with Ganor's research findings, that terrorism is always political regardless of the underlying ideological or religious reasons.[85] Walker labours this point, arguing further that the UK definition of terrorism is overbroad and should focus on the chief cause of terrorist action, being political.[86] It is clear that the goal of terrorism is to effect political change,

---

[84] Irish related terror still remains a threat to the UK's mainland, evidenced by the increase in threat level set by the Joint Terrorism Analysis Centre and the Security Service (MI5), from moderate to substantial in May 2016 https://www.gov.uk/terrorism-national-emergency/terrorism-threat-levels accessed 31 May 2016. See also http://www.bbc.co.uk/news/uk-36267052 accessed 31 May 2016. See also 'Continuity IRA claims responsibility for Dublin boxing weigh-in shooting at Regency Hotel' 8 February 2016, http://www.belfasttelegraph.co.uk/news/republic-of-ireland/continuity-/-claims-responsibility-for-dublin-boxing-weighin-shooting-at-regency-hotel-34433366.html accessed 8 February 2016. For IRA/32CSM see http://www.belfasttelegraph.co.uk/news/republic-of-ireland/continuity-ira-claims-responsibility-for-dublin-boxing-weighin-shooting-at-regency-hotel-34433366.html accessed 8 February 2016

[85] B. Ganor (2014) *Defining Terrorism: Is One Mans Terrorist Another Mans Freedom Fighter?* In D. Lowe, A. Turk and D. K. Das, *Examining Political Violence: Studies of Terrorism, Counterterrorism and Internal War,* (CRC Press) p.12

[86] *Supra* as per C. Walker (2009) p.10

which may be underscored by an ideological or religious view.[87] Comay adds weight to this point proposing political terrorism is in fact always driven by social or ideological ambitions.[88] Ganor has contended the same position where he refers to a statement by Duvall and Stohl, in Schmid's book titled Political Terrorism:

> Motives are entirely irrelevant to the concept of political terrorism. Most analysts fail to recognise this and, hence, tend to discuss certain motives as logical or necessary aspects of terrorism. But they are not. At best, they are empirical regularities associated with terrorism. More often they simply confuse analyses.[89]

The concept of political cause is sufficiently broad, effectively removing the need for other causes.[90] When reviewing this area of law, Lloyd recognised this fact and in light of it discussed the possibility of retaining the definition under the PTA.[91] The UK Government in their response to Lloyd's recommendations illustrated this point, which begs the question as to why other causes were added in the first place:

> The Government notes that Irish, domestic, and international terrorist groups are driven by the same desire to achieve political change by violent means.[92]

---

[87] *Supra* as per B. Ganor (2014) p.12

[88] M. Comay (1976) Political Terrorism, *Mental Heath and Society*, 3, 249-261. See also: C. H. Simmons and J. R. Mitch (2001) Labeling Public Aggression: When Is It Terrorism? *The Journal of Social Psychology*, 125:2, 245-251, 246.

[89] A. P. Schmid (1984) Political Terrorism, SWIDOC, Amsterdam and Transaction Books, p.100. See also *Supra* as per B. Ganor (2002) 294

[90] B. Saul (2010) *Defining Terrorism in International Law,* (Oxford University Press) p.45. See also B. Xhelili (2012) Privacy & Terrorism Review: Where have we come in 10 years? *Journal of International Commercial Law and Technology*, 7(2), 121-135, 129

[91] *Supra* as per The RT Hon Lord Lloyd of Berwick (1996) Chapter 6, paragraph 6.13: Lord Lloyd stated, 'the existing definition in PTA section 20 "the use of violence for political ends…" could be retained, subject to the addition of the word "serious" before "violence", and an amplification of what is meant by "political ends"'.

[92] *Supra* as per Legislation Against Terrorism, A consultation paper (1998) at 3.6

The current reviewer of anti-terrorism legislation David Anderson suggested that the causes elements be 'trimmed', in order to render the definition more clear and precise.[93] Trimming the causes is not the same as removing the causes all together, a point illustrated here as it could render the definition of terrorism even more overbroad, applicable to almost any given criminal offence, unless of course the potential terrorist offences are specifically outlined.[94] It could be argued therefore, the additions of the religious and ideological cause along with the racial cause are unnecessary and problematic, since terrorism is always political.[95]

However, in contrast to this view, the UK is currently faced with a terror threat inspired by, and based upon a religious interpretation. Groups such as al-Qaeda and IS want to change the western world by implementing their religious interpretation and strict Sharia law. This does not sound entirely political and therefore the religious cause element is necessary to capture terrorist action taken under this cause.

Political or Religious Cause: The difference

The UK has a long and distinguished history in dealing with politically inspired terrorism. Religiously inspired terrorism is quite a different story, with the UK

---

[93] *Supra* as per D. Anderson (2014) p.81

[94] R *v Khawaja* [2006] 214 C.C.C. (3rd) 399. Canadian Criminal Code section 83.01(1)(b)(i)(A): the motive clause defines terrorist activity as 'an act or omission, in or outside Canada, that is committed in whole or in part for a political, religious or ideological purpose, objective or cause'. See also *Supra* as per C. Walker (2009) p.10. See also *Supra* as per D. Anderson (2014) p.81

[95] *Supra* as per B. Ganor (2014) p.12. See also discussion on religious tolerance and the rule of law in: Lord Bingham (2007) The Rule of Law, *Cambridge Law Journal*, 66(1), 67-85, 82

courts approach turning on evidential matters in determining the right cause.[96] It must be remembered that the judiciary can apply no real substantive tests because no definition of the causes exists within the Terrorism Act 2000. This was seen in *R (CC) v Commissioner of Police of the Metropolis and another* where Justice Collins refers to the causes listed under the Terrorism Act 2000.[97] The same can be said of all terrorism cases, where the judiciary illustrate this reliance.[98] In *R v G* and *R v J* the House of Lords heard evidence that J had in his possession a digital file containing a document entitled 'How Can I Train Myself for Jihad', '39 Ways to Serve and Participate in Jihad', and another called the 'Al Qaeda Training Manual'.[99] Similarly in *R v Zafar*, although much more complex, the fact remained the defendants 'were charged under section 57(1) of the 2000 Act, with possessing computer disks and hard drives containing extreme political and religious material', which the prosecution alleged 'were part of a settled plan to commit a terrorist act or acts in Pakistan'.[100] Academically, Schmid traces the courts difficulty in assessing whether the terrorist action was inspired by political or religious causes. He argues that, '…since terrorists generally challenge the monopoly of violence of the state and its ability to protect its citizens', terrorist acts obtain political significance even when the motivation for them is not

---

[96] *A and Others v Secretary of State for the Home Department* [2004] UKHL 56, [199]

[97] [2011] EWHC 3316, [3]

[98] See *Gillan and Quinton v United Kingdom* [2010] 50 E.H.R.R. 45, [28], and *R (on the application of Lord Carlile of Berriew QC and others) v Secretary of State for the Home Department* [2014] UKSC 60, [17], [118]

[99] [2009] UKHL 13, [26]-[27]

[100] [2008] 2 WLR 1013

primarily political but religious.'[101] Although the UK's Crown Prosecution Service charged *G* and *J*, and *Zafar* as having political and religious motivations, research shows that religious terrorism is inherently different from political.[102] Pantazis and Pemberton take the point further, mooting that terrorism inspired by a religious cause represents new terrorism and therefore new challenges, stating:

> The *new* terrorism can be differentiated in terms of different actors, motivations, aims, tactics and actions from the *old* twentieth-century concept of terrorism. For instance, the *new* terrorists are inspired by religious extremism and ethnic-separatism (rather than political or ideological causes) and are not predisposed to political negotiation...[103] [My emphasis]

The difference between religious and political causes is compounded when looking at this issue from a wider context. Research illustrates that in an exclusively religious context, a key feature of religious practices is the ritual of making sacrifices.[104] The impact of this line of thinking means that the terrorist attack and victimisation is often perceived by the terrorist as a legitimate sacrifice, in a positive sense, consisting of both attacking innocent citizens' viewed as the enemy, and the physical act of killing oneself and becoming a martyr.[105] Human rights violations are rationalised by, and invoked by, a divine law that supersedes

---

[101] A. P. Schmid (2004) Frameworks for Conceptualising Terrorism, *Terrorism and Political Violence*, 16:2, 197-221, 200

[102] A. Richards (2014) Conceptualizing Terrorism, *Studies in Conflict & Terrorism*, 37:3, 213-236, 225

[103] C. Pantazis and S. Pemberton (2009) From the "old" to the "new" suspect community: examining the impacts of recent UK counter-terrorist legislation, *British Journal of Criminology*, 49(5), 646-666, 650

[104] D. Young (1999) *Origins of the Sacred: The Ecstasies of Love and War* (New York: St. Martin's Press) p.208

[105] M. Juergensmeyer (2000) Terror in the Mind of God: The Global Rise of Religious Violence (University of California Press) p.167: 'The idea of martyrdom is an interesting one. It has a long history within various religious traditions, including early Christianity. Christ himself was a martyr, as was the founder of the Shiı´ Muslim tradition, Husain. The word martyr comes from a Greek term for 'witness', such as a witness to one's faith. In most cases, martyrdom is regarded not only as a testimony to the degree of one's commitment, but also as a performance of a religious act, specifically an act of self-sacrifice'.

man-made laws.[106] The French philosopher Blasé Pascal noted in the 16th century:

> Men never do evil so openly and contentedly as when they do it from religious conviction.[107]

The UK courts require substantive evidence in order to make their assessments. This is where information regarding the particular group(s) that the defendant is accused of having links with, or having been inspired by, become rather important. The IS terrorist group highlights the ambiguity inherent with the undefined terms, in assessing whether the group is political or religious.[108] Whilst predominantly religious and following their own extreme interpretation of Islam the group has evidenced some political aspirations having proclaimed a caliphate in June 2013 crossing the borders of Syria and Iraq.[109] IS appears to satisfy the additional factors needed to exist in order to fuse religion with political violence as laid out by Schmid.[110] Factually, the forming of a caliphate sets them apart from other terrorist groups who have a predominantly religious cause, such as al-

---

[106] A. H. Cook and M. O. Lounsbery (2011) Assessing the Risk Posed by Terrorist Groups: Identifying Motivating Factors and Threats, *Terrorism and Political Violence*, 23:5, 711-729, 724. See also Hazel Blears in the Counter-Terrorism and Security Bill, House of Commons 3rd sitting, 16 December 2014, Column 1312-1313

[107] R. S. Robins and J. M. Post (1997) *Political Paranoia: The Psychopolitics of Hatred* (New Haven, Yale University Press) p.144

[108] The so called 'Islamic State' is a Salafi Islamist group following an Islamist Wahhabi and Takfiri doctrine developed historically from Sunni Islam. See G. Kepel (2002) *Jihad: The Trail of Political Islam*, (Harvard University Press) pp.219-222. See also S. G. Jones (2014) A Persistent Threat: The Evolution of al-Qaiada and Other Salafi Jihadists, *RAND National Defense Research Institute* available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR637/RAND_RR637.pdf accessed 8 February 2016. See also M. Haider (2013) European Parliament identifies Wahabi and Salafi roots of global terrorism, available at http://www.dawn.com/news/1029713 accessed 8 February 2016

[109] See http://english.al-akhbar.com/node/20378 accessed 8 February 2016

[110] *Supra* as per A. P. Schmid (2004) 212

Qaeda, Jabhat Fatah al-Sham (formally called al-Nusra and aligned with al-Qaeda), and Al-Shabaab, who follow a similar extreme interpretation of Islam and enforcement of their religious beliefs through the implementation of Sharia Law.[111]

Although the religious cause was added in response to the rise in the international Islamist threat, its inclusion could now be questionable in light of greater understanding of the Islamic religion, and the fact that religion for many is very personal and subjective.[112] UK MP's Yasmin Qureshi and Dr Lewis advocated this particular point during the passing of the Counter-Terrorism and Security Act 2015.[113] Placing this highly contextual term into a piece of legislation is perhaps quite hazardous, especially when considering the UK Government's aim in prevention, and has been seen to damage community relations within the UK.[114] Since the 1990s it has been somewhat clear many Muslims perceive that they are treated as a suspect community and targeted by police due to their religion, and

---

[111] H. Mustapha (2014) The al-Nusra Front: From Formation to Dissension, Policy Analysis Series, *Arab Centre for Research and Policy Studies*, pp.3, 10, 14 and 20. See also: S. J. Schulhofer, T. R. Tyler and A. Z. Huq (2011) American Policing at a Crossroads: Unsustainable Policies and the Procedural Justice Alternative, *Journal of Criminal Law & Criminology*, Vol. 101, No. 2, 335-374, 369. The al-Nusra groups have now changed theor name to al-Sham, for further information see http://edition.cnn.com/2016/08/01/middleeast/al-nusra-rebranding-what-you-need-to-know/ accessed 5 December 2016

[112] R. Douglas (2010) Must terrorists act for a cause? The motivational requirement in definitions of terrorism in the United Kingdom, Canada, New Zealand and Australia, *Commonwealth Law Bulletin*, 36:2, 295-312, 303 (3.4). See also M. Elliott (2004) Parliamentary sovereignty and the new constitutional order: legislative freedom, political reality and convention, *Legal Studies* 22, 340-376, 322

[113] Counter-Terrorism and Security Bill, House of Commons Second Reading, 2 December 2014, Column 253 for Dr Lewis, and 2 December 2014: Column 262 for Yasmin Qureshi.

[114] Counter-Terrorism and Security Bill, House of Commons Second Reading, 2 December 2014, Column 263 as per Jeremy Corbyn MP. See also T. Choudhury and H. Fenwick, (2011) The impact of counter-terrorism measures on Muslim communities, *Equality and Human Rights Commission Research report 72*, Durham University, p.8

those few who commit terrorist actions, in the name of Islam.[115] It was in fact the early Prevent strategies under the UK's CONTEST policy that proved most divisive, raising these issues whereby the religious cause element was seen as commensurate with Islamophobia.[116] The extremism here was considered, and was violent extremism linked to Islamist ideology.[117] This made them feel discriminated against and demonised for the actions of a few terrorists, using the name of Islam incorrectly in their view, which in turn challenges integration and the creation of a British and European identity.[118] It has been suggested that this negatively impacts upon the positive nature of strong Muslim identity, offering empowerment and allowing them to challenge cultural practices within their own religion.[119] Although politically inspired rather than religiously, for Hillyard during the Irish Troubles many Irish Catholics and British born Catholics of Irish descent felt similarly discriminated against by UK counterterrorism legislation aimed at prevention.[120]

---

[115] *Ibid*

[116] D. Batty (2016) Prevent strategy 'sowing mistrust and fear in Muslim communities', The Guardian, 3 February 2016, available at https://www.theguardian.com/uk-news/2016/feb/03/prevent-strategy-sowing-mistrust-fear-muslim-communities accessed 5 December 2016

[117] See Countering International Terrorism: The United Kingdom's Strategy, HM Government July 2006, Cm 6888 at section 3. Although developed from 2003, the revised version was available from 2006

[118] *Supra* as per T. Choudhury and H. Fenwick, (2011) p.8. Also note despite this point being heavily questioned by the Chair, Keith Vaz, at the recent Home Affairs Select Committee hearing on Countering Extremism, Karim and Dad asserted that IS and other similar groups interpret the Quran into their own perverse ideology. They confirmed this ideology is under no circumstances to be regarded as religious, see Home Affairs Select Committee, Countering Extremism. Evidence heard from Zulfiqar Karim, Bradford Council for Mosques (18 Mosques), and Fazal Dad, Senior Imam, Abu Bakr Mosque, Bradford, 12 January 2016, BBC Parliament Channel viewed 19 February 2016. See also: https://sjiyad.wordpress.com/2014/07/24/7-reasons-why-daesh-are-not-muslim-actually-conflict-with-islam-and-go-against-the-quran/ accessed 8 February 2016

[119] J. S. Carpenter, M. Levitt and M. Jacobson (2009) Confronting the Ideology of Radical Extremism, *Journal of National Security Law & Policy*, Vol. 3:301-327, 322

[120] See P. Hillyard (1993) *Suspect Community: People's Experience of the Prevention of Terrorism Act in Britain* (Pluto Press)

In contrast Pantazis and Pemberton dispute there is any empirical evidence to suggest that the police are currently targeting individuals based needlessly on their religious identity.[121] Regardless however, the facts remain that IS and al-Qaeda have a religious foundation and ideology, and have recently been the main terrorist threat, hence why the UK's international terrorist threat level is 'severe', and as a result the figures show that from 2001 to 2010 there were 237 convictions in the UK for terrorist related activity, with 87 per cent of these citizens' being Muslim.[122]

Religious or Ideological Cause

The former UK Prime Minister David Cameron frequently stated that the IS group is not based on Islam, or Islamic, but on an extremist, Islamist ideology.[123] These Islamist groups are based on an extreme view of Sunni Islam, known as Salafi and Wahhabism. This political statement seems to fit with Neumann's theory

---

[121] C. Pantazis and S. Pemberton (2009) From the "old" to the "new" suspect community: examining the impacts of recent UK counter-terrorist legislation, *British Journal of Criminology*, 49(5), 646-666, 649

[122] *Supra* as per T. Choudhury and H. Fenwick (2011) p.75. See also I. Mandoza (2012) What's in a name: Challenging the word "Islamist", The Chicago Monitor, critical perspectives on mainstream media, available at http://chicagomonitor.com/2012/05/whats-in-a-name-challenging-the-word-islamist/ accessed 9 February 2016. See also P. Beinart (2015) What Does Obama Really Mean by 'Violent Extremism'? The Atlantic, available at http://www.theatlantic.com/international/archive/2015/02/obama-violent-extremism-radical-islam/385700/ accessed 9 February 2016. See also https://lawyerssecularsociety.wordpress.com/2015/05/01/is-there-really-any-difference-between-islam-and-islamism/ for debate on the terms used, Islam, Islamism, Islamic and Islamist, accessed 9 February 2016

[123] O. Crowcroft (2015) What's the correct name for the worlds most dangerous terrorists? International Business Times, available at http://www.ibtimes.co.uk/why-isis-hate-being-called-daesh-whats-correct-name-worlds-most-dangerous-terrorists-1531506 accessed 9 February 2016. See also http://www.dnaindia.com/world/report-isis-is-not-islamic-call-them-daesh-david-cameron-2151363 accessed 9 February 2016

surrounding radicalisation that two elements are always present.[124] Firstly there must be a grievance, usually rooted in political discontent, and secondly, an ideology.[125] Anderson provided evidence for this and relying on Neumann's theory, confirmed that a quarter of all terrorists currently serving custodial sentences in the UK are Muslim converts.[126] Perhaps then, they are not practicing religious beliefs at all, but rather an ideological belief founded from the religion, as suggested by Cameron's assertion. This potentially highlights a greater political understanding of the 21st Century terrorist threat and perhaps a move away from utilising the religious cause element. This emphasises the political value of the terrorist label. Rather than having definitive legal definitions for such phrases, politicians can effectively remove all references to either of them, or alter the meaning of the phrases to suit their particular needs at any given time, thereby applying them malleably.

Pantucci insinuates this by putting forward a rather negative argument that by adding a religious cause into the UK legal definition of terrorism, the Government can effectively decide who are good Muslims and who are bad, by their own engagement within the communities.[127] However, it could be argued that rather

---

[124] P. R. Neumann, opinion cited in M. Sedgwick (2010) The Concept of Radicalisation as a Source of Confusion, *Terrorism and Political Violence*, Vol. 22, No. 4, 480.

[125] A. P. Schmid (2013) Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review, International Centre for Counter-Terrorism-The Hague (ICCT), p.3

[126] Home Affairs Select Committee, Countering Extremism. Evidence heard from David Anderson QC, Independent Reviewer of Anti-Terrorism Legislation, 19 January 2016, BBC Parliament Channel viewed 19 February 2016

[127] R. Pantucci (2010) A contest to democracy? How the UK has responded to the current terrorist threat *Democratization* 17(2), 251-271, 262

than the negative viewpoint put forward here by Pantucci, it is simply a matter of UK law enforcement and the Government, making their way through a new threat that they did not entirely understand. In the early days of the Islamist threat UK policing and security agencies were learning about this new threat first hand, and serious questions required answering, such as who they were and what type of threat they pose.[128]

The ideological cause in particular is perhaps better referred to as a 'catch-all' cause. The problem here is the broadness of the term ideological that could potentially capture anything such as animal rights groups' activity, or anti-abortion groups, not normally associated with the 21st Century general understanding of terrorism.[129] During the drafting stages of the Terrorism Act 2000 Parliamentarians raised concerns with the inclusion of the ideological cause, where the then Home Secretary Jack Straw was questioned as to whether or not industrial strike action would amount to an act of terrorism, as per the definition, which was topical at the time given the UK fire fighters were on national strike.[130] Such action could have been perceived as influencing the Government for an ideological cause, to alter its policy on pay and working conditions and subsequently found to be endangering people's lives by withdrawing labour.[131]

---

[128] See https://www.mi5.gov.uk/the-rise-of-the-islamist-terrorist-threat and also https://www.theguardian.com/commentisfree/2016/apr/04/prevent-hate-muslims-schools-terrorism-teachers-reject accessed 3 December 2016

[129] *Supra* as per P. Wilkinson (2006) p.4

[130] *Supra* as per C. Walker (2009) at p.10

[131] *Ibid*

Although the Home Secretary unequivocally confirmed that although industrial action would be omitted from capture, this fact is not reflected in the legislation, despite his assurances the ideological cause was aimed at action by eco-terrorism, anti-abortion groups and animal liberation groups as per above. Without legislative certainty, it could be argued there is little in place to legitimately stop a successive government deeming such action as terrorist. Interestingly, industrial action has been expressly omitted from the legal definition of terrorism in Canada and Australia. In addition to omitting industrial action, the Canadian legal definition of terrorism does not include an act or omission committed during an armed conflict, as in accordance with customary international law, or the activities by military forces or a state in exercise of their duties, as discussed further below.[132]

The Causes and Freedom of Expression

There is perhaps little to deny the effectiveness of the causes element when looking into the terrorist offences introduced for example under sections 1 and 2 of the Terrorism Act 2006. Enacted in the aftermath of the 7th July London bombings in 2005, the provision were introduced to deal with religious extremist hate preachers and the sheer amount of extremist religious text available in print and online, that served to influence others to become terrorist. To this end section 1 criminalises the encouragement of terrorism and section 2 the distribution of

[132] *Ibid*

terrorist publications, which may inspire terrorist action.[133] In practice, this broadly phrased Act can then be used by policing and security agencies when differentiating between freedom of expression and expression that crosses the line into potential terrorist activity, when carrying out electronic communications data surveillance under an IPA authority.

Utilising this authority, if law enforcement, monitoring electronic communications data through the IPA authority, discovered for example a citizen planning to carry out attacks in the name of the Irish republican cause, then this may satisfy the political element. Likewise, if a person were to advocate serious violence with the aim of preserving animal rights by attempting to force the UK to keep the Hunting Act 2004 in place, this may raise law enforcements alarm when picking up electronic communications data, that could be seen as potentially terrorist acts, satisfying the ideological element.

This is further emphasised by the fact that the provisions in the Terrorism Act 2006 rely on the definition of terrorism under the Terrorism Act 2000, as raised prior to the enactment, in the Third Report of Session 2005–06 of the Joint Committee of the House of Lords and House of Commons on Human Rights.[134] The breadth of the Terrorism Act 2006 mixed together with the broad definition of terrorism raised serious concerns for the Committee where they found 'the

[133] These can be committed recklessly, which certainly has an impact on article 10 Freedom of expression under the European Convention of Human Rights.

[134] HL Paper 75-I, HC 561-I

creation of the offence of encouragement of terrorism defined as broadly as in section 1 of the Terrorism Act 2000 is to criminalise any expression of a view that armed resistance to a brutal or repressive anti-democratic regime might in certain circumstances be justifiable, even where such resistance consists of campaigns of sabotage against property, and specifically directed away from human casualties'.[135] The former Home Secretary, John Reid MP, admitted this was the effect of the offence, but went on to defend the scope saying:

> …there is nowhere in the world today where violence can be justified as a means of bringing about political change.[136]

Regardless however, the Committee remained concerned and called for urgent changes to the definition of terrorism, to be brought in line with the EU Council Framework Decision and the UN Security Council Resolution 1566, 'to avoid a high risk of such provisions being found to be incompatible with Article 10 ECHR freedom of expression and related Articles'.[137] Other low threshold parts to the definition of terrorism were pointed out to this regard, such as the phrase 'influence'.

Regardless of the scope, the 2006 Act has not been a huge success story for the UK, given there has only been a few convictions. This could be due to the high threshold of evidence required, and could also be in part because these types of terrorist activities take place on the Internet. Now that the IPA has been passed,

---

[135] *Ibid* at paragraph 12

[136] *Ibid*

[137] *Ibid,* In attempting to satisfy the Committee's concerns, the then Home Secretary announced Lord Carlile would undertake a review of the definition of terrorism.

the chances of law enforcement's alarm being raised by such behaviour are set to arguably increase exponentially. Testing whether or not the line into terrorist activity has been crossed, the IPA's bulk interception, bulk acquisition and bulk equipment interference powers, discussed in Chapter Three, will undoubtedly play a huge role in the 21st Century, in the digital age. This in turn could generate a surge in use of the Terrorism Act 2006.

The Threshold of Influence

The phrase influence is extraordinarily broad particularly when taken together with the ideological cause. The phrase does not fit comparatively with other jurisdictions, especially when the fact that protests and industrial actions are not expressly safeguarded under UK legislation.[138] Illustrative of the UK's ability to 'gold-plate' EU law and international law, utilising catchall phrasing of this nature has been criticised by Anderson, as setting the bar 'remarkably low'.[139] In Anderson's analysis, he draws on comparable definitions from the EU, Council of Europe, the UN, Commonwealth countries and the United States of America where the standard is set higher, substituting the word influence for 'compel,[140] unduly compel,[141] influence by intimidation,[142] coerce,[143] intimidate,[144] and

---

[138] See the Canadian Criminal Code R.S.C.1985, c. C-46, s83.01(1)(b)(ii)(E)

[139] *Supra* as per D. Anderson (2014) p.85

[140] Canadian Criminal Code R.S.C.1985, c. C-46

[141] Council Framework Decision on combating terrorism 2002/475/JHA

[142] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, section 2331, Part 1 Chapter 113B (ii) of the United States Code 18. However, when assessing domestic terrorism the threshold is lowered to 'influence the policy of a government', under Part 5B(ii).

[143] The Federal Bureau of Investigation's US Code of Federal Regulations, see http://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition accessed 14th October 2014

force'.[145] Lord Lloyd, in drawing inspiration from the USA Federal Bureau of Investigation's (FBI) definition suggested, 'to intimidate or coerce a government' should become the set standard.[146] In attempting to satisfy the concerns raised in the Third Report of Session 2005–06 of the Joint Committee of the House of Lords and House of Commons on Human Rights, the then Home Secretary John Reid MP announced Lord Carlile would undertake a review of the definition of terrorism. Carlile inevitably agreed with Lloyd and pressed the point in his 2007 report to the then Government:

> The existing law should be amended [to ensure] actions cease to fall within the definition of terrorism if intended *only to influence*… [My emphasis][147]

This made little difference in the end as John Reid defended the existing law in his reply to Carlile, explaining he did not see the use of the phrase influence as setting the bar too low. It would appear at least, that despite the reservations over this low threshold, not only advanced by the independent reviewers but also the judiciary and academic community, the Government are unwilling to change it.[148]

---

[144] *Ibid*

[145] *Supra* as per D. Anderson (2014) p.86

[146] *Supra* as per The RT Hon Lord Lloyd of Berwick (1996) Appendix E, Part 1. See also G. Joffe (2008) The European Union, Democracy and Counter-Terrorism in the Maghreb, *Journal of Common Market Studies* 46(1), 147-171, 155. The Federal Bureau of Investigation's US Code of Federal Regulations defines terrorism as,'...the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives'. The Federal Bureau of Investigation's US Code of Federal Regulations, see http://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition accessed 14th October 2014

[147] *Supra* as per Lord Carlile of Berriew Q.C. (2007) p.47

[148] *Supra* as per D. Anderson (2014) p.88

According to Anderson's findings, the rationale behind the unwillingness to raise the threshold to 'intimidate' for instance, is that the phrase itself removes the possibility of argumentation being raised surrounding whether or not the Government can actually be intimidated by terrorist actions or threat of actions.[149] An example of hostage taking was posed, whereby the release negotiated by the Government, or an international organisation, would come more readily within the ambit of influence, rather than intimidate.[150] Anderson was not swayed by this argument and in agreement it is suggested, the phrase 'unduly compel' should serve as 'influences' replacement. Considering that influencing the Government is the legitimate aim of all political activity, such as the recent strike action by junior doctors in 2016, it is unsafe for the UK Government to continue its use in counterterrorism legislation.[151] Interestingly, as to whether or not the Government can actually be intimidated or influenced, or indeed the life of the nation threatened merely by an act of terrorism was raised in *A and Others v Secretary of State for the Home Department* where Lord Hoffmann made it clear that citizens' lives are incomparable with the life of the nation:

> …its institutions and values, endure through generations…England is the same nation as it was at the time of the first Elizabeth or the Glorious Revolution. The [Spanish] Armada threatened to destroy the life of the nation, not by loss of life in battle, but by subjecting English institutions to the rule of Spain and the Inquisition. The same was true of the threat posed to the [UK] by Nazi Germany in the Second World War. This country, more than any other in the world, has an unbroken history of

---

[149] *Ibid*

[150] *Ibid*

[151] P. Crish (2016) Junior doctors' strikes will continue as minister plans to impose new contracts, CIPD available at: http://www.cipd.co.uk/pm/peoplemanagement/b/weblog/archive/2016/02/12/junior-doctors-39-strikes-will-continue-as-minister-plans-to-impose-new-contracts.aspx accessed 13 February 2016

> living for centuries under institutions and in accordance with values which show a recognisable continuity.[152]

The EU's approach certainly seems to raise the threshold. Article 1 of the EU Council Framework Decision on combating terrorism provides that terrorism includes:

1. seriously intimidating a population; or
2. unduly compelling a Government or international organisation to perform or abstain from performing any act; or
3. seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.[153]

The actions that amount to terrorism are extremely similar to the UK and Commonwealth countries.[154] The phrases used however, appear to raise the threshold in terms of what aims amount to terrorism. As opposed to the UK's 'intimidate the public' and 'influence a government', the EU's model stipulates that the action must 'seriously intimidate a population' and 'unduly compel a government'.[155]

Taking the additional specified actions as per above, this is a much more thorough definition. Conversely, no counterterrorism legislation existed in the EU prior to al-Qaeda's terrorist attacks on the 11th September 2001 on the US. In conjunction

---

[152] *A and Others v Secretary of State for the Home Department* [2004] UKHL 56, [91]

[153] *Supra* as per EU Council Framework Decision, (2002/475/JHA)

[154] *Ibid*

[155] *Ibid*

with this attack, the fact that many EU Member States had no specific counterterrorism legislation led the EU to respond by introducing the framework decision as per above.[156] The purpose was to ensure Member States responded to the transnational threat and to enable co-operation between them supported by EU policy programmes.[157] The then EU's Justice and Home Affairs Council confirmed that the protection of the lives and property of its citizens', within the area of citizenship, freedom, security and justice, is the core task providing legitimacy to extensive public powers and policies, where EU citizens' expect EU action protecting their health and safety.[158]

Canada use similar language in their approach to defining terrorism where section 83.01(1) and (b) of the Canadian Criminal Code defines terrorism as:

> …as an act or an omission, inside or outside Canada that is committed for a political, religious or ideological objective or cause, and with the intention of *intimidating* the public or a segment of the public, or *compelling* a person, government or organisation to do or to refrain from doing any act, whether inside or outside of Canada.[159] [My emphasis]

This definition is perhaps a little easier on the eye providing a more everyday style of language, however, although the 'compelling' element raises the threshold, the addition of 'person' arguably does not. The UK specifies that

---

[156] C. C. Murphy (2015) *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law*, (Oxford: Hart Publishing) p.17

[157] Commission (EC) (2007) Report from the Commission based on Art 11 of the Council Framework decision of 13 June 2002 on combatting terrorism, Brussels, COM(2007)681 6th November 2007, p.10

[158] Council of the European Communities (2005) Communication from the Commission to the Council and the European Parliament Brussels COM(2005)124 6th April 2005, p.2. See also Council of the European Union (2005a) The European Union Counter-terrorism Strategy 14469/4/05 30th November 2005

[159] See the Canadian Criminal Code R.S.C.1985, c. C-46, s83.01(1)(a) and (b)(i)(A) and (B). See also R. Douglas (2010) Must terrorists act for a cause? The motivational requirement in definitions of terrorism in the United Kingdom, Canada, New Zealand and Australia, *Commonwealth Law Bulletin* 36(2), 295-312, 295

'serious' violence is required, against mere 'violence' here, albeit that intentionally:

> …causes death or serious bodily harm to a person, endangers a person's life, causes a serious risk to the health or safety of the public or any segment of the public, causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or, causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in conduct referred to in any of clauses (A) to (C).[160]

The Canadian definition explicitly includes:

> conspiracy, attempt or threat to commit any such act or *omission*, or being an accessory after the fact or counselling in relation to any such act or omission.[161] [My emphasis]

The Australian definition is also similar in approach, where the Criminal Code 1995 was amended by the Security Legislation Amendment (Terrorism) Act 2002, meaning that the action must be taken for advancing a political, religious or ideological cause, aimed at influencing or intimidating a government Australian or foreign, or intimidating the public or a section of the public.[162] The Australian legislation, similar to the Canadian model also omits action taken by way of protest, dissent or industrial action.[163]

Serving to lower the UK's threshold further and effectively remove the necessity for an action to influence the Government or international organisation is section

---

[160] See the Canadian Criminal Code R.S.C.1985, c. C-46, s83.01(1)(a) and (b)(i)(A) and (B), (ii)(A) to (E)

[161] *Ibid*

[162] Criminal Code 1995, s 100.1(b) and (c)(i) and (c)(ii)

[163] Criminal Code 1995, s 100.3(a)

1(3) of the Terrorism Act 2000 that contains an exclusory provision for the use of firearms and explosives.[164] The UK's definition of terrorism thus changes to:

> …the use or threat of action, involving firearms or explosives, made for the purpose of advancing a political, religious, racial or ideological cause.

At first, one might question the importance of this provision; given the obviousness that such destructive methods and action must be terrorism. It is argued however, this serves to over-complicate the definition of terrorism, as it is irrelevant and unnecessary given that such action would most certainly serve to intimidate the public, or section of the public in any regard.[165] Similar to the proliferation of causes, it simply adds further convolution to an already complex definition, unnecessarily stretching the applicability of the terrorist label.[166] As an example should a citizen decide to threaten (i.e. the use or threat of action) a bank manager with a firearm (i.e. involving firearms or explosives), for the purposes of having the bank cancel all existing debt of all local citizens' (i.e. made for the purpose of advancing and ideological cause), the terrorist label here could potentially be ascribed. Thus one could argue the provision removes the triadic nature of terrorism, thereby supporting Hacker's earlier assertion that the terrorist label could move to the dyadic.[167]

---

[164] Terrorism Act 2000, s 1(1)(b)

[165] R. English (2010) *Terrorism: How to Respond*, (Oxford University Press) p.4

[166] *Supra* as per C. H. Simmons and J. R. Mitch (2001) at 246. See also *Ibid* at p.90

[167] *Supra* as per F. J. Hacker (1980) 143-159

Anderson would disagree that this provision unnecessary stretches the applicability of the label however, as he confirms that although the significance of this provision may be small, to effectively remove the target provision, would directly counter the intention of the Terrorism Act 2000.[168] Regardless, he did go on to recommend the removal of this provision in his 2014 report, noting he was not swayed by the argument put forward by the then Home Secretary Charles Clarke:

> … [section 1(3)]…is to cover for instance, an assassination in which the terrorist's motive might be less to put the public in fear, or to influence the Government, than to 'take out' the individual…[169]

Anderson further explains that there is no reason as to why such action should be seen as terrorism, and not simply murder. Critically, he appears to have overlooked the fact that this provision fits within, the rather historical rationale used by the international community in attempting to define an act of terrorism.

EXTRA-JURISDICTIONAL EFFECT OF UK LAW: AN INTERNATIONAL THREAT NEEDS AN INTERNATIONAL RESPONSE

The similarity between the legal definitions of terrorism between nation states within the Commonwealth and the EU illustrate the international nature of the 21st Century terrorism threat and the fact that international security is as important as

[168] *Supra* as per D. Anderson (2014) p.89

[169] *Ibid*

national security.[170] Put plainly, 21st Century terrorists know no borders, rendering such provisions essential within the guise of international cooperation.[171] This legal similarity is pertinent when the policing and security services are monitoring electronic communications data between members of the same group communicating in different parts of the world, for example UK IS fighters in Iraq communicating with UK IS members encouraging or planning attacks in the UK.

To this end and similar to other nation states, an extra-jurisdictional approach is introduced by way of section 1(4) of the Terrorism Act 2000, stating that an act of terrorism applies to one committed or planned in any state in the world, not just the UK. The definition of government came under judicial scrutiny in *R v F* and *R v Gul*, where the UK Court of Appeal held that the phrase was not restricted to representative or democratic governments, applying to all countries, additionally and controversially, to those governed by tyrants and dictators.[172] It may be the case that the apprehension of the UK being known internationally as a safe haven for terrorists and supporters, made its way from Parliamentarians to the judiciary.[173] Focusing on *Gul*, his appeal against conviction for terrorist offences was based on a number of factors. Overall *Gul's* legal argument turned on his

---

[170] *Supra* as per The RT Hon Lord Lloyd of Berwick (1996) Chapter 2 paragraph 2.4

[171] *Ibid*

[172] *R v F* [2007] EWCA Crim 243, [9], [16], and *R v Gul* [2012] EWCA Crim 280, [23], [51], and *R v Gul* [2013] UKSC 64, [42], and the Terrorism Act 2000 s 1(4)(d), '…"the government" means the government of the United Kingdom, of a Part of the United Kingdom, or a country other than the United Kingdom'

[173] *R v F* [2007] EWCA Crim 243, [16] and *R v Gul* [2012] EWCA Crim 280 [51]

assertion that section 1 of the Terrorism Act 2000 was too broad given its inheritance:

1. The Terrorism Act 2000 intended to give effect to the UK's international treaty obligations and the concept of terrorism in international law does not extend to military attacks by a non-state armed group against state, or inter-governmental organisation, armed forces in the context of a non-international armed conflict, and that this limitation should be implied into the definition in section 1;
2. Rather closely connected, the second argument was based on the fact that it would be wrong to read the Terrorism Acts of 2000 or 2006 as criminalising in the UK an act abroad, unless that act would be regarded as criminal by international law norms;
3. The third argument raised by the appellant was that some qualifications must be read into the very wide words of section 1 of the Terrorism Act 2000.[174]

Unlike comparative nation states, the UK does not omit action taken during an international armed conflict. The first argument therefore is largely correct. The International Convention for the Suppression of Terrorist Bombings in 1997 and the International Convention for the Suppression of the Financing of Terrorism in 1999 excludes attacks by insurgents on military forces during non-international armed conflicts.[175] Additionally the 1977 Additional Protocol I to the 1949 Geneva Conventions (protection is afforded within Article 14 of the UN Charter) relate to international armed conflict, which has the effect of somewhat, indemnifying insurgents fighting against occupation in exercising self-determination during international armed conflicts.[176]

---

[174] [2012] UKSC 64, [24]

[175] [2012] UKSC 64, [52], See also Terrorism Act 2000 ss 62-64 that formed the basis of *Gul's* argument, that the Terrorism Act 2000 and by extension the Terrorism Act 2006 should conform to the international norm, given they were enacted under the UK's international obligations. The second part focused on the criminalisation of terrorist actions being more comprehensive and wider in the UK than required by international norms, [2013] UKSC 64, [43], and *R v Gul* [2012] EWCA Crim 280, [19](i)(ii)

[176] *R v Gul* [2012] EWCA Crim 280, [28]

It interesting to note that despite previous international attempts at creating a definition of terrorism, the UN General Assembly in 2012 could still not agree on the differences between terrorism and a 'legitimate struggle of peoples fighting in the exercise of their right to self-determination'.[177] For McKeever it is naturally difficult to reconcile, 'both the general abhorrence for violence which is indiscriminate and/or actively targets civilians, with the acknowledgment that some forms of political oppression may be so unjust as to legitimate violent action by the oppressed'.[178] In order to deal with the freedom fighter conundrum and to secure an effective move forward, the International Community has attempted to focus on the wrongful nature of terrorism, rather than on the intent.[179] As a result subsequent conventions have all adopted an operational definition of a specific type of terrorist act, without referring to underlying motivational aspects, or causes, be it for political or ideological purposes.[180] The primary focus is concentrated on non-state actors adopting a criminal law enforcement model to address the problem, with emphasis on increasing global co-operation.[181]

---

[177] *R v Gul* [2013] UKSC 64, [45]-[47]

[178] *Supra* as per D. McKeever (2010) 114

[179] A. Gioia (2006) *The UN Conventions on the Prevention and Suppression of International Terrorism,* in G. Nesi, ed., *International Cooperation in Counter-terrorism: The United Nations And Regional Organizations in the Fight Against Terrorism*, (Ashgate) p.4

[180] A. Byrnes (2002) Apocalyptic Visions and the Law: The Legacy of September 11, *a professorial address by Byrnes at the ANU Law School for the Faculty's 'Inaugural and Valedictory Lecture Series'.*

[181] *Ibid*

Returning to the UK, the Supreme Court rejected the idea of judicial intervention that would effectively serve to introduce legislative change allowing for some sort of freedom fighter exclusion.[182] The Court decided that the nature of the broad definition was known to Parliament prior to enactment and have had the opportunity to revisit it, as a result of the various independent reviewers of anti-terrorism legislation conclusions and recommendations.[183] Another important point is that the UK's legislative measures and the judicial response may have been different if the EU Council's Framework Decision in 2002 contained similar freedom fighter type exclusions. Regardless, as accepted by the Supreme Court, the UK Parliament is supreme and able to legislate on any matters it chooses.

In his analysis written prior to the UK Supreme Court's findings, Coco supports *Gul's* argumentation and raises some important issues, proposing the UK Court of Appeal should have interpreted the UK domestic legislation in light of current international frameworks.[184] However, his analysis appears to fall on the pretence that the UK Parliament cannot gold-plate international law and that UK courts, although not requested to do so in this case, can question the validity of Acts of Parliament. Theory surrounding UK Parliamentary Sovereignty suggests the UK Parliament is capable of gold-plating and constructing law on any matter it

[182] [2013] UKSC 64, [33]-[38]

[183] *Ibid*, [39]

[184] A. Coco (2013) The Mark of Cain, *Journal of International Criminal Justice* 11(2), 425

chooses.[185] It is important to note the capability of the UK Parliament, in creating unfettered extra-territorial provisions.[186] This has been seen in other types of statues, such as section 72 of the Sexual Offences Act 2003 and section 1 of the War Damages Act 1965.[187] The only time an Act of Parliament may be challenged by the courts is if the legal matter in question relates to an EU provision, or the UK statute contravenes the European Convention on Human Rights as per the Human Rights Act 1998.[188]

Unlike other comparative jurisdiction there is no defence in the UK, freedom fighter style or otherwise available for an accused to use within the terms under the Terrorism Act 2000, which does not exempt what could be termed 'terrorism in a just cause'.[189] The Canadian judiciary in *R v Khawaja* tested the Canadians armed conflict exclusion, where *K* claimed that the situation in Afghanistan since 2002 represented a war within the legal definition and therefore his actions were carried out during an armed conflict and in accordance with international law.[190] However, because K's actions involved acts of violence in the UK and Pakistan, and were based on a violent Islamist ideology, the Court found his actions went beyond the Afghanistan conflict. The Court also held the conflict in Afghanistan

---

[185] *R v Gul* [2012] UKSC 64, [53]. See also K. Syrett (2011) *The Foundations of Public Law, Principles and Problems of Power in the British Constitution* (Palgrave Macmillan) p.100, 'Gold-plating' is the exercise that refers to the UK government legislating further than is required by international law.

[186] *R v Gul* [2012] EWCA Crim 280, [56], and *R v Gul* [2013] UKSC 64

[187] *Madzimbamuto v Lardber-Burke* [1969] 1 AC 645, [723], See also *Supra* as per K. Syrett (2011) p.104

[188] See *Mccartys Ltd. v Smith* [1980] ECR 1275 (Case 129/79) for EU law, and see *Gillan v UK* [2010] 50 EHRR 45 (4158/05) (ECHR) for European Convention on Human Rights

[189] *Ibid*, [27]. See also *Supra* as per D. McKeever (2010) 113

[190] [2012] SCC69, [2012] 3 S.C.R. 555

represented an armed insurrection carried out based on violent jihad against the newly appointed Afghan government, and non-Islamic regimes and civilians.[191]

This illustrates that even when a state has a freedom fighter style defence, the tests applied by the judicial authority appear to be stringent and protective of maintaining the status quo. This fits with Netanyahu postulation that freedom fighters are in fact not capable of perpetrating terrorist acts:

> For in contrast to the terrorist, no freedom fighter has ever deliberately attacked innocents. He has never deliberately killed small children, or passers-by in the street, or foreign visitors, or other civilians who happen to reside in the area of conflict or are merely associated ethnically or religiously with the people of that area…The conclusion we must draw from all this is evident. Far from being a bearer of freedom, the terrorist is the carrier of oppression and enslavement.[192]

The facts discussed in *Gul* however, highlight that even if a freedom fighter exclusion did exist within the UK's legislative framework, it would have made little difference to the outcome. It also suggests the unimportance of the UK Court seeking advice as to whether or not the conflicts were to be regarded as an international armed conflict, given *Gul* posted a video containing not only attacks on Coalition forces, but also civilians that were in the US twin towers on 11th September 2001 at the time of al-Qaeda's attack. It also included other attacks on civilians and excerpts from martyrdom videos with symbols associated with proscribed organisations listed under Schedule 2 of the 2000 Act.[193]

---

[191] *Ibid*, [100], [102]

[192] B. Netanyahu (1985) *Terrorism: How the West Can Win*. (Farrar, Strauss and Giroux, New York) p.27

[193] *R v Gul* [2012] EWCA Crim 280, [6], [20](1)(2). See also Terrorism Act 2000, s 3(1)(a) and Schedule 2

Despite these facts the Court thought the need to elucidate further, confirming international law had developed insofar as criminalising terrorism in times of peace.[194] International Humanitarian Law and International Criminal Law specifically refer to civilians and organised groups within their definition, and cover acts of terrorism during an international armed conflict.[195] Defining terrorism as an act carried out primarily against civilians, international rules such as those provided by article 33(1) of the Fourth Geneva Convention, effectively ban terrorism, with other conventions considering it to be a war crime.[196] What is clear from the UK court's decision in not allowing a freedom fighter defence, is finding it unpalatable the idea of branding some types of terrorism as officially acceptable:

> …acts by insurgents against the armed forces of a state anywhere in the world which seek to influence a government…made for political purposes are terrorism. There is no exemption for those engaged in an armed insurrection and an armed struggle against a government.[197]

Whilst this statement may add some weight to Coco's argument, it certainly seems to suggest the courts have universal jurisdiction over terrorism.[198] In responding to such criticism, the UK Court of Appeal relied on the *Lotus* case presided over by the Permanent Court of International Justice, affirming that its

---

[194] *Ibid*, [33]

[195] A. Cassese (2008) *International Criminal Law* (2nd Edition, Oxford University Press) p.171

[196] Fourth Geneva Convention 1949: 'terrorist acts are prohibited if perpetrated by civilians or organised groups in occupied territories or in the territory of a party to the conflict'. See also: Second Additional Protocol 1977, article 4(1), 4(2)(d), 13(2), 51(2). See also *Ibid* pp.171-173

[197] *R v Gul* [2012] EWCA Crim 280, [16]

[198] *Supra* as per A. Coco (2013)

jurisdiction was not questionable given the lack of explicit prohibitions against labelling as terrorists, non-state armed groups attacks on state armed forces, in non-international armed conflicts.[199]

Furthermore, although the evidence given by the former UK Foreign Secretary confirming the conflicts in Afghanistan and Iraq during 2008 and 2009 were regarded as non-international armed conflicts, thereby rendering *Gul's* argument weightless, the impact of the judicial decision reinforces the UK's Governments commitment to the international effort to combat terrorism and serves to prevent individuals from planning action to take place on foreign soil from the UK.[200] This mirrors the approach taken by the UK Government at the time of drafting the Terrorism Act 2000. Seeking to protect foreign governments from terrorism planned and organised in the UK was supplementary reinforced by the Crime (International Co-operation) Act 2003 that confirms a resident in the UK would be guilty of an offence if actions abroad would constitute an offence within the UK under the Terrorism Act 2000.[201] It would be interesting to see where the UK Government would stand should a citizen return from fighting in Syria or Iraq with Kurdish forces against IS, given this has not been recognised as an

---

[199] *S. S. Lotus (France v Turkey)* [1927] PCIJ Series A, No 10, [44], and *R v Gul* [2012] EWCA Crim 280, [47]-[49]

[200] *R v F* [2007] EWCA Crim 243, [9], [16], and *R v Gul* [2012] EWCA Crim 280, [20], [23], [28], [51], and *R v Gul* [2013] UKSC 64. See also A. Murray (2012) Acts of was or acts of terrorism? Case Comment, *Journal of Criminal Law,* 76(4), 298-302, 299

[201] Crime (International Co-operation) Act 2003, s 63A-E. Terrorism Act 2000 ss 54, 56-61.

international armed conflict.[202] At the time of writing many UK citizens' are fighting alongside Kurdish forces, who are currently battling for Mosul against IS's stronghold.[203] For some States, such as Turkey, the British citizens' fighting with the YPG (or People's Protection Units) are classed as terrorists, but in the UK they are not.[204] This is entirely dependent upon which group or organisation citizens' join. For example in relation to Turkey who has been in conflict with the Kurdish group the PKK, where the PKK are looking for independence of Kurdish territory from Turkey, under section 3 and Schedule 2 of the Terrorism Act 2000 the PKK are a proscribed group in the UK. As such they are seen as a terrorist organisation, yet the YPG and YPJ in Syria, which are the army factions of the Syrian Kurds currently fighting IS and the al-Assad regime are not proscribed, and as such any UK citizen that joins the YPG/YPJ would not be deemed to be a terrorist and neither are the actions of this group seen as terrorist action in the UK.[205]

---

[202] E. Saner (2015) Brits abroad: is it against the law to fight ISIS? The Guardian, 25 February 2015, available at https://www.theguardian.com/world/shortcuts/2015/feb/25/brits-abroad-against-law-fight-isis accessed 5 December 2016

[203] See http://www.bbc.co.uk/news/world-middle-east-33083213 and http://www.bbc.co.uk/news/world-middle-east-33083256 accessed 5 December 2016

[204] S. Sharma and A. MacDonald (2016) British volunteers in Syrian Kurd forces are 'terrorists', Turkey says. Middle East Eye, 1 September 2016, available at http://www.middleeasteye.net/news/turkey-british-ypg-terrorist-syria-874419624 accessed 5 December 2016. See also I. Drury (2015) Public schoolboy who quit City to fight ISIS returns home: Briton who spent five months alongside Kurdish forces says he can justify actions if questioned by police, Mail Online, 10 June 2015, available at http://www.dailymail.co.uk/news/article-3119071/ISIS-fighting-city-trader-returns-home-UK.html accessed 5 December 2016

[205] For current list of UK proscribed organisations: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/578385/201612_Proscription.pdf. See also C. Davies (2015) Girl becomes first Briton convicted of trying to join fight against Islamic State in Syria, The Guardian, 20 November 2015, available at https://www.theguardian.com/uk-news/2015/nov/20/girl-becomes-first-briton-convicted-of-trying-to-join-fight-against-islamic-state-in-syria and http://thekurdishproject.org/history-and-culture/kurdish-nationalism/pkk-kurdistan-workers-party/ accessed 30 December 2016. See also M. Blake (2017) Blackburn activisty becomes first British woman to join fight against

Turkey on the other hand, sees the YPG/YPJ as simply PKK factions and classes them also as terrorist. However, the YPG/YPJ is not a proscribed group in the UK, therefore fighting with them is not deemed to be terrorist action, despite Turkey's position on this subject.

Concerns with regards the lack of a provision allowing a freedom fighter style defence were actually raised during the debating stages of the Terrorism Act 2000, whereby Parliamentarians focused on the proposed vagueness surrounding the terms used, and whether such a provision would have unfairly criminalised modern equivalents of the Suffragettes or the South African opponents of the apartheid.[206] Sir Igor Judge in *R v F* appeared to have proffered caution in not permitting some defence typology:

> The call of resistance to tyranny and invasion evokes an echoing response down the ages. We note, as a matter of historical knowledge, that many of those whose violent activities in support of national independence or freedom from oppression, who were once described as terrorists, are now honoured as 'freedom fighters'.[207]

Although acknowledging this, the Court held, '…terrorism is terrorism, whatever the motives of the perpetrators'.[208] Igor Judge's statement was unsurprisingly rejected by the Government, which led Lord Carlile, the then independent

---

ISIS in Syria, The Guardian, available at https://www.theguardian.com/uk-news/2017/feb/09/blackburn-activist-kimberly-taylor-becomes-first-british-woman-join-fight-isis-syria accessed 14 February 2017.

[206] A. W. Bradley and K. D. Ewing (2011) *Constitutional and Administrative Law*, (15th Edition, Pearson Education Ltd) p.590. See also C. Walker (2008) Terrorism: Terrorism Act 2000 ss. 1 and 58 – possession of terrorist documents, Case Comment, *Criminal Law Review* [2008] 160-165, 162. Suffragettes were members of women's organisations in the late 19th and early 20th century that advocated the extension of the "franchise", or the right to vote in public elections, to women.

[207] *R v F* [2007] EWCA Crim 243, [9]

[208] *Ibid*, [9] and [27]

reviewer of anti-terrorism legislation in 2007, to advocate a form of statutory obligation that required the executive look into the nature and target of the action, and towards international legal obligations, prior to the instigation of criminal charges.[209] Walker proffers a rather scathing view for not creating or allowing a type of freedom fighter defence or exception where he states:

> …an antidote to the trend that the UK Government values friendship with oil-owning despots much more highly that the political freedom exercised by refugee underdogs.[210]

Despite the international conventions, the UK Court of Appeal drew attention to the fact that no internationally agreed definition of terrorism exists. Although re-visited in 2002 and 2004 by the Member States of the UN, the impasse in the negotiations surrounded whether such a definition would be applicable to the armed forces of a state (state terrorism) and to liberation movements (freedom fighters).[211] Focusing on the latter point, domestically this provides a problem as expressed by the UK judiciary above, because should violent action or the threat of action by persons engaged in armed conflict overseas be distinguished, it would no longer constitute terrorism.[212] The UK judiciary have shown that although deliberate targeting of civilians is prohibited by International Humanitarian Law and could constitute a war crime, such prosecutions are highly

---

[209] *Supra* as per Lord Carlile of Berriew Q.C. (2007) paragraph 58

[210] *Supra* as per C. Walker (2008) 165

[211] T, Deen, (2005) U.N. Member States Struggle to Define Terrorism, Inter Press Service, see http://www.ipsnews.net/2005/07/politics-un-member-states-struggle-to-define-terrorism/ accessed 2 September 2015

[212] *R v Gul* [2012] EWCA Crim 280, [23], and *R v Gul* [2013] UKSC 64, [42]

unusual.[213] The UK Court of Appeals decision follows such concern, where it was held that the conflicts in Afghanistan and Iraq were both regarded as non-international armed conflicts, thereby removing the possibility of a claim for combatant immunity for legitimate insurgency.

UK DISCRETIONARY POWER TO PROSECUTE

Perhaps providing some reprieve from the over broad definition of terrorism, the executive functions are able to offer some moderation, prior to formal charges being brought. Under section 117 of the Terrorism Act 2000, prior to the instigation of proceedings the consent of the Director of Public Prosecutions (DPP) is required.[214] However, allowing discretionary power to the DPP was criticised by the UK Supreme Court in *R v Gul*, as 'intrinsically unattractive' amounting to the legislature abdicating prosecutorial powers to an unelected, albeit respected and independent lawyer.[215] The Court focused on the risk of undermining the rule of law given that although the DPP is accountable to Parliament, open and democratically accountable decisions are not made in same manner and form as those in Parliament.[216] It must be mentioned however, that

[213] *Supra* as per D. Anderson (2014) p.26

[214] Terrorism Act 2000, s 117(2)(a)

[215] *R v Gul* [2013] UKSC 64, [35]-[36]

[216] *Ibid*

other areas of UK criminal law have wide definitions that are moderated by the DPP. In fact this appears to work reasonably well.[217]

The Sexual Offences Act 2003 serves to provide such an example whereby consent to sexual activity for persons under 16 was removed by way of section 4.[218] Therefore, two persons both under the age of 16 would effectively be guilty of committing an offence given they are unable to legally consent.[219] Following a similar trend in reassuring Parliamentarians that the term 'ideological' would not extend to industrial action under the 2000 Act, the then Home Secretary made it clear that charges would not be brought against children under 16 who engaged in consensual sexual activity.[220] The ambiguity of this statement is quite staggering but beyond the ambit of this discussion. This has since led the Crown Prosecution Service guidance to emphasis, 'it was not Parliaments intention to punish children unnecessarily.'[221] This type of safeguarding power could also be utilised to narrow the denotation of 'Government' within the definition of terrorism, to allow, at least at some level, a freedom fighter exclusion.

Given the extremely broad nature of the Terrorism Act 2000, it is argued that without this safeguard the law could potentially be used inappropriately. It is

---

[217] Such as the Sexual Offences Act 2003

[218] See http://www.cps.gov.uk/legal/p_to_r/rape_and_sexual_offences/consent/ accessed 19 January 2016

[219] D. Ormerod (2008) *Smith and Hogan Criminal Law* (12th Edition, Oxford University Press) pp.706-708

[220] *Ibid*

[221] *Supra* as per http://www.cps.gov.uk/legal/p_to_r/rape_and_sexual_offences/consent/ accessed 19 January 2016

further contended that although the DPP safeguard is useful, it does not replace legislative certainty.

POLITICAL VALUE OF TERRORISM

The impact of this lack of legislative certainty is realised, where political influence and the political value of the terrorism, currently prevails over its legal one making its use difficult in legal discourse.[222] Internationally and arguably domestically, left to its political meaning terrorism can change substantially to suit the interests of a particular state and government at a particular time.[223] For this reason it is argued the law should prevail and provide a clear and precise legal position, denying terrorism its political currency built upon historical attachments.[224] For Gale, the lack of precision mitigates against due process of law', whereby the law should be as precise and foreseeable as possible as held in *Steel and others v United Kingdom,* and*, Hashman and Harrup v United Kingdom*.[225] This is perhaps more prevalent within the international arena where the issue of an objective legal definition is compounded by the fact there are two

---

[222] S. Zeidan (2004) Desperately Seeking Definition: The International Community's Quest for Identifying the Specter of Terrorism, *Cornell International Law Journal*, Volume 36, Issue 3, Article 5, 491-496, 491-492. See also: *Supra* as per B. Saul (2006) at p.3

[223] *Ibid*

[224] The political value can be seen historically during the Peninsula Wars of 1809-1813, evidenced more recently where the Taliban and Osama bin Laden represented the US in Afghanistan, seen as President Regan's freedom fighters (Mujahideen) and supported by the US Central Intelligence Agency (CIA), where they were resisting the Soviet occupation. They changed however, to President Bush Jnr's terrorists particularly after 2001. See G. Chaliand (1987) *Terrorism: From Popular Struggle to Media Spectacle* (London: Saqi Books) p.37. See also *Supra* as per C. Walker (2009) at p.1. See also *Supra* as per S. Zeidan (2004) 492

[225] *Supra* as per C. J. S. Gale, (2006). *Steel and others v United Kingdom* [1999] 28 EHRR 603 [54] and; *Hashman and Harrup v United Kingdom* [2000] EHRR 241 [31]

terms of terrorism, by the State and freedom fighters.[226] State terrorism and issues surrounding counter-insurgency are both beyond the ambit of this thesis, however, in the interests of fullness, Marian Price, a convicted IRA terrorist, draws on this particular issue:

> I don't see any distinction between al-Qaeda and what George [W] Bush's pilots did in Afghanistan. I would equate those two as terror, because that's what they are designed to do…to terrorise a population into surrender. That's the real terrorism.[227]

The difference in opinion evidences further the associated subjectivity of the label and shows that the politically loaded term can be used beyond its legal meaning.[228] It also shows that the term can be abused extensively thereby confusing the concept.[229]

CONCLUSION

There are two main problems concerning the UK's legal definition of terrorism under the Terrorism Act 2000. The first is a definitional problem whereby the phrases used remain undefined by Parliament. The proliferation of undefined

---

[226] *Supra* as per S. Zeidan (2004) 494-495

[227] *Supra* as per R. English (2010) at p.20

[228] *Supra* as per C. Walker (2009) at p.3, See also *Supra* as per B. Saul (2006) at p.3

[229] *Ibid* as per B. Saul (2006) at p.3. See also W. Laqueur (1987) *The Age of Terrorism* (Boston: Little, Brown and Company) p.143. See also: M. Freeman (2005) *Order, Rights and Threats: Terrorism and Global Justice*, in R. A. Wilson (ed) *Human Rights in the War on Terror* (Cambridge University Press). For example see United Nations ComHR preambles in 1998/47, 1999/27, 2000/30, 2001/31, 2002/35. It has also been made clear that terrorist activity cannot be used as a means to protect human rights. See A. Byrnes (2002) Apocalyptic Visions and the Law: The Legacy of September 11, a professorial address by Byrnes at the ANU Law School for the Faculty's *Inaugural and Valedictory Lecture Series*, May 30, 2002, available at https://law.anu.edu.au/CIPL/StaffPapersTalks&Submissions/Byrnes30May02.pdf accessed 12 December 2015

causes has resulted in some difficulty in deciding which to apply to a particular case, thereby effecting at least to some degree judicial application.

The second problem is intrinsically linked to the first, being the political currency of the terms use. In order to solve this, the UK could re-define terrorism and seek to remove as many political references apart from the cause element, and introduce exclusion clauses for actions taken by way of protest and industrial action and dissent, or during an international armed conflict in accordance with customary international law. Although it has been demonstrated that the UK legal definition of terrorism works reasonably well in practice, the lack of definitional syntax increases the political value and rule of law criticisms. For this to change, the UK must re-define an act of terrorism in line with international law and comparative nation states. It could potentially read:

> Terrorism is the use or threat of serious violence, designed to unduly compel a government or an international organisation, or to seriously intimidate the public, or section thereof, and is made for the purposes of advancing a political, religious, ideological, or racial cause.
>
> Protest, dissent or industrial action is omitted from this definition. Action taken during an armed conflict as part of a legitimate struggle of peoples fighting in the exercise of their right to self-determination is not terrorism, unless such action is directed towards non-combatants and/or civilians.

CHAPTER TWO. THE 21ST CENTURY TERRORIST THREAT: HOW TERRORIST GROUPS AND TERRORISTS COMMUNICATE, AND THE UNKNOWN THREAT

INTRODUCTION

This chapter outlines the way in which terrorist groups, and individual terrorists communicate in the 21st Century. Concentrating on the terrorist group Islamic State as a case study, this chapter will highlight the interdisciplinary relationships formed between the group and its individual supporters and cells, by utilising digital means. The chapter will explore the vertical effect of the group's propaganda and communication through the Internet, and how this impacts upon the current risk posed to UK security from terrorists. The rationale for focusing on the IS terrorist group is their efficient and prolific use of 21st Century digital technology. The vertical effect of IS's successful and expert use of electronic communications data will be assessed, illustrating the need for new legislative measures. The horizontal effect of terrorist communication will then be analysed, which will demonstrate the difficulties posed to UK lawmakers, and UK policing and security agencies, specifically with regards to encryption technology in the 21st Century, and the growth of the darknet.

Following on from discussing the problems faced, the chapter will then place emphasis on the UK's legal efforts made to combat the collection of terrorist

materials, the dissemination of such and efforts to prohibit direct and indirect encouragement to commit a terrorist act. The effects of terrorist communication in radicalising citizens' to commit acts of terrorism will then be discussed, showing a worrying trend in jihadi tourism and increased individual operational abilities.

TERRORIST GROUP: ISLAMIC STATE

For the media and the world the IS terrorist group appeared to come from nowhere and spread across Syria and Iraq at incredible speed.[230] According to news reports, IS was founded by Abu Musab al-Zarqawi in 2004. Originally the group was called Islamic State in Iraq and the group became an umbrella organisation under al-Qaeda in Iraq in 2006.[231] In 2010 the leadership was transferred to Awwad Ibrahim Ali al-Badri al-Samarrai, also known as al-Baghdadi, who started to rebuild its military capabilities and within three years the group was carrying out terrorist attacks in the local region.[232] In an attempt to draw more support to IS, al-Samarrai took the name Abu Bakr al-Baghdadi, and in April announced the merger of IS with other groups to create the Islamic State

[230] D. Byman (2015) Al Qaeda, The Islamic State and the Global Jihadist Movement, (Oxford University Press) pp.166-167. See also M. W. Nance (2015) The Terrorists of Iraq: Inside the Strategy and Tactics of the Iraqi Insurgency 2003-2014, (CRC Press) pp.297-300

[231] See http://www.bbc.co.uk/news/world-middle-east-29052144 accessed 27 October 2016

[232] *Supra* as per Byman at pp.306-308

in Iraq and the Levant/al-Sham (ISIL/ISIS).[233] Taking advantage of political unrest in the region ISIL/ISIS grew exponentially taking control of various villages, towns and cities, finally resulting in the group's proclamation of a Caliphate, becoming known thereafter simply as Islamic State. Abu Mosa was appointed as the head press officer, and in June 2014 made it clear that the Caliphate had been established, stating:

> …the Islamic State has been established. And we will not stop. Don't be cowards and attack us with drones. Instead send your soldiers, the ones we humiliated in Iraq. We will humiliate them everywhere, God willing, and we will raise the flag of Allah in the White House.[234]

Building from this statement and in order for the group to expand and fill the shortfall of fighters, a press office was developed launching an advertising and marketing campaign. As a result of the statement and the swift gains of territory in the Anbar area of Iraq and North Syria the UK proscribed the terrorist group in July 2014.[235] Since then IS have perhaps become one of the most notorious and influential groups within the Middle East and North Africa, posing a direct terrorist threat not only to those regions, but to the nation states around the world. The level of violence directed towards all those that oppose their own religious interpretation and political doctrine has been merciless, with beheadings of UK,

---

[233] Abu Bakr is an infamous name within the Islamic religion, being the name of the prophet Muhammad's father-in-law and chief adviser, becoming a caliph. This name resonates with Muslims and deep within the Muslim psychology, and was therefore chosen very carefully. For further information see P Mosendz (2014) How the head of ISIS got his name: Abu Bakr al-Baghdadi chose a name with historic resonance in the Muslim world, Europe Newsweek, http://europe.newsweek.com/abu-bakr-al-baghdadi-abu-dua-invisible-sheikh-awwad-ibrahim-ali-al-badri-al-282939?rm=eu accessed 27 October 2016

[234] See http://www.counterextremism.com/content/abu-moussa-isis-press-officer-june-2014. See also http://www.theatlantic.com/international/archive/2014/08/isil-press-officer-abu-mosa-killed-by-syrian-army/378994/ accessed 27 October 2016

[235] House of Commons Library (2014) The Terrorism Act 2000: Proscribed Organisations, Standard note SN/HA/00815, 25th July 2014, available at researchbriefings.files.parliament.uk/documents/SN00815/SN00815.pdf, p.8

US and Japanese citizens', and Syrian opposition forces, and massacres of Sunni Muslim cities such as Tikrit in Iraq.[236] Attacks inspired by IS, have more recently been committed in Paris in November 2015 and on a Tunisian holiday resort resulting in 38 UK citizens' deaths. In Nice on Bastille Day, a lone actor inspired by IS killed 86 civilians and injured 303, by driving a 17-tonne heavy good vehicle through a crowd.[237] Atrocities such as these have been witnessed by the world at large due to the group's efficient use of electronic communications technology.

21ST CENTURY METHODS OF COMMUNICATION: HOW TERRORIST GROUPS USE THE INTERNET IN THE DIGITAL AGE

Utilising the Internet to market the IS brand, which is now available in over forty languages, the group has been able to infiltrate citizens' homes and effectively influence them into joining the fight in Syria and Iraq, or to commit lone Islamist attacks in their home nation states.[238] For Klausen, the Internet and social media outlets have been a gift to terrorist groups such as IS, allowing them to meet their strategic aims in recruitment, financing and publicising their cause.[239] An example of an image that seems to resonate with this line of thinking is below.

---

[236] N. Khomami (2015) Mohammad Emwazi: who were his victims? The Guardian, 13 November 2015, available at http://www.theguardian.com/uk-news/2015/nov/13/mohammed-emwazi-who-were-his-victims accessed 20 November 2016

[237] See http://www.bbc.co.uk/news/world-europe-36801671 accessed 20 November 2016

[238] J. Klausen (2015) Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq, *Studies in Conflict & Terrorism* 39(1), 1-22, 3

[239] *Ibid*

Figure 1, taken from https://www.reddit.com/r/jihadpropaganda/ accessed 21 November 2016

These images and IS's propaganda is spread through the Internet by largely utilising social media outlets. Such outlets consist of Twitter, Facebook and YouTube, in addition to dedicated websites that publish online Islamist magazines translated into various languages, such as the Dar al-Islam and Dabiq, both created by IS, and Inspire created by al-Qaeda, found on the dedicated website Jihadology.[240] IS have created a media ministry and effectively decentralised social media use. In forming part of this ministry, IS have shown great awareness

[240] See http://jihadology.net/category/dar-al-islam-magazine/ and https://azelin.files.wordpress.com/2016/07/al-qacc84_idah-in-the-arabian-peninsula-e2809cinspire-guide-2-nice-operatione2809d.pdf accessed 27 October 2016

building capabilities through mass Internet media attracting others to their cause. One of these tactics included the holding of a hostage John Cantlie, who read out messages from IS explaining the group had been misrepresented by Western media and they would be presenting the truth in future videos.[241] These videos, as with all IS's propaganda are skilfully produced to a high quality, with great care taken in terms of presentation. For Milton, the mixing of fear and reason makes a potent combination.[242]

In creating and maintaining the centrally controlled Ministry of Media, IS have managed to spread it multilingual propaganda effectively. Such outlets to the Ministry include the al-Furqan Institute, l'tisaam Media Foundation, Anjad Media Foundations, and the English based outlet the al-Hayat Media Centre.[243] The al-Furqan manufactures DVDs, posters and brochures that the al'tisaam then disseminate through the Internet in various languages, including English, French, German and Russian.[244] IS's high quality glossy magazine Dabiq is also printed in several different languages and contains a larger quantity of articles and

---

241 BBC News (2014) Video of British hostage John Cantlie released, 18th September 2014, available at http://www.bbc.co.uk/news/uk-29258201 accessed 20 November 2016

242 D. Milton (2014) The Islamic State: An Adaptive Organisation Facing Increasing Challenges, in al-Ubaydi, Lahoud, Milton and Price (editors), The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State, December 2014, The Combatting Terrorism Centre at West Point, p.53, available at www.ctc.usma.edu accessed 20 November 2016

243 *Ibid*

244 A. Khan (2014) What ISIL's English-language propaganda tells us about its goals, Aljazeera 20 June 2014, available at http://america.aljazeera.com/watch/shows/america-tonight/articles/2014/6/19/how-isil-is-remakingitsbrandontheinternet.html accessed 20 November 2016. See also H. J. Ingram (2015) The strategic logic of Islamic state information operations, *Australian Journal of International Affairs* 69(6) 729-752, 732

presentations that seek to legitimise IS's actions and the idea of the Caliphate, all aimed at recruitment.[245] IS's latest 15th issue of Dabiq starts with:

> The spark has been lit here in Iraq, and its heat will continue to intensify – by Allah's permission – until it burns the Crusader armies…[246]

Along with various links to videos, all of which represent high quality filming, there are many articles dedicated to legitimising IS's struggle against the West, and what they call the Crusaders.[247] The articles themselves are extremely bias and clearly aim to spread their rather cynical take on Christianity, Judaism and all other forms of religion and non-religion that do not follow their own interpretation of Islam.[248] With one photo showing a jihadi fighter holding a kitten and then one showing children playing, the magazine is clearly attempting to show a caring side to the IS.[249] One particular story glamorises an individual Islamist fighter story and illustrates the terrorist attack that took place in Nice:

> Between the release of this issue of Dabiq and the next slaughter to be executed against them [the West] by the hidden soldiers of the Caliphate - who are ordered to attack without delay - the Crusaders can read into why Muslims hate and fight them, why pagan Christians should break their crosses, why liberalist secularists should return to the fitrah (natural human disposition), and why sceptical atheists should recognize their Creator and submit to Him. In essence, we explain why they must abandon their infidelity and accept Islam, the religion of sincerity and submission…[250]

---

[245] H. J. Ingram (2015) Three Traits of the Islamic State's Information Warfare, T*he Rusi Journal* 159(6) 4-11, 5

[246] Dabiq (2016) Breaking The Cross, Issue 15, 1437 Shawwal, p.1, available at http://jihadology.net accessed 15 November 2016

[247] *Ibid*

[248] *Ibid* p.67

[249] *Ibid* p.10

[250] *Ibid* p.4

Figure 2, taken from Dabiq (2016) Breaking The Cross, Issue 15, 1437 Shawwal, p.10, available at http://jihadology.net accessed 15 November 2016

Figure 3, taken from Dabiq (2016) Breaking The Cross, Issue 15, 1437 Shawwal, p.39, available at http://jihadology.net accessed 15 November 2016

Figure 4, taken from Dabiq (2016) Breaking The Cross, Issue 15, 1437 Shawwal, p.68, available at http://jihadology.net accessed 15 November 2016

In attempting to rationale their terrorist actions one section of the magazine is titled, 'Why we hate you and why we fight you'.[251] As one would expect, the hatred starts with the fact Christians are in fact Christian, then the article moves on to describe how Western views are far too liberal, using images such as below. What must be remembered is that these messages may perhaps resonate with many people and simply seek to radicalise others in their call for support.

Figure 5, taken from Dabiq (2016) Breaking The Cross, Issue 15, 1437 Shawwal, p.32, available at http://jihadology.net accessed 15 November 2016

Social Media: Twitter, Facebook and YouTube

Social media is open source and essentially available for all citizens' to use worldwide. IS have used this rather cynically to their advantage to disseminate their message. In 2015 the Director of Europol confirmed the IS terrorist group is believed to directly control 50,000 different twitter accounts and coupled with

[251] *Ibid*

individual Islamists were sending up to 100,000 twitter messages per day in an attempt to market, radicalise others and plan an attack.[252]

Berger and Morgan further this claim, arguing IS may actually have direct control of over 90,000 twitter accounts, thereby doubling the amount of daily messages sent.[253] In August 2016, Twitter announced they had closed over 235,000 accounts with links to IS over a six-month period.[254] Such IS messages read:

> You can sit at home and play call of duty or you can come here and respond to the real call of duty…Kill the police and soldiers…carry out lone wolf operations…smash his head with a rock, or slaughter him with a knife, or run him over with your car, or throw him down from a high place, or choke him, or poison him…Muslims stand by its black brothers and sisters. Your [You're] all welcome to Islamic State we will embrace you and love you.[255]

For Ingram, although these messages and the dissemination of information regarding IS actions overseas have proved effective through social media; they are 'more strategic plagiarists than geniuses'.[256] According to Ingram, the group has simply mimicked the way in which international businesses and companies

---

[252] See http://www.dailymail.co.uk/sciencetech/article-3747501/Twitter-s-terror-crackdown-Social-network-says-shut-235-000-accounts-linked-Islamic-State-groups-six-months.html accessed 27 October 2016

[253] J.M. Berger and J. Morgan (2015) The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter, 20 March 2015, Center for Middle East Policy at Brooking, available at http://webcache.googleusercontent.com/search?q=cache:nUpiATbv50wJ:www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf+&cd=1&hl=en&ct=clnk&gl=uk accessed 21 November 2016

[254] See http://www.dailymail.co.uk/sciencetech/article-3747501/Twitter-s-terror-crackdown-Social-network-says-shut-235-000-accounts-linked-Islamic-State-groups-six-months.html accessed 27 October 2016

[255] See http://www.memrijttm.org/jihadi-reactions-to-nice-terror-attack-we-want-paris-before-rome.html. See also http://www.independent.co.uk/news/world/middle-east/isis-urges-more-attacks-on-western-disbelievers-9749512.html accessed 27 October 2016

[256] H. Ingram (2016) Militant Islamist propaganda targeting Muslims in the West: comparing Inspire and Dabiq narratives, Terrorist Use of the Internet: Assessment and Response, Dublin City University, Ireland.

have used social media to increase their position.[257] This has resulted in their success at spreading their message, thereby gaining support and financial donations.

IS have posted many videos on YouTube, which are often graphic and horrifying, showing the beheading and killing of their so called enemies. They have also used it to spread their message and show recent supporters to their cause siting happily holding a firearm, knives and grenades. These often too have a message of their own, encouraging others to join them in the fighting in Syria and Iraq.[258] As with Twitter, supporters use this format to continue IS's message and add their own comments, often creating their own specific channel.[259] Anjem Choudary represents one such example in the UK, where his YouTube channel remains live despite his criminal conviction for terrorist offences.[260]

In order to combat terrorist use of social media, Internet companies have started using new software originally designed to remove copyrighted material. Looking for 'hashes' that is a unique digital fingerprint assigned to specific videos posted online, the Internet companies' software is now able to automatically target terrorist material. Due to the advancing capabilities highlighted here, it is

---

[257] *Ibid*

[258] See https://www.youtube.com/watch?v=lFlsv0xpBKc at 19:50, for mass killing see 32:00, and see https://www.youtube.com/watch?v=WS2bX8X7eZk accessed 22 November 2016

[259] See https://www.youtube.com/channel/UCOr3TFdnT1yyrQIVQV007gw accessed 22 November 2016

[260] See http://www.dailymail.co.uk/news/article-3750223/Outrage-extremist-hate-videos-starring-hate-preacher-Anjem-Choudary-s-followers-available-online-despite-jailing.html accessed 22 November 2016

possible that such groups will increase their usage of other means of dissemination. First they could increase their use of specific Internet webpages allowing for anonymity of postings. Second they could simply increase the use of the 'darknet', which UK law enforcement agencies' are currently struggling to effectively police. With all of these formats, the aim is to bring people round to their way of thinking.

Regardless of this action, along with Facebook's, Keith Vaz MP, former Chair of the Home Affairs Select Committee said:

> Huge corporations like Google, Facebook and Twitter…are consciously failing to tackle this threat and passing the buck by hiding behind their supranational legal status, despite knowing that their sites are being used by the instigators of terror. The companies' failure to tackle this threat has left some parts of the Internet ungoverned, unregulated and lawless.[261]

Katz highlights the difficulty faced by policing and security agencies as they endeavour to monitor social media.[262] She explains how, with the benefit of encryption, IS are circumventing the blocking of their twitter feeds by having multiple backup accounts.[263] Furthermore, a point that seems to be overlooked it that IS's social media campaign is networked, rather than having a centralised person in control. Many of IS's recruits average the age of 24, meaning many have grown up with social media as part of their lives, which in turn means tools

---

[261] See http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-twitter-google-isis-daesh-internet-youtube-social-media-home-affairs-a7208131.html accessed 27 October 2016

[262] R. Katz (2015) How Islamic State is still Thriving on Twitter, 11 April 2015, InSite Blog on Terrorism & Extremism, available at http://news.siteintelgroup.com/blog/index.php/entry/377-how-the-islamic-state-is-still-thriving-on-twitter accessed 19 November 2016

[263] *Ibid*

such as Twitter and Instagram come easy to them.[264] For Katz this represents the real threat of IS as they use Twitter to launch recruitment and calls for lone jihad.[265] Supporting citizens' simply re-post or quote what they see from those they follow.[266] This particular part forms IS's unofficial communications strategy whereby the number of followers can be increased with the use of hashtags.[267]

THE INTERNET AND APPLICATION PROTOCOLS, SMARTPHONES AND ENCRYPTION

It must be remembered that citizens' born in the early 1990's have not known life without the Internet. Due to the growth in technology the use of written letters and telephone landlines were the first to decline. Research shows that in 1989 the main types of communication were by letters and landline.[268] From 2014 less than three in ten 16-24 year olds continue with this method. In fact less than 16% of UK households no longer have a landline and the UK Communications Infrastructure Report suggests this will decrease further bringing an end to their use as citizens' prefer Internet telephony.[269] Now, electronic mailing (emails) and text messaging are becoming a thing of the past. Utilising smart phones, instant

---

[264] See http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media accessed 27 October 2016

[265] *Supra* as per Katz

[266] See https://www.theguardian.com/uk-news/2016/aug/16/anjem-choudary-convicted-of-supporting-islamic-state accessed 20 September 2016

[267] *Supra* as per J.M. Berger and J. Morgan (2015)

[268] *Supra* as per D. Anderson (2015) pp.49-50

[269] *Ibid*

direct messaging applications more commonly known as chat apps, such as Apples iMessage and Facebook Messenger, appears to be the current favourite.[270] To this end, the ownership of smartphones has dramatically increased, since 2000 to 2014, which effectively allows for many different types of electronic communication methods.[271]

The Internet

Internet technology and the growth in use have been extensive, as people tend to favour making a call via the smart phone or tablet over the Internet. The number of citizens' making an Internet call (VOIP) has tripled between 2009 and 2014.[272] In addition to this vast increase in volumes of information sent and received, it is estimated that in 2016 one zettabyte of data will travel over the Internet, with Cisco predicting this will double by 2019.[273] It is important to note that in addition to this growth in use, the Internet is not territorially bound making it difficult for law enforcement to trace information sent through. Emails for example are not confined to the country of origin or receipt, rather they move freely across borders utilising the quickest path possible. This means of course an

---

[270] D. Anderson (2015) A Question of Trust: Report of the Investigatory Powers Review, London: The Stationary Office, pp.49-50, 'Instant messaging apps have overtaken traditional SMS services. In 2012, 19 billion messages were sent per day on instant messaging apps, compared to 17.6 billion text messages. Since 2012 the number of instant messaging apps has grown considerably.' See also https://www.whatsapp.com, and http://en.people.cn/102774/8568312.html accessed 31 July 2015

[271] *Ibid*

[272] OFCOM, The Communications Market (2016), Telecoms and networks, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0026/26648/uk_telecoms.pdf accessed 21 November 2016

[273] This is the equivalent of 667 trillion films. See J. Titcomb (2016) World's internet traffic to surpass one zettabyte in 2016, The Telegraph, 4 February 2016, available at http://www.telegraph.co.uk/technology/2016/02/04/worlds-internet-traffic-to-surpass-one-zettabyte-in-2016/ accessed 21 November 2016

email between two people in the UK may actually travel via another country. The servers of email services for many companies, such as Hotmail and Gmail, are based outside the UK.[274] Therefore, although UK legislation may require Internet and service providers to hold data for a certain length of time, the transnational nature means external agreements must be drafted.

The Internet structure is made up of three categories.[275]

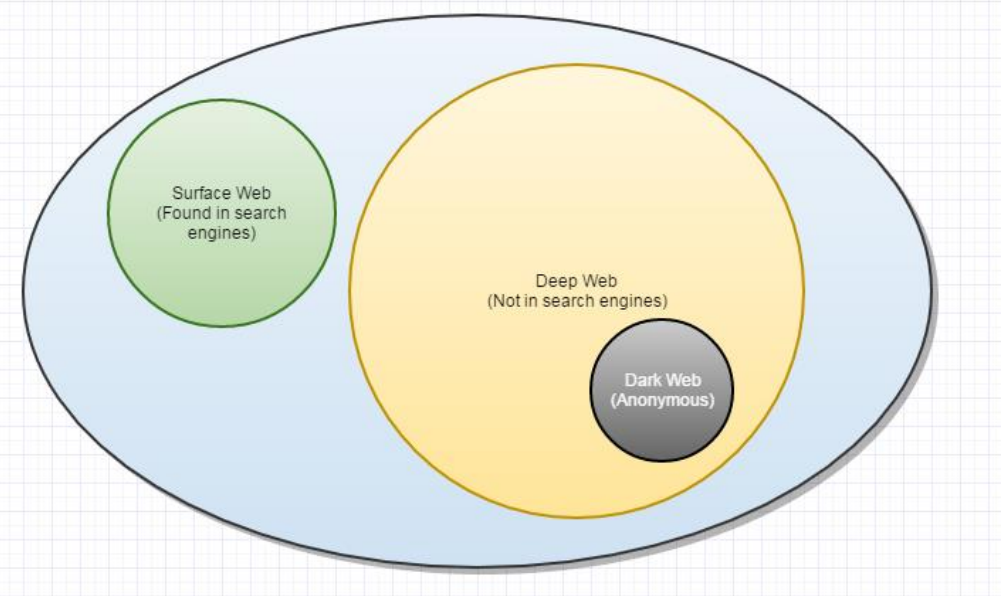

Figure 6, what the Internet structure looks like, taken from https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference accessed 20 November 2016

The 'surface web' represents webpages that can be found using standard search engines such as Bing and Google.[276] This is what the majority of users see and can find. The 'deep web', or 'invisible web', represents parts of the open web

[274] *Supra* as per D. Anderson (2015) p.51

[275] See https://www.reference.com/technology/basic-structure-internet-91e2893b49bd7bbd accessed 20 November 2016

[276] *Ibid*

that are simply not indexed by standard search engines.[277] Although sinister sounding, this part of the web has many legitimate uses such as, web email, online banking and PayPal, and videos on demand such as those available through Amazon.[278] It makes up almost 90 per cent of Internet usage figures.[279] The 'dark web' or 'darknet' is a small proportion of the invisible web that consists of tens of thousands of websites.[280] To clarify the current acronyms and types of Internet companies:

- Communications Service Providers (CSPs) provide services that transport information electronically. Examples of CSPs include companies such as British Telecom, Skype and TalkTalk, Facebook and Twitter. They may be based anywhere in the world, and offer communications services and Internet access;
- Companies that simply provide Internet access are referred to as Internet Service Providers (ISPs);
- Companies that provide applications or services, over the physical networks provided by CSP's and ISP's are called Applications Service Providers (ASPs). Examples of ASP's include Google, Whatsapp, Snapchat, Facebook, Yahoo, Skype and Apple.

Attributing the Communication

Aggravating the current problem surrounding terrorist communication is the difficulty in attributing Internet communication to a specific user of a device. Devices, such as computers, laptops and smartphones when utilising a network, use an IP address. There is only one IP address assigned to an Internet router, which can of course accommodate many devices. It has been noted by Brown

---

[277] *Ibid*

[278] P. Paganini (2012) The good and the bad of the Deep Web, The Hacker New Magazine, 17 September 2012, available at http://securityaffairs.co/wordpress/8719/deep-web/the-good-and-the-bad-of-the-deep-web.html accessed 21 November 2016

[279] *Ibid*

[280] *Ibid*

that this infrastructure of the Internet makes it difficult for the policing and security agencies to attribute a particular communication to the sender, and thereby offers a 'cloak of anonymity'.[281] Firstly, many family members and friends effectively share the IP address and also share devices. Secondly is the fact that IP addresses change depending upon where the person is accessing the Internet from, such as from the home to coffee shop or place of work. More seriously is the fact that thirdly a person can utilise software that purposefully creates ghost, or proxy IP addresses that are then untraceable.[282] It is therefore sometime impossible for the agencies to discover which device was used and by whom.[283]

In an attempt to remedy this problem, the Counter Terrorism and Security Act 2015 (CTSA) was enacted, partly to, 'address the difficulty that arises when IP addresses are shared by a number of users simultaneously, by requiring the retention of "relevant internet data" in addition to the shared IP address'.[284] However, this attempt appears to have failed because the CSP can only provide the data of the subscribed person, usually the bill payer, not the details of the

---

[281] C. S. D. Brown (2015) Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology, Vol 9, Issue 1, January-June 2015, p.58, available at http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf accessed 21 November 2016

[282] *Ibid* at p.68

[283] *Ibid*

[284] The Home Office Counter-Terrorism and Security Bill Factsheet, Part 3 Internet Protocol (IP) Address Resolution available https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/540538/CTS_Bill_-_Factsheet_5_-_IP_Resolution_v2.pdf accessed 22 November 2016

person using a particular device at a particular time.[285] This represents what has been termed a 'capability gap in communications data' that has 'a serious impact on the ability of law enforcement to carry out their functions'.[286] Intensifying this gap further is the fact there is now a fragmentation of telecommunications and communications data service providers. This is built in to their respective business models highlighting the difference between a UK landline call and a Voice Over Internet Protocol (VOIP). Landline calls are much more traceable with the provider knowing the endpoints of both parties to the call, whereas, the majority of VOIP services, such as Skype, operate over through an Internet connection.[287] Many Internet and Over-The-Top (OTT) providers are based overseas, which makes obtaining data from them by the UK policing and security agencies more difficult.[288] OTT providers in particular are free at the point of access and require little to none subscriber data, and additionally 'communications data relating to a single communication may not be in a single location due to the collaboration of companies'.[289]

Application Protocols and Encryption

When terrorist groups such as al-Qaeda in the Arabian Peninsula (AQAP) first started using encryption technology it was in its infancy. During the investigation into Rajib Karim communications to Anwar al-Awlaki, it became clear to the

---

[285] *Ibid*

[286] *Ibid*

[287] *Supra* as per D. Anderson (2015) p.52

[288] For OTT see: http://digiday.com/platforms/what-is-over-the-top-ott/

[289] *Supra* as per D. Anderson (2015) p.52

policing and security agencies that Karim used a multi-layered approach to encrypting his messages. This whole process was vastly time consuming, as Karim would first write the message into a Microsoft Excel document using macros to encrypt it, then copy and paste that into a Microsoft Word document. This document would then be saved using the 'password protect' feature that is unbreakable should the password used be long and complex. The document was then compressed and encrypted using another piece of software called RAR, again unbreakable, and then posted online through a URL shortened to render the metadata anonymous.[290] It took UK law enforcement nine months to decrypt Karim's computer.[291] For Graham, things have now moved on whereby the 'ubiquity of encryption in commercially available messaging tools and devices has made it increasingly easy for terrorists to communicate securely'.[292]

Encryption has now legitimately developed as a commercial communication technology and commodity, and is readily available, whereby two main forms exist:

1) Encryption in transit: this provides security during the transmission;
2) End to end encryption: this renders the message unreadable to all but the sender and intended recipient.

---

[290] R. Graham (2016) How Terrorists Use Encryption, Combating Terrorism Center, available at https://www.ctc.usma.edu/posts/how-terrorists-use-encryption accessed 21 November 2016

[291] V. Dodd (2011) British Airways worker Rajib Karim convicted of terrorist plot, Guardian, 28 February 2011, available https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim accessed 21 November 2016

[292] R. Graham (2016) How Terrorists Use Encryption, Combating Terrorism Center, available at https://www.ctc.usma.edu/posts/how-terrorists-use-encryption accessed 21 November 2016

The first example represents technology used by the banking industry to make communication safe and secure for customers. The second type, in addition to device encryption, seems to follow a similar rationale having been developed for smart phone and tablet device usage. End-to-end encryption is when the contents of a message are converted into an unreadable form, whereby only the person with the correct decryption key can read it. Both communication and device encryption is legitimately important in securing an individual's privacy, given it is perhaps safe to say the majority of smart phone users for example, store private information, photos and notes in their phones memory, which can then be stored on an iCloud server.[293] It is also important to mention that particularly since the introduction of applications such as Apple Pay, smart phone and server encryption forms an essential part of providing the customer with a high level of safety.[294]

In order to ensure this high level of security, the network provider or company overseeing the communication exchange, is often unable to decrypt a message, or gain entry into an individual's data stored on their smart phone.[295] Whilst these represent genuine uses for encryption and introduces an increased level of customer security, what often follows such legitimate technological advances is criminal exploitation.[296] This is where the problems faced by terrorist communication are felt on the capabilities gap in increasing the pressures on

---

[293] See https://support.apple.com/en-gb/HT202303 accessed 21 November 2016

[294] See https://support.apple.com/en-gb/HT203027 accessed 21 November 2016

[295] *Ibid*

[296] R. Smith (1998) Criminal exploitation of new technologies, Australian Institute of Criminology, Trends & Issues in Crime and Criminal Justice No. 93, 1

policing and security agencies in the 21st Century. Apples security on the iPhone for example is extremely high, whereby the device and the internal memory disk are individually encrypted. Remaining with Apple for the moment, since 2014 they have provided data encryption built in to its software, and accordingly they have stated that:

> Apple has no way to decrypt iMessage and Face Time data when it's in transit between devices. So unlike other companies' messaging services, Apple does not scan your communications, and we wouldn't be able to comply with a wiretap order even if we wanted to.[297]

Messaging Applications

21st Century messaging application technology follows a similar format to Apple's iMessage service. More commonly known as 'chat apps', when they were first developed the encryption technology used stopped at the service providers' server, meaning that policing and security agencies could obtain the electronic communications data. This also meant of course that cyber criminals could also hack into the service providers' server and obtain the same data. This led to one of the first chat apps to employ end-to-end encryption, called Telegram. Al-Qaeda operatives were very quick to start using this technology illustrating terrorist exploitation of this legitimate development.[298] Currently there are now many direct messaging applications, in addition to Apples iMessage, all offering

---

[297] *Supra* as per D. Anderson (2015) p.206. See also Apple's website http://www.apple.com/uk/privacy/approach-to-privacy/

[298] See http://gizmodo.com/the-best-and-worst-encrypted-messaging-apps-1782424449 accessed 21 November 2016

end-to-end encryption protocols, such as Whatsapp, Facebook Messenger, Instagram, Wickr, Line, Signal and Google.[299]

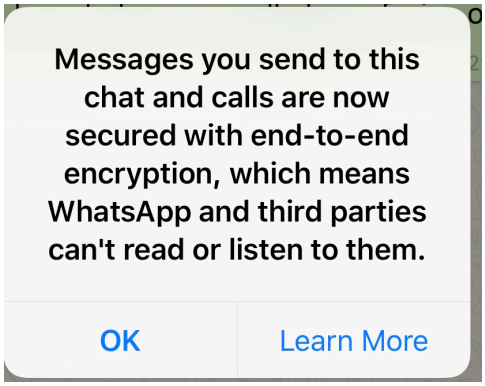

Figure 7, Whatsapp notice 5 December 2016, taken from my Whatsapp account

The technology used is similar to that used by the military on personal computers, rendering it near impossible to break. In addition, most chat apps now automatically delete messages after an hour or a day, depending upon the users settings. The growing user trend in this type of software has caused concern for UK law enforcement. The encryption allows terrorists to communicate freely and if caught, evidential problems may ensue because the messages are no longer available, or traceable. According to GCHQ, such devices and applications have become the 'command and control network' of terrorists.[300] The terrorists who attacked Paris for example utilised messaging apps in addition to using disposable 'burner' phones to congregate in safe houses in Belgium.[301] This allowed them to

[299] See http://gizmodo.com/the-best-and-worst-encrypted-messaging-apps-1782424449 and http://www.techtimes.com/articles/169154/20160709/9-messaging-apps-with-end-to-end-encryption-facebook-messenger-whatsapp-imessage-and-more.htm accessed 21 November 2016

[300] GCHQ chief accuses US tech giants of becoming terrorists, networks of choice, The Guardian, 3 November 2014 available at https://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan accessed 21 November 2016

[301] J. Stone (2016) ISIS Terrorists Used Disposable Burner Phones, Activated Just Hours Before, To Carry Out Paris Attacks, International Business Times, 21 March 2016, available http://www.ibtimes.com/isis-terrorists-used-disposable-burner-phones-activated-just-hours-carry-out-paris-2340265 accessed 21 November 2016

plan and thereby carry out their attack on 15 November 2015 resulting in 130 deaths with hundreds more injured.[302]

It is worth mentioning that it would not be difficult for the would-be-terrorist to quickly learn about all the available encryption techniques. In April 2016, the IS French online magazine Dar al-Islam demonstrated the importance of securing communications.[303] This further illustrates how the Internet assists terrorists in creating and maintaining an international presence, and according to Ban Ki-moon, Secretary-General of the United Nations, 'the Internet is a prime example of how terrorists can behave in a truly transnational way'.[304] These issues have led to Wainwright, Director of Europol to comment:

> …as the communications of terrorist networks and criminal groups have moved increasingly [online], it's opened up a whole new wave of problems for us even in the open internet, let alone the Darknet.[305]

The Darknet

Utilising specific software and Internet configurations, the darknet allows for a 'world of complete freedom and anonymity, where users say and do what they like, uncensored, unregulated, and outside of society's norms'.[306] An illegal

---

[302] *Ibid*

[303] R. Graham (2016) How Terrorists Use Encryption, Combating Terrorism Center, available at https://www.ctc.usma.edu/posts/how-terrorists-use-encryption accessed 19 November 2016

[304] *Ibid*

[305] See http://www.dailymail.co.uk/sciencetech/article-3747501/Twitter-s-terror-crackdown-Social-network-says-shut-235-000-accounts-linked-Islamic-State-groups-six-months.html#ixzz4OIUlFVVU accessed 27 October 2016

[306] *Ibid*

market place exists, such as the well-known 'Silk Road'; where people can buy and sell illegal items such as drugs, counterfeit goods, child pornography, books and firearms. Europol in their 2016 TE-SAT report, which illustrates the development of a 'professional, service-based underground economy', has identified the proliferation of cyber-crime and terrorism.[307] IS is also known to operate through this medium, in raising funds and selling books on how to carry out jihad, and how to make bombs and create homemade firearms.[308] The darknet works by sending and receiving messages through a network that involves a process known as 'onion rooting'.[309] This process protects the identity of the people involved in the electronic communication by wrapping layers around it. According to Lakhani this renders the communication impenetrable and therefore untraceable.[310] A software programme called 'Tor' is one of the most popular networks, and is used by IS because this permits them to hide their location and identity. Encrypted jihadi forums exist, along with chat rooms where terrorists and supporters can communicate freely, without fear of detection.[311] Parts of this network allow the transfer of unique funds undetected, and make purchases of

[307] Europol (2016) EU Terrorism Situation and Trend report TE-SAT 2016, Hague: Europol, pp.8-9

[308] http://uk.businessinsider.com/isis-is-using-the-dark-web-2015-7 accessed 21 November 2016

[309] http://uk.businessinsider.com/isis-is-using-the-dark-web-2015-7. See also http://www.pri.org/stories/2016-05-13/how-isis-recruits-online-using-encryption-chat-rooms-and-even-dating-sites accessed 21 November 2016

[310] *Ibid*

[311] *Ibid*

explosives, and firearms (of a type that are illegal in the UK), and fraudulent passports along with other items.[312]

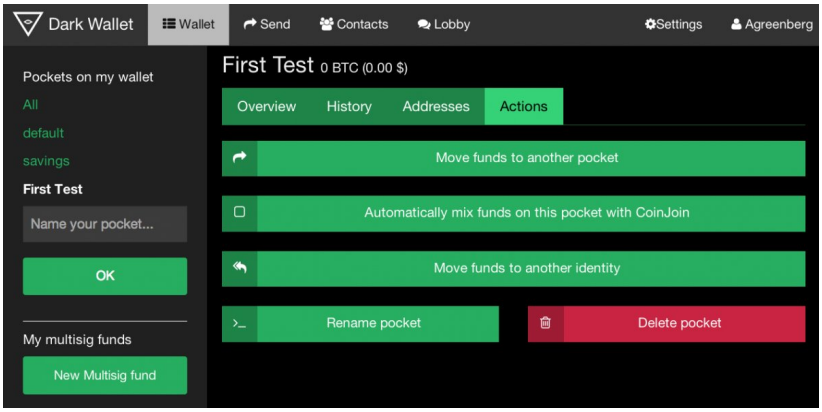

Figure 8, the Dark Wallet, taken from N. Bertrand (2015) ISIS is taking full advantage of the darkest corners of the Internet, Business Insider UK, http://uk.businessinsider.com/isis-is-using-the-dark-web-2015-7?r=US&IR=T accessed 5 December 2016

Figure 9, semtex explosive, taken from J. Patrice (2016) Bombs used by ISIS in Brussels terror attacks are for sale online, NewsGrio, http://www.newsgrio.com/articles/world/uk/244032-bombs-used-by-isis-in-brussels-terror-attacks-are-for-sale-online.html accessed 5 December 2016

[312] See: http://www.huffingtonpost.com/kevin-goodman/internet-black-markets_b_4111000.html. See: http://www.foxnews.com/tech/2015/04/23/darknet-danger-organs-murder-credit-card-info-all-for-sale-on-internet.html accessed 20 November 2016

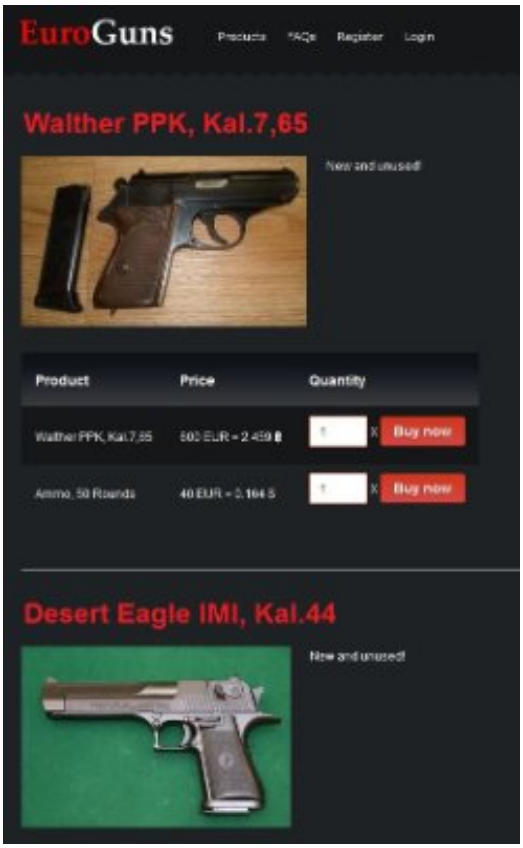

Figure 10, Items for sale through the Darknet taken from B. Chacos (2013) Meet Darknet, the hidden, anonymous underbelly of the searchable web, PC World, http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html accessed 5 December 2016

Figure 11, ability to buy a new identity, taken from M. Zimmerman (2015) Darknet danger: Organs, murder, credit card info all for sale on Internet's underbelly, http://www.foxnews.com/tech/2015/04/23/darknet-danger-organs-murder-credit-card-info-all-for-sale-on-internet.html accessed 5 December 2016

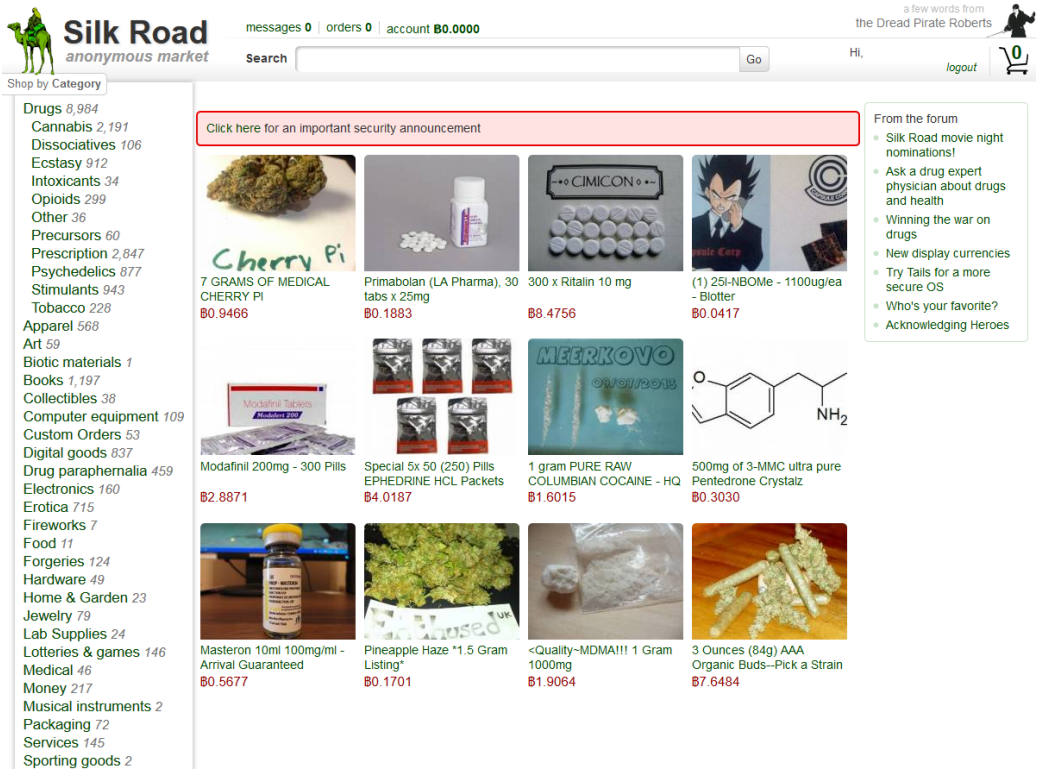

Figure 12, Silk Road taken from B. Chacos (2013) Meet Darknet, the hidden, anonymous underbelly of the searchable web, PC World, http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html accessed 5 December 2016

It is not very difficult to find using a 'normal' search engine, such as Google, and neither is it difficult to download the Tor software programme.[313] Tor has been in operation since October 2003 and is described as providing an open network, 'that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and State security'.[314] But in actual fact Tor allows a person to access the deeper realms of the darknet, called 'Onionland'.[315] Utilising Tor,

[313] See https://www.google.co.uk/#q=Tor accessed 30 November 2016

[314] See https://www.torproject.org accessed 21 November 2016

[315] See http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html accessed 21 November 2016

'Onionland' allows criminals a free space to work and effectively, 'cloak themselves in obscurity with specialised software that guarantees encryption and anonymity between users, as well as protocols or domains that the average person will never stumble across'.[316]

The main concern is that terrorists could be able to launch more advanced attacks, and by utilising Tor, become harder for policing and security agencies to detect and prevent attacks. Europol's 2016 TE-SAT report confirms that IS has an advanced level of encryption knowledge. Coupled with Anders Breivik's step-by-step guide on how to use Tor and Onionland, and the use of the darknet, it is clear that the 'likelihood of future attacks being based on new modus operandi with a stronger cyber dimension' is an increasing reality.[317] 'Terrorists have certainly demonstrated their flexibility and willingness to learn and further develop their technical skills'.[318] To this end policing the darknet represents a very real challenge for policing and security services. For Brown law enforcement agencies', 'face a serious capabilities gap', both in terms of expertise and budget.[319] To tackle the latter, the UK's former Treasury Minister George Osborne MP committed an extra £1.9 billion to be invested in cybercrime, in

---

316 http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html accessed 21 November 2016

317 *Supra* as per Europol (2016)

318 *Ibid*

319 C. S. D. Brown (2015) Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology, Vol 9, Issue 1, January-June 2015, p.92, available at http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf accessed 21 November 2016

November 2015.[320] This investment will partially be used to increase the lacking expertise, whereby according to news reports, GCHQ is planning to share their cryptography and intelligence analysis knowledge with other private companies in a hope to collaborate on an effective approach to cybercrime.[321] In addition GCHQ and the NCA have co-located a Joint Operations Cell (JOC) in order to increase their abilities.[322]

It is clear, that propaganda spread through open sources such as social media, through to mainstream Internet providing dedicated websites, to the Darknet allowing for the purchase of illegal weapons and information useful to a terrorist, overall IS's digital communicational strategy has proved first class. Such propaganda has led directly to the radicalisation of citizens' resulting in terrorist attacks being committed, or thwarted. Such radicalisation was seen in the UK in 2015, where a 15-year-old boy from Blackburn used Internet communication to plot with Australian counterparts to behead Australian police officers at the ANZAC day celebrations. Having received a life sentence, the UK now has the youngest convicted terrorist.[323] In the UK in 2015 seven major planned IS attacks

---

[320] https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security accessed 22 November 2016

[321] R. Perez (2016) GCHQ to fund startups to fight cyber-crime, SC Magazine available at http://www.scmagazineuk.com/gchq-to-fund-startups-to-fight-cyber-crime/article/524540/ accessed 20 November 2016

[322] http://www.nationalcrimeagency.gov.uk/news/736-gchq-and-nca-join-forces-to-ensure-no-hiding-place-online-for-criminals accessed 21 November 2016

[323] BBC News (2015) Anzac Day terror plot: Blackburn teenager admits inciting attack, 23 July 2015, available at retrieved from http://www.bbc.co.uk/news/uk-england-manchester-33633915 accessed 20 November 2016

were prevented by the policing and security services, with intelligence suggesting more were being planned.[324]

CONCLUSION

Terrorist groups and self-starters have embraced modern communication technology, using it from marketing up to coordinating an attack. Given these technological advancements have brought about economic and societal change, it is of little surprise that it has had a similar effect of terrorism and criminality.[325] It is interesting to note that in response the then UK Prime Minister David Cameron announced that if he was leading the next government, he would introduce legislation in 2016 to eliminate 'safe spaces' for terrorists to communicate.[326]

It is estimated that technology doubles every two years.[327] Although beyond the ambit of this thesis, this figure is now vehemently contested with some recent debates suggesting technological advancements are slowing down. However, for Tim Simonite the growth in mobile telephonic smart phone applications, the

---

[324] S. Coates (2015) PM: seven terror attacks in UK stopped in last year, The Times, 16 November 2015, available at http://www.thetimes.co.uk/tto/news/uk/article4615198.ece accessed 20 November 2016

[325] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf accessed 23 November 2016

[326] *Ibid*

[327] See https://www.extremetech.com/extreme/210872-extremetech-explains-what-is-moores-law accessed 23 November 2016

figure of two years could prove to be a little low.[328] It is reasonably well known the legislature is slow in keeping up with the growth in technology, and it is surmised this would continue for the foreseeable future. A unique threat has been created, whereby the vertical effects of terrorist groups' communication radicalise others, then the horizontal effect that allows people to operate under an anonymity cloak, who have advanced independent operational abilities with potential access to explosives and firearms purchased on the darknet.

Considering this predicament, legislation, namely the IPA, has been created aimed at policing the Internet. A cooperative approach with ISP's is essential to this aim, ensuring the dark sides of the web are monitored and then removed should they be deemed illegal. It is also essential the Government collaborate with smart phone application providers to allow targeted decryption of messages.

[328] See https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/ accessed 23 November 2016

CHAPTER THREE. PART ONE. THE UK'S LEGAL RESPONSE TO TERRORISM COMMUNICATION IN THE 21ST CENTURY: THE NECESSITY OF BULK COMMUNICATIONS DATA SURVEILLANCE

INTRODUCTION

This Chapter will look at the legislative measures the UK Government has introduced in their attempt to deal with terrorist electronic communication and the resulting terrorist threat. The technological advances have been made clear in the previous chapter, now the emphasis will alter to assess the UK's policing and security agencies tasks, in carrying out efficient and effective surveillance on terrorist activity and terrorism communications. Starting with the legal surveillance powers in the UK and focusing on those aimed at dealing with counterterrorism, the chapter will focus on the main contentious issue facing the UK's legal response to terrorism communication in the 21st Century that are the bulk interception and retention of electronic communications data powers, and bulk equipment interference.

The UK's surveillance legal framework changed on the 29th November 2016 with the enactment of the Investigatory Powers Act 2016 (IPA). This Act does not entirely replace the existing foundations stone to the surveillance framework, provided by The Regulation and Investigatory Powers Act 2000 (RIPA). For the

purposes of the thesis, the IPA does replace the bulk powers found under RIPA and introduces a new decryption power. This chapter will show that the surveillance structure consists largely of RIPA and the IPA, which delivers the required structural integrity. The chapter will start with an in-depth analysis on the IPA, focusing on the extent of the powers of bulk data surveillance, which reveals legislative definitional difficulties within the UK's key approach. The analysis then examines the broadness of the powers, albeit with restricted access to the data collated, illustrating the minimum protection afforded to citizens', especially when dealing with open source data, considered to be private. Case examples will be used to demonstrate how complicated and difficult terrorist communication can be, and whether the materials communicated cross the legal terrorism threshold.

The need for the IPA will become clear once the chapter has highlighted the difficulty faced by the UK's law enforcement agencies' in deciphering friend from foe, particularly in light of the extensive technological advancements made in electronic communications. Part Two of this Chapter will then focus on other counterterrorism-focused measures, illustrating the apparent ineffectiveness, which may change as a result of the IPA.

THE INVESTIGATORY POWERS ACT 2016

The IPA was enacted on the 29th November 2016. In bringing a number of legislative surveillance of communications powers contained in other UK statutes into one statute, it contains nine parts with 272 sections. This makes the IPA a substantial statute designed to make it easier for relevant agencies to apply for authorities and warrants as well as making it easier for the courts to determine under which statute the authority or warrant was issued. At the preamble of the Act it states:

> An Act to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

Forming a significant part of the UK's legal surveillance framework, it provides structural support to already existing powers located under RIPA, the Intelligence Services Act 1994 (ISA) and the Security Services Act 1985 (SSA).[329] Although RIPA continues to provide the foundation stone to this legal framework, the IPA is significantly larger amending parts of RIPA, the ISA and additionally the Wireless Telegraphy Act 2006. Bringing them within the IPA's ambit, it focuses more on electronic communications data surveillance and bulk powers, in line with 21st Century technology and to combat terrorist communication discussed in

[329] Investigatory Powers Act 2016, s 251

the previous Chapter.[330] It could be argued that the IPA has missed the opportunity to bring the UK's legal surveillance framework within the ambit of one piece of legislation, meaning that the various surveillance powers and authorisations remain scattered throughout other statutes. RIPA for example still governs the different types of surveillance, such as random or overt (i.e. the use of CCTV), and directed or covert, where the targets are monitored from static observation points and followed, and intrusive surveillance where premises and property is interfered with. Prior to the IPA, RIPA did also govern the interception of communications and electronic communications data, whereby communications are monitored either under a direct-targeted authority or a bulk data warrant. RIPA also governs the use of covert human intelligence sources (CHIS) more commonly known as informants. However, both Houses of Parliament and the various committee stages gave careful consideration to the IPA, who seemingly decided that it was unnecessary for the Act to merge all the various powers into one. The IPA appears to be focused entirely on powers related to the surveillance of electronic communications data, and is arguably already adequately large.

This particular point was emphasised by the Rt. Hon. Dominic Grieve QC in the Intelligence and Security Committee's report into the IPA.[331] Grieve's Report found that the IPA, although makes, 'some attempt to improve transparency', the

[330] Investigatory Powers Act 2016, s259

[331] The Rt. Hon. Dominic Grieve QC MP (2016) Intelligence and Security Committee of Parliament, Report on the draft Investigatory Powers Bill, 9 February, HC 795, p.1

Intelligence and Security Committee were, 'disappointed to note that it does not cover all the agencies' intrusive capabilities.[332] As a general overview, Part One of the Act proffers a new human rights approach from the UK Government, dealing specifically with privacy protections including offences and penalties for the misuse of electronic communications data surveillance.[333] It appears the UK Government has learnt from previous case decisions and critiques, and ensured there is a form of judicial scrutiny, wider safeguards to protect personal data and privacy rights. It also serves to remove certain powers to obtain communications data previously authorised under RIPA, such as some local authorities and those listed under Schedule 2 of the IPA.[334] Part Two of the IPA introduces the use of targeted interception, which needs to be considered alongside Part five dealing with the use of targeted equipment interference. Part Two continues to introduce two further types of interception warrant, which are targeted examination and mutual assistance.[335] The list of person able to request an interception warrant are the same as listed in section 6 of the RIPA, albeit with the introduction of some language simplification.[336]

Parts Three and Four deal with the obtaining and the retention of, and access to electronic communications data. Parts Six and Seven introduce new bulk powers,

---

[332] The Rt. Hon. Dominic Grieve QC MP (2016) Intelligence and Security Committee of Parliament, Report on the draft Investigatory Powers Bill, 9 February, HC 795, p.1

[333] Investigatory Powers Act 2016, s 11

[334] Investigatory Powers Act 2016, s 12

[335] Investigatory Powers Act 2016, s 15(1)

[336] Investigatory Powers Act 2016, s 18(1)

the retention of such and the use of personal datasets, with part eight providing a new oversight regime, and part nine providing the Secretary of State the powers to review the operation of the IPA, initially within the first six months and then subsequently five years after, and to report to Parliament with the findings.[337] The authorisation processes are similar in nature to those already provided for under RIPA, requiring the Secretary of State to sanction the warrant, however, as will be discussed later, the Act does introduce a 'double lock' system whereby an independent judicial commissioner must review the authorisation prior to any police action, and the authorisation of the warrant is to be reviewed at a later stage by a new Independent Investigatory Powers Commissioner.[338]

Given the restraints placed on this thesis, it is proposed to concentrate on the new legalised bulk powers of interception, acquisition and equipment interference, and their impact on privacy, whilst discussing the new oversight regime and safeguards, with particular reverence to judicial review principles.

The Bulk Powers: The general rationale

The bulk powers of surveillance are perhaps the most important parts of the IPA. They are aimed at closing the UK's law enforcement agencies' technological capabilities gap covered in Chapter Two. They are not entirely uncontroversial, because they have the potential to affect the whole population, or a large section

[337] Investigatory Powers Act 2016, s260. See also House of Lords Second Reading 27 June 2016, Volume 773, Column 1361-1362, available at https://hansard.parliament.uk/lords/2016-06-27/debates/1606278000466/InvestigatoryPowersBill

[338] Investigatory Powers Act 2016, s 19 and 23

thereof, although in practice this is unlikely, and are aimed at identifying potential terrorists that remain unknown to the policing and security agencies. It is quite simply about finding potential investigative leads, perhaps better explained as allowing law enforcement an opportunity to 'find the needle in the hay stack', as highlighted in Chapter Two, and developed further below when looking at issues surrounding the traceability and typecasting of terrorists. The bulk powers contained in the IPA are split into 4 sections:

- Section 136 Bulk interception warrants;
- Section 158 Power to issue bulk acquisition warrants;
- Section 176 Bulk equipment interference warrants;
- Section 199 Bulk personal datasets.

The former Director General of the Security Service (more commonly known as MI5) Lord Evans evidenced the essential part they play in countering the terrorist threat, using an example of how the agency might use the bulk powers provided during the First Sitting Committee Debate on the IPA in March 2016.[339] He suggests that using these powers allows law enforcement find people who 'might' be members of IS and thereby 'may' pose a threat by:

> …look[ing] at *all individuals* from the UK who are known to have travelled into or out of the Middle East and the area around Syria over the past six months.[340]

Once this task is complete, law enforcement can then narrow the field of search by looking for electronic communications data on individuals who have been in Molenbeek for example, because, 'it looks as though quite a lot of the problems

[339] *Supra* as per First sitting Committee Debate Session 2015-16, at Column 23

[340] *Ibid*

have emerged from that particular part of Brussels'.[341] The next steps continue to narrow the field as Evans explains:

> …Put all those elements of data together and you will end up with perhaps a few dozen…You might then say, "Let's take all those phones and see which of those telephones has been in first or second-order contact with known extremists"…That might refine it down from 150 to half a dozen. Then you might start to think, "Actually, there's quite a high likelihood, although one cannot be certain, that these half a dozen might be people of security interest"…At that point, having gone through those various layers of putting different sorts of data together, comparing, contrasting and seeing what comes out, you might say, "Perhaps for those half a dozen, some more targeted form of surveillance is justified"…Once you have done that, [subject to authorisations] you might then find that some of them are self-evidently not, because they are BBC journalists who have been following the story or similar…But you might find that you have one or two who look as though they might be IS activists…so you put some resource into establishing what they are doing and who they are associating with.[342] [My emphasis]

This represents the, 'sort of process in which the Security Service have used these sorts of capability over the last 10 years or so', and according to Evans it has been 'absolutely central' to law enforcement agencies' in identifying individuals involved in terrorist planning.[343] The information attained is then fed through into more intensive investigations, enabling policing and security agencies to prevent terrorist attacks.[344] Regardless of the centrality, these powers form part of the agencies capabilities and it is quite clear from this statement that UK law enforcement have been using bulk collection powers for over the last ten years, with little to none legal regulation. According to Evans, the IPA merely places

---

[341] *Ibid*

[342] *Ibid*

[343] *Ibid*

[344] *Supra* as per First sitting Committee Debate Session 2015-16, at Column 23

legal regulation in an attempt to remedy the lacking provisions, transparency and accountability.[345]

BULK INTERCEPTION OF ELECTRONIC COMMUNICATIONS DATA AND CONTENT: THE LEGAL DEFINITIONS

The entire framework provides extraordinarily vast surveillance powers to State agencies, particularly law enforcement agencies' when acting in the interests of national security. One of those powers allows for the bulk interception and acquisition, and retention of electronic communications data. In order to understand the extent of these powers, the legal definition of electronic communications data and what is meant by interception must first be elaborated on.

Electronic communications data is data in the course of transmission, which does not include the content, and the interception of communications is the action of procuring data in transition.[346] Electronic communications data remains defined in RIPA as:

> …the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication *is being*, or *has been*,

[345] *Ibid* at Column 23

[346] Regulation of Investigatory Powers Act 2000, s 2(7)

> transmitted is used for *storing* it in a manner that enables the intended recipient to collect it or otherwise to have access to it [My emphasis].[347]

However, due to the inclusion of the word 'storing', the interception may ultimately lead the policing and security agencies to look at some, if not all of the content, as per the general understanding of the word 'content'.[348] Confusingly, should law enforcement require access to data that is not in the course of transmission, then this is known legally as 'content', which has not been defined in RIPA. This has now been addressed and under section 261(6) of the IPA, content is defined as:

> "Content", in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means *any element* of the communication, or *any data attached* to or *logically associated* with the communication, which *reveals* anything of what might reasonably be considered to be the meaning (if any) of the communication, but -
>
> (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be *disregarded*; and
> (b) anything which is systems data is not content. [My Emphasis]

This appears to mean that should the content be inadvertently obtained as part the electronic communications data, for example the content of a text message or email in transmission, it is to be disregarded. However, the IPA has not taken the opportunity to redefine 'communications data'. It is therefore difficult to assess if this definition of 'content' has remedied the confusion surrounding the word

---

[347] Regulation of Investigatory Powers Act 2000, s 2(7). See Investigatory Powers Act 2016, s 261(5)

[348] Regulation of Investigatory Powers Act 2000, s 1(1) and 1(A)(3) and Wireless Telegraphy Act 2006, s 48(1)(4), Intelligence Services Act 1994, s 3(1)(a), and Security Service Act 1989, s 1(2)(3)

'storing' under RIPA. In 2013, the UK's Court of Appeal in *R v Coulson* ultimately held that electronic communications data is to be classed as being in the course of transmission, when it is stored on an Internet server.[349] This in turn means, that what may at first be generally considered to be content, such as an email, is in fact communications data, whilst it is being, or has been sent, or is in fact stored on an Internet server.

The impact of *Coulson* cannot be understated, as it permits UK law enforcement agencies' access to the contents stored on an Internet server. Storing information by this method has increased exponentially in the 21st Century, particularly since the introduction of the online 'Cloud' systems. These 'clouds' allow vast amounts of data to be stored, as covered in Chapter Two, such as that saved on smartphones or other smart devices, or word documents and research papers. It is debateable whether or not the definition of 'content' under the IPA has remedied this given it remains untested by the courts.

Bulk Communications Data: Interception, Collection and Retention

Bulk interception of electronic communications data was provided for under section 8(4) of RIPA. Section 136 of the IPA has now replaced these provisions, maintaining law enforcement capabilities and introducing further safeguards. The idea behind this power is to allow law enforcement agencies' to effectively monitor the Internet traffic and for the interception of large volumes of electronic

[349] *R v Coulson* [2013] EWCA Crim 1026.

communications in order to acquire the communications of terrorists and serious criminals that would not otherwise be available.[350] Should the warrant be authorised it could potentially establish links between known suspects, and also serve to increase the understanding of their behaviour. It could also assist law enforcement to understand new technologies, and how connections and multiple methods of electronic communications are made.[351]

It was argued during the IPA's passage through Parliament that the initial collection and retention of bulk data lacked the requisite necessity and proportionality, despite a warrant having been granted.[352] Anderson so much as agreed with this point, confirming that the, 'bulk powers are extraordinarily broad in scope'.[353] Eric King, the Director of 'Don't Spy On Us' voiced concerns with regards the level of interception practiced by GCHQ in particular, disproportionately that permits the collection of, '50 billion pieces of communication every single day'.[354] For King, it is this initial collection stage that lacks safeguards and accountability, and is deployed as a phishing exercise at the will of the security agencies.[355] He provided an example whereby GCHQ

---

[350] Operational Case for Bulk Powers, p26, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

[351] Draft Codes of Practice: Investigatory Powers Act 2016, Paragraph 6.3, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/561091/16-10-18_Interception_code_of_practice_draft.pdf accessed 8 December 2016

[352] *Supra* as per First sitting Committee Debate Session 2015-16, at Column 13

[353] *Ibid* at Column 7

[354] *Ibid* at Column 13

[355] *Ibid*

intercepted, '50 million pieces of webcam traffic', with three to eleven per cent of material containing undesirable nudity, under a computer programme named Optic Nerve.[356] Once collected, GCHQ, 'deployed facial recognition on it' without any further warrants being required'.[357] A computer programme completes this process, with little or no input from a human source.[358] With the processing complete, it is the next stage that requires authorisation via a targeted warrant.[359] In admitting that the security agencies however, require the power to collect data and analyse it, King confirmed that the more one knows and understands about the inner workings of the security agencies the 'more reassured' one becomes.[360] There certainly exists within the political establishment a clear difference of opinion between those that know and understand this work to those that do not in offering support for the IPA and increased State powers. Considering the sheer amount of terrorism related electronic communications data traffic and the successful expert use by IS as covered in Chapter Two, such powers are essential in reducing and combating the threat posed.

In procedural terms, a bulk interception warrant can be issued under section 136 of the IPA, should conditions A and B be met. Condition A represents the main purpose of the warrant, which must be one or more of the following:

[356] *Ibid*

[357] *Ibid*

[358] *Ibid* at Column 14

[359] *Ibid* at Column 13

[360] *Ibid* at Column 20

(a) the interception of overseas-related communications;
(b) the obtaining of secondary data from such communications.[361]

Condition B is that the warrant authorises the person to whom it is addressed to secure any of the following activities:

(a) the interception, in the course of their transmission by means of a telecommunication system, of communications described in the warrant;
(b) the obtaining of secondary data from communications transmitted by means of such a system and described in the warrant;
(c) the selection for examination, in any manner described in the warrant, of intercepted content or secondary data obtained under the warrant;
(d) the disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.[362]

Importantly the IPA defines secondary data in relation to communications, which could include:

1. messages sent between items of network infrastructure to enable the system to manage the flow of communications;
2. router configurations or firewall configurations;
3. software operating systems;
4. the period of time a router had been active in a network;
5. the location of a meeting in a calendar appointment;
6. photograph information.[363]

Interestingly, section 136(5) permits under the warrant the interception of communications that are not specifically described in the warrant. This means that law enforcement agencies' are able to use unconstrained methods not reliant upon the type of surveillance device being used or the type of communication

[361] Investigatory Powers Act 2016, s 136(2)

[362] Investigatory Powers Act 2016, s 136(4)

[363] Investigatory Powers Act 2016, s 137. See also Investigatory Powers Bill Explanatory Notes, p.50, 8 June 2016, available at http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040en.pdf accessed 8 December 2016,

being intercepted. Surveillance legislation has been somewhat hindered in the past, focused on the types of devices and surveillance techniques used. For example as evidenced in *Khan v UK*, the Interception of Communications Act 1985 (ICA) failed at the time to offer a progressive surveillance framework, instead being limited by surveillance technology such as cordless telephones and private networks.[364]

Bulk Acquisition

Following the same procedural authorisation process is section 158, which deals with the power to issue bulk acquisition warrants. According to the bulk acquisition draft code of practice, this type of warrant authorises the obtainment of electronic communications data from a communication service provider (CSP).[365] This may comprise of the systems data and the communications content.[366] Here the UK Government have introduced a two-stage process, firstly obtaining the bulk electronic communications data from a CSP, and secondly selecting from that data, communications to be examined.[367] This type of warrant is not targeted and thereby not constrained to a specific operation. It is therefore limitless in terms of the amount of electronic communications data that can be obtained. This is a seriously invasive power and as such only members of the

---

[364] *Khan v UK* [2000] 31 EHRR 1016, ECHR 195. See I. Leigh (1986) A Tappers Charter? *Public Law*, 8-18. See also *Effick* [1994] 99 Cr. App. R. 312, and *Halford v UK* [1997] EHRLR 540

[365] Bulk Acquisition Draft Code of Practice, Published for consultation alongside the Investigatory Powers Bill, Home Office, Spring 2016, at 1.2, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/505412/Bulk_Acquisition_draft_code_of_practice.PDF accessed 22 December 2016

[366] *Ibid* at 2.8

[367] *Ibid* at 3.1

security agencies can apply for the warrant, such as the Secret Intelligence Service and GCHQ.

The Type of Data: Access and Procedure

Two issues arise from both the bulk powers of interception and acquisition of electronic communications data. These are the type of communication and then the problems associated with Internet Connection Records (ICR). Firstly, once the electronic communications data is intercepted and then stored, law enforcement such as the Secret Intelligence Service can acquire the communications data under the IPA.[368] With similar provisions present to those governing interception, it must be evidenced that obtaining such electronic communications data is necessary for one of the purposes set out in the IPA, and that it is necessary and proportionate to do so.[369] Additional safeguards are provided currently by the office of the Interception Commissioner, currently the Rt. Hon. Sir Stanley Burnton, (although this position will be amalgamated to create a new Independent Investigatory Powers Commissioner), who oversees the security agencies arrangements for access to the data.[370]

Procedurally, in accessing the collected communications data, it is important to note at this point that the level of authorisation required depends on the level of information requested, and by whom. Public authorities for example, can only

[368] Investigatory Powers Act 2016, s 158(1)

[369] Investigatory Powers Act 2016, s 158(1)(b). See also Regulation of Investigatory Powers Act 2000, s 2(7)

[370] See https://www.mi5.gov.uk/interception-of-communications accessed 29 April 2016, and http://www.iocco-uk.info accessed 29 April 2016

request service use information and subscriber information. Policing and security agencies however, may be able to access all three types, dependent upon the specific agency. Whilst a designated police inspector may request and authorise subscriber information, only a superintendent may authorise a request for traffic data and service use information. In order to understand further, RIPA divides communications data into three categories:

1) ***Traffic Data*** that identifies the person or suspect, the apparatus used, and the location or address of where a communication is transmitted including the information about a computer file or a program, which has been accessed or run in the course of sending or receiving a communication.[371] Traffic data includes location software used by mobile telephones (geodata) when either stationary or moving, and private Wi-Fi networks. According to the Acquisition Code, website addresses beyond the Uniform Resource Locator (url) first slash are not traffic data, but classed as contents. IP addresses remain classed as traffic data;[372]
2) ***Service Use Information*** relates to the use of a specific telecommunications service. The service provider records and holds the usage frequency and specific details of the service used by the citizen, such as the amount of data downloaded;[373]
3) ***Subscriber information*** includes data such as their postal address, telephone numbers and email address. It can also cover their bank account data and personal information divulged at the time the citizen requested an account with the service provider.[374] [My emphasis]

However, providing the interception of electronic communications is necessary and proportionate, the law enforcement agencies' can use their powers of

---

[371] Regulation of Investigatory Powers Act 2000, s 21(4)(a), 21(6)

[372] Acquisition Code, paragraph 2.20 states, '…traffic data may identify a server or domain name (i.e. a web site) but not a web page'. As pointed out by the Interception of Communications Commissioners Office, there is a degree of ambiguity arising out of the absence of any definition of 'content' within RIPA. See the Interception of Communications Commissioner's submission to D. Anderson Q.C. (2015). Also note the Acquisition Code provides at 2.26 and at 42 that IP addresses can be stored by a service provider in conjunction with subscriber information, in which case it would need to be treated as subscriber information, not traffic data.

[373] Regulation of Investigatory Powers Act 2000, s 21(4)(b) and s 22(4)

[374] Regulation of Investigatory Powers Act 2000, s 21(4)(c)

interception through RIPA and the IPA, which is issued under any international mutual assistance agreement.[375]

Internet Connection Records: The definition and controversy

ICR's have caused some controversy and are covered specifically by section 62 of the IPA. According to the UK's Prime Minister Theresa May they are the modern day equivalent of an itemised telephone bill, a fact others uncompromisingly dispute.[376] The Shadow Home Secretary Andy Burnham for example has argued they are much more enlightening than an itemised bill, revealing an itinerary style that includes location data.[377] Regardless, May laboured the point that:

> …Internet connection records *do not* provide access to a person's *full web browsing* history. An Internet connection record is a record of what *Internet services a device* or person has *connected* to, not every web page they have visited.[378] [My emphasis]

ICR's however, are not a real record *per se*, or indeed similar to that of a call data record held by telephone service operators. At best they may be a collection of, or a subset of retained electronic communications data. The problem here is that 'an operator subject to a retention order will have to decide on a case-by-case basis what data the operator shall retain, and it will not be the same for all

---

[375] Regulation of Investigatory Powers Act 2000, ss 4, 6. See also Investigatory Powers Act 2016, ss 10, 15, 18, 20, 40, 56, and Schedule 9, 1

[376] House of Commons Second Reading, 15 March 2016, Column 830, available at http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0001.htm#16031546000001

[377] *Ibid*

[378] *Ibid* at Column 820

operators and could be very different indeed'.[379] The next issue is with regards the definition of ICR's under the IPA, whereby section 62(7) states that ICR's means communications data that:

> …may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and, comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).[380]

Clearly, as indicated in earlier text provided by the UK Government, ICR's will be used by law enforcement to identify the communications service to which a device is connected; in an attempt to close the capabilities gap as discussed in Chapter Two.[381] According to the Government an ICR does not represent a citizen's full Internet browsing history, only a record of the services connected to. Therefore, following this statement, an ICR would only show the URL up to the first slash, as in www.blarblarblar.co.uk, as opposed to www.blarblarblar.co.uk/isis/mosul. On this basis, 'it seems reasonable to assume that in relation to app-based access to the Internet via smartphones or tablets the ICR would include the activation of the app, but nothing further'.[382]

---

[379] Andrews and Arnold Ltd. (2015) Written evidence (DIP0001) submitted to the Joint Committee on the Draft Investigatory Powers Bill, available at https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf accessed 24 November 2016

[380] Investigatory Powers Act 2016, s 62(7)

[381] Draft Investigatory Powers Bill: Guide to Powers and Safeguards, November 2015, Cm9152

[382] P. Bernal, Supplementary written evidence (IPB0018) submitted to the Joint Committee on the Draft Investigatory Powers Bill, available at https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf accessed 24 November 2016

The definition of ICR's do not seem to be satisfactory in terms of precision and clarity, and the accompanying codes of practice offer no real practicable assistance as such. The IPA describes the functions of ICR's are to identify which 'person or apparatus is using an internet service where, the service and time of use are already known, but the identity of the person or apparatus using the service is not known'.[383] According to the IPA, ICR's can be used to identify which internet communications service is being used, and when and how it is being used, and by whom.[384] Finding who the specific person was who used the particular device is only possible however, by performing some sort of profiling. Additionally, the ICR could also be utilised to confirm the identity of the person who is obtaining access to, or running a computer file or computer program, which involves making available, or acquiring, material whose possession is a crime'.[385] For Bernal, all three examples of how ICR's can be used are 'poorly suited to performing these functions'.[386] ICR's can potentially carry more communications data than required, hence be more intrusive on the individual's privacy, and at the same time provide inadequate information to enable for law

[383] Investigatory Powers Act 2016, s 62(3)

[384] Investigatory Powers Act 2016, s 62(3)

[385] Investigatory Powers Act 2016, s 62(3)

[386] P. Bernal (2015) Supplementary written evidence (IPB0018) submitted to the Joint Committee on the Draft Investigatory Powers Bill, available at https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf accessed 24 November 2016

enforcement to make a decision as to whether or not target surveillance be initiated.[387]

Prime Minister Theresa May's statement is misleading therefore, because ICR's cannot simply be equated to an itemised telephone bills because they do not record whom a citizen has been communicating with.[388] Instead they show a record of websites visited which has the potential to reveal innocent intimate, personal and sensitive data.[389] The information that can be attained from this Internet history is much higher than an itemised telephone bill, with the potential to tell the citizens' political interests, general health, and sexuality. According to Bernal this, 'makes ICRs ideal for profiling and potentially subject to function-creep/mission- creep'.[390] It would appear that using ICR's in this fashion is the only way of accurately assessing the identity of the user. As covered in Chapter Two, IP addresses are useless to this regard. Because of the amount of information that an ICR can yield, it is not surprising that the Government would want potential access to it in preventing serious crime, and pre-empting a terrorist attack.

---

[387] *Ibid*

[388] *Ibid*

[389] *Ibid*

[390] *Ibid*

These powers are not only aimed at terrorism however, given that ICR's are often used to combat online child sexual exploitation.[391] Ministers Simon Hoare and Lucy Frazer noted that ICR's had led to the identification by police of at least 600 child abusers in the UK, where it was shown that, '92% of the communications data requested proved helpful'.[392] Anderson's 2015 report further highlights this fact, where only 1% of communications data was used in investigating terrorism, against 15 % used for sexual offences and vulnerable or missing persons.[393]

Terrorism	1%
Firearms and explosives	5%
Financial offences	10%
Sexual offences and Vulnerable or missing persons	15% (9% and 6%)
Harassment or stalking and Homicide, attempted murder & threats to kill	15% (7% and 8%)
Drugs offences	25%
Offences against the person and Offences against property	22% (11% for each)

[391] House of Commons Second Reading, 15 March 2016, Column 830, available at http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0001.htm#16031546000001

[392] First sitting Committee Debate Session 2015-16, Investigatory Powers Bill, Publications on the Internet, Column 13 and 20, 24 March 2016 available at http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160324/am/160324s01.htm accessed 30 August 2016

[393] *Supra* as per D. Anderson (2015) p.135

Other offences	7%

Table 1, percentage of electronic communications data used for specific crimes, taken from D. Anderson (2015) A Question of Trust: Report of the Investigatory Powers Review, London: The Stationary Office.

Internet Connection Records: Vulnerabilities

The problem with operators holding ICR data is the linked risk to criminality, meaning that the potential for new vulnerabilities are fashioned by the gathering and retaining of ICR's. In terms of cybercrime and cyber terrorism, the databases of ICR's could potentially be interfered with, or in other words hacked into, and used maliciously. The recent hacking of TalkTalk provides an example of this vulnerability to data privacy. According to news reports, as opposed to being carried out by professional criminals, it was in fact a bored 17 year old who wanted to 'show off'.[394] Cyber security is becoming increasingly important in the 21st Century, and it is concerning to note that some service providers do not have adequate high levels of security built in to their frameworks.[395] It is clear from news reports that, even for those that do have high levels of security, companies such as Apple and Sony, and some banking corporations, have all been vulnerable to hacking.[396] It therefore follows that ICR databases may provide an attraction

[394] See http://www.bbc.co.uk/news/uk-37990246 accessed 7 December 2016

[395] See http://www.bbc.co.uk/news/technology-38223805 accessed 7 December 2016. See also http://www.ispreview.co.uk/index.php/2016/06/uk-inquiry-threatens-fine-isps-internet-data-security-fails.html accessed 7 December 2016

[396] See for example: L. Bell (2016) Millions of Apple devices at risk of attack due to a security bug, Wired Cyber Security, 22 July 2016, available at http://www.wired.co.uk/article/apple-security-bug-hackers-steal-your-password accessed 7 December 2016. See https://www.ft.com/content/f6c1c0b3-af81-3ac8-812c-d26a66e5ba8a accessed 7 December 2016. See also https://hakin9.org/hacking-social-media-threats-vulnerabilities-threats-anti-threats-strategies-for-social-networking-websites/ accessed 7 December 2016

for cyber criminals. Additionally, the vulnerabilities are intensified by the potential for human error or internal corruption.[397]

Internet Connection Records and Open Source Intelligence: The privacy conundrum

Although the necessity of these bulk powers to attain ICR's have proved useful, it remains the case that electronic communications data surveillance represents the new contemporary method of collecting information about an individual. This is understandable given the growth in technology and the use of citizens', which continually expands as highlighted in Chapter Two. For Clarke, this has resulted in this type of surveillance becoming the guiding principle for 'social control, particularly by managing populations through collection, sorting, management and risk assessment of data.[398] Further evidence of this move is located in the 2008 Home Affairs Select Committee's report titled 'A Surveillance Society', where it was concluded that the 'foundation for all new surveillance is the database'.[399] According to Haggerty, data surveillance has moved from the traditional top-down, or panoptic state approach to more of an informational gathering exercise carried out by retailers, employers, insurers, HMRC, and

---

[397] *Ibid*

[398] R. Clarke (1991) *Information Technology and Dataveillance*, in C. Dunlop and R. Kling (eds), *Computerization and Controversy: Value Conflicts and Social Choices* (Academic Press, Inc. Waltham)

[399] Home Affairs Select Committee, A Surveillance Society? Fifth Report of Session 2007-2008 (HC 2008-2009 58-I)

information intermediaries such as social networks and online gaming companies.[400]

In a rather surprising twist law, enforcement agencies have copied the approach taken by private companies and implemented this use to their own procedures. Following the changes in technology, as Trottier proffers, data surveillance in terms of social media policing forms part of this new contemporary framework.[401] This move however, is essential in dealing with the issues raised in Chapter Two, concerning how terrorist groups communicate by exploiting social media and electronic communications. Considering private companies and private individuals use Open Source Intelligence and Social Media Intelligence, to monitor other people in way that might assist in private civil litigation matters, it is not a tall ask to permit the same ability for Law enforcement, in assisting them to prevent a terrorist attack.

Open Source Intelligence (OSINT) is defined as the collection, analysis and use of data from openly available sources for intelligence purposes.[402] Whilst there is some overlap, Social Media Intelligence (SMI or SOCMINT) involves the analysis of social media, Facebook and YouTube for example, in order to measure

---

[400] K. Haggerty (2006) *Tearing Down the Walls: On Demolishing the Panopticon*, in D. Lyon, *Theorizing Surveillance: The Panopticon and Beyond* (Willan). See R. Jones (2000) Digital Rule: Punishment, Control and Technology, *Punishment and Society* 2:5. See also R. Boyne (2000) Post Panopticism, *Economy and Society* 29, 285. See also W. Bogard (2006) *Welcome to the Society of Control*, in K. D. Haggerty and R.V. Ericson eds, *The New Politics of Surveillance Visibility* (University of Toronto Press)

[401] D. Trottier (2012) *Social Media as Surveillance: Rethinking Visibility in a Converging World,* (Ashgate Publishing)

[402] B.J. Koops, J. Hoepman and R. Leenes (2013) Open source intelligence and privacy by design, *Computer Law and Security Review* 29:676

and arguably monitor the 'millions of people digitally arguing, talking, joking, condemning and applauding online', in order to facilitate the identification of criminal activity, 'indicate early warning of outbreaks of disorder, provide information and intelligence about groups and individuals, and help understand and respond to public concerns'.[403] Considering IS's decentralised electronic communications strategy raised in Chapter Two, monitoring individuals that like or re-tweet for example, an IS's message is essential. They both represent the new 21st Century categories of intelligence used by the UK policing security agencies.[404] As above, private companies and individuals, for example a solicitor, also use this type of intelligence in identifying fraudulent civil claims for personal injury. Considering the extensive use of the Internet and open sources data, it is not surprising to see an increase in the utilisation for intelligence.

The Intelligence and Security Committee's report of 2015 highlighted the fact, that the Internet carries the communications of 2.4 billion Internet users. In one minute, those 2.4 billion transfer 1,572,877 gigabytes of data, including 204 million emails, 4.1 million Google searches, 6.9 million messages sent via Facebook, 347,222 posts to Twitter and 138,889 hours of video watched on YouTube.[405] This highlights the point that increasingly people are living their

---

[403] D. Omand (2012) #Intelligence, *Centre for Analysis of Social Media, Demos*, 24 April, available at http://www.demos.co.uk/project/intelligence/ accessed 22 August 2016

[404] D. Omand, J. Bartlett and C. Miller (2012) Introducing Social Media Intelligence, *Intelligence and National Security Review* 27:1

[405] Intelligence and Security Committee, Privacy and security: a modern and transparent legal framework, HC 1075 2014/15, 12 March 2015, paragraph 55

lives online. Having the ability to tap into this dearth of information has proved essential for law enforcement agencies'. To this end, the potential value of OSINT and SOCMINT available to law enforcement agencies' was first realised during the investigation into the London 2011 riots.[406] This allows for intelligence-led policing, where predictive analytical software is used to anticipate and predict crime.[407] According to the RUSI report of 2015, the majority of intelligence that was collected by UK policing and security agencies, up to 95%, originated from OSINT, not closed sources.[408] It could be argued that this is a much more cost-effective method of conducting electronic communication data surveillance.[409] James Clapper of the US Office of the Director of National Intelligence described social media in 2014 as being 'huge for intelligence purposes'.[410] Anderson also refers to the increasing use and central reliance on OSINT and SOCMINT in his 2015 report.[411]

---

406 P. Lewis *et al* (2012) *Reading the Riots: Investigating England's Summer of Disorder* (Guardianshorts, London School of Economics and The Guardian, London 2012) Chapter 8

407 C. Miller and S. Ginnis et al (2015) The road to representivity (Centre for the Analysis of Social Media at Demos/IPSOS Mori, September 2015) at http://www.demos.co.uk/project/the-road-to-representivity/ accessed 12 July 2015

408 The Royal United Services Institute (RUSI) A Democratic Licence to Operate: Report of the Independent Surveillance Review Panel of the Independent Surveillance Review, Whitehall Reports, 13 July 2015, available at https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review, paragraph 3.16

409 *Ibid*

410 See https://www.dni.gov/index.php/about/leadership/director-of-national-intelligence

411 *Supra* as per D. Anderson Q.C. (2015) p.55

This type of electronic communications data surveillance fits with the understanding of intelligence-led policing.[412] For Tilley, this represents the best practical way for the police to do business, 'more smartly, incorporating modern information technology and modern methods', involving 'developing and maintaining a detailed and up-to-date picture of patterns of crime and criminality in order to intervene most effectively'.[413] Fitting in further with the risk-management style of counterterrorism measures, intelligence-led policing has shifted from reactive to proactive in nature.[414] Examples of the operational and procedural side to OSINT and SOCMINT systems include the EU's Virtuoso OSINT software. This allows law enforcement agencies' to gather together OSINT and Raytheon's Rapid Information Overlay Technology (RIOT) in to one place, allowing assessments to be carried out quickly, by tracking an individual or group over different social networking sites.[415]

This area of surveillance lacks expressed legal regulation and legal analysis. The acquisition of OSINT and SOCMINT is carried out without the consent or perhaps knowledge of the user. Perhaps this is simply down to the assumption

---

412 N. Tilley (2008) *Modern Approaches to Policing: Community, Problem Orientated and Intelligence Led*, in T. Newburn, Handbook of Policing (Willan) pp.373-383

413 *Ibid*

414 T. Newburn, T. Williamson and A. Wright (2008) *Handbook of Criminal Investigation* (2nd edition, Willan) p.653.

415 B.J. Koops (2013) Police Investigations in Internet Open Sources: Procedural Law Issues, *Computer Law and Security Review* 29:654. See also, S. Vaughan-Nicols (2013) Raytheon Riot: Defence Spying is Coming to Social Networks, ZDNet, 12 February, available at http://www.zdnet.com/raytheon-riot-defense-spying-is-coming-to-social-networks 7000011191/, See also R. Gallagher (2013) Software that Tracks People on Social Media Created by Defence Firm, The Guardian, 10 February, available at http://www.theguardian.com/world/2013/feb/10/software-trackssocial-media-defence accessed 23 August 2016

that such open source information is accessible to the world, and therefore 'fair-game' for law enforcement surveillance. However, considering the amount of private, personal and intimate information disclosed via social media, coupled with the increase in police surveillance, often used to profile and target individuals autonomously, presents a serious concern in terms of privacy. Current surveillance laws do not regulate OSINT or SOCMINT, so they remain vague and underexplored. In assessing this issue, for Gillespie OSINT and SOCMINT do not require legal regulation because 'when postings are public and available for all to see it unlikely that it could be concluded that the viewing of the information is covert in that there must be an awareness that those in authority could look at the postings'.[416]

However, receiving little public attention or legal analysis, private information shared on a public format such as social media, remains private if one were to follow the framework of the EU's 2002 e-Privacy Directive, discussed at length in Chapter Four. Accordingly, Omand *et al* concluded that the use of OSINT and SOCMINT must be 'grounded in respect for human rights and the associated principles of accountability, proportionality and necessity'.[417]

---

[416] A. Gillespie (2009) Regulation of Internet Surveillance, *European Human Rights Law Review* 4, 552

[417] D. Omand, J. Bartlett and C. Miller (2012) Introducing Social Media Intelligence, *Intelligence and National Security Review* 27:1, 7. See also D. Omand, J. Bartlett and C. Miller for UK Cabinet Office (2010) A Strong Britain in an Age of Uncertainty: The National Security Strategy (HMSO 2010), p 5. See also G. Deleuze (1992) Postscripts on the Societies of Control, October Winter Ed 59:3

The US has led the key developments in this area, where a 2012 survey of 1,221 federal, State and local law enforcement agencies' highlighted four out of five enforcement professionals admitted to using SOCMINT in the course of their investigations.[418] Of the many stories provided, one in particular was emphasised whereby the law enforcement official stated that:

> …Further investigation (utilising Facebook) revealed the threats were credible and we conducted follow-up investigations, which revealed a student intent on harming others (detailed emails and notebooks). The student was in the process of attempting to acquire weapons. It's my belief we avoided a 'Columbine' type scenario.[419]

For Trottier, the EU Member States and UK have been slow to utilise fully OSINT and SOCMINT in comparison, describing it as still in a 'formative stage'.[420] It did however prove pivotal during the police investigation into the London Riots in 2011, where encrypted Blackberry instant messages and Twitter were used.[421] It was also interesting to see the police using social media to enhance the chances of identifying suspects, by creating a Flickr account and by

---

[418] LexisNexis® Risk Solutions (2012) Survey of Law Enforcement Personnel and Their Use of Social Media in Investigations. www.lexisnexis.com/investigations available at https://www.lexisnexis.com/risk/downloads/whitepaper/Infographic-Social-Media-Use-in-Law-Enforcement.pdf accessed 10 November 2016

[419] *Ibid*

[420] D. Trottier (2015) Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques, *European Journal of Cultural Studies* 18:4-5, 542.

[421] V. Dodd (2011) Police accessed BlackBerry messages to thwart planned riots, The Guardian, 16 August 2011, available at https://www.theguardian.com/uk/2011/aug/16/police-accessed-blackberry-messages-thwart-riots accessed 10 November 2016, see also K. Wynn and K. Blyth (2011) Predicting a riot: at what price privacy? Practical Law Company, available at http://uk.practicallaw.com/9-507-6354, see also C. Williams (2011) London Riots: BlackBerry Manufacturer offers to help police, Telegraph, 8 August 2011, available at http://www.telegraph.co.uk/technology/blackberry/8689313/London-riots-BlackBerry-manufacturer-offers-to-help-police-in-any-way-we-can.html. See also J. Ball and P. Lewis (2011) Twitter and the Riots: How the News Spread, The Guardian, 7 December 2011 available at http://www.theguardian.com/uk/2011/dec/07/twitter-riots-how-news-spread accessed 23 August 2016

posting pictures they effectively conscripted the public to assist in the identification of individuals.[422] Although perhaps beyond the ambit of the thesis, police forces across the UK have recently created Facebook accounts and often post pictures of wanted suspects.[423] Exact figures are difficult to attain, as is the actual effectiveness however, in 2012 a news report suggested that there were 4,908 reports in which Facebook and Twitter were factored.[424]

Similar to the US, as part of OSINT and SOCMINT, the UK has started to use predictive profiling technological systems such as the IBM Predictive system.[425] In 2013, the UK launched the EMOTIVE project using an OSINT approach whereby the experimental automated software scanned up to 2000 tweets per second.[426] In response to the potential growth in utilising open sources as part of law enforcement intelligence, the UK College of Policing in 2015 issued guidance on its use.[427] It notes that 'open sources of information are widely available but

---

[422] J. Bartlett, C. Miller, J. Crump and L. Middleton (2013) Policing in an Information Age, Centre for Analysis of Social Media, Demos, March, available at http://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365 23 August 2016

[423] See https://www.facebook.com/cheshirepolice/?fref=ts&ref=br_tf accessed 30 December 2016. See also http://www.digitaltrends.com/social-media/the-new-inside-source-for-police-forces-social-networks/ accessed 14 February 2017

[424] See https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter and https://smallbiztrends.com/2015/12/police-using-facebook-to-solve-crimes.html accessed 30 December 2016

[425] T. Thomson (2010) Crime Software may help police predict violent offences, The Guardian, 25 July 2010, available at http://www.guardian.co.uk/uk/2010/jul/25/police-software-crime-prediction. See also IBM (2010) Ministry of Justice Chooses IBM Predictive Analytics to Make Streets Safe, IBM Press Release, 16 March 2010.

[426] BBC News (2013) Computer Program uses Twitter to map mood of nation, 7 September 2013, available at http://www.bbc.co.uk/news/technology-24001692 accessed 31 July 2016

[427] College of Policing (2015) Intelligence collection, development and dissemination, available at https://www.app.college.police.uk/app-content/intelligence-management/intelligence-cycle/ accessed 23 August 2016

may not be accurate, reliable or valid'.[428] Despite this, when used in conjunction with other intelligence sources, it has been proved to be useful in seeking a prosecution for terrorist offences.[429] This was seen recently with the prosecution of Anjem Choudary and Mohammed Rahman, following their online posts on YouTube, Twitter and on an extremist website, encouraging support for the IS terrorist group.[430] Whilst this is an important point, Choudary was a key figure in al-Muhajiroun, a group that was proscribed by the UK. Choudary was prolific in his quest, constantly re-inventing the group using different names following continuous proscription. Some of the names used were Ghurabaa, Isman4UK, and Muslims Against Crusades. In supporting IS law enforcement assessed 20 years' worth of material, held on 333 electronic devices containing 12.1TB of data.[431]

The law enforcement agencies' use of OSINT and SOCMINT has yielding some positive results. Concerns turn on two specific points however, being they potentially lack legal regulation and privacy safeguards. It terms of legal regulation, it is not as simple to merely state the information in the public domain is fair-game for authorities to use as part of their data mining or profiling exercises, as this should almost be expected. Rules exist through RIPA, the IPA

---

[428] *Ibid*

[429] *Ibid*

[430] J. Grierson, V. Dodd and J. Rodrigues (2016) Anjem Choudary convicted of supporting Islamic State, The Guradian, 16 August, available at https://www.theguardian.com/uk-news/2016/aug/16/anjem-choudary-convicted-of-supporting-islamic-state accessed 20 September 2016

[431] V. Dodd (2016) Anjem Choudary jailed for five-and-a-half years for urging support for ISIS, The Guardian, 6 September 2016, available at https://www.theguardian.com/uk-news/2016/sep/06/anjem-choudary-jailed-for-five-years-and-six-months-for-urging-support-of-isis accessed 30 December 2016

and the other Acts of Parliament as per above, controlling access to electronic communications data and equipment inference discussed below. Bartlow, drawing on Semitsu's words, confirms that:

> Facebook is a giant surveillance tool, no warrant required, which the government can use in a mind boggling creative range of ways with almost no practical constraints from existing laws.[432]

Whilst there may be some obviousness to the fact that SOCMINT should not require privacy protection, Edwards and Urquhart note three rebutted points.[433] First is the potential it greatly advances intelligence in terms of data mining and profiling. This is because, in addition to pictures, videos and interest links, the authorities peruse through the individuals friends list, or follows and followers, in order to draw up a type of social graph.[434] Another important point to mention is the fact some social media sites automatically post an individual's location upon posting.[435] This type of profiling, could lead authorities to draw a 'guilty by association' conclusion. Inferences can also be drawn from this type of data, utilising software such as EMOTIVE, whereby the analysis is done through automated algorithmic means targeting online behaviours, rather than involving at that early stage, human scrutiny. It has been evidenced that an analysis of

---

[432] J. Semitsu (2011) From Facebook to Mug Shot: How the Death of Social Networking Privacy Rights Revolutionized Online Government Surveillance Pace Law Review 31:1, 291-381. See also A. Bartow (2011) Facebook and the Fourth Amendment: Expecting Any Privacy May be Unreasonable, Jotwell, 18 April 2011, available at http://cyber.jotwell.com/2011/04/ accessed 30 December 2016

[433] L. Edwards and L. Urquhart (2015) Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence? *Social Science Research Network*, p.14

[434] *Ibid*

[435] *Ibid*

Facebook 'Likes' can be used to indicate the most sensitive of data including sexuality for example. According to a recent study carried out at Cambridge University, 'by mining Facebook Likes, the computer model was able to predict a person's personality more accurately than most of their friends and family'.[436]

The second point surrounds the reliability of the content posted on social media. One may find oneself 'tagged' in a picture that is either not you, or has been doctored to a severe extent.[437] One can also be added to groups and pages without actually accepting the invitation.[438] The third and final observation point revolves around the constant changes in social media platforms that require the user to update their privacy settings regularly. As highlighted by Edwards and Urquhart, 'different privacy settings and different changes, apply to different types of content, such as posts, comments, groups, photos and friends lists'.[439] It is both well known that some users are deluded in their belief that all the information on social media is private, and that they have protected themselves adequately by updating their security settings.[440] For these reasons, it is argued this, 'contributes strongly to an argument that material placed on social media can still carry with it reasonable expectations of privacy'.[441] This is continually highlighted through Facebook for example, whereby despite reassurances that information added to

[436] See http://www.cam.ac.uk/research/news/computers-using-digital-footprints-are-better-judges-of-personality-than- friends-and-family#sthash.OSQ8dqdr.dpuf accessed 7 December 2016

[437] *Ibid* at p.15

[438] *Ibid*

[439] *Ibid*

[440] *Ibid*

[441] *Ibid* at p.16

Facebook will remain safe and secure, some users post a meaningless notice re-affirming their privacy.

Figure 13 taken from https://blog.malwarebytes.com/cybercrime/2016/10/facebook-will-make-all-posts-public-not/ accessed 8 December 2016

Despite the UK Government recent ability to provide legal regulation, there remains no specific guidance, or indeed a mention in the UK surveillance legislation regarding the acquisition of OSINT and SOCMINT data. There is furthermore little evidence to suggest the policing authorities consider them as constrained by RIPA, or now the IPA by extension.[442] This is not surprising given that open sources can be used by anyone, such as an employer who can Google search a prospective employee and access their social media, without a warrant or authority. Therefore, one might argue why law enforcement state

[442] *Ibid*

agencies be handicapped by having to obtain an authority, not forgetting that access to such communications data could save citizens' lives.

Considering the reality of social media's use it could be argued such data collection should fall within the meaning of RIPA and IPA, meaning that it is treated the same as covert and intrusive, and thereby within the remit of interception of communications data.[443] This would create a safeguarding level of protection for an individual's privacy, requiring the same authorisations, and internal and external controlling mechanisms. Floinn and Ormerod purpose an interception warrant be necessary, especially when policing authorities utilise 'backdoor' methods, by means of equipment interference, in order to acquire direct messages send through social media.[444] Whilst one could assume such messages are no longer within the definition of communications data, section 2(7) of RIPA extends the period of transmission to 'anytime when the system is used for storing it in a manner that enables the intended recipient to collect it or otherwise have access to it'.[445] This would fit with the earlier mentioned case *R v Coulson* where it was held voicemail messages stored for future use remained in transmission.[446] The impact of the IPA on this legal authority is as yet unknown.

---

[443] M. O'Floinn and D. Ormerod (2011) Social networking sites, RIPA and Criminal Investigations, *Criminal Law Review* 10:766

[444] *Ibid*

[445] Regulation of Investigatory Powers Act 2000, s 2(7)

[446] *R v Coulson* [2013] EWCA Crim 1026

What is clear from RIPA and the IPA is the fact that the main aim is to intercept communications data in 'real time'. This is essential to law enforcement in keeping up with the potential terrorists, and allows them to pre-empt the next step, as the terrorists' progress with their plans. It remains unclear if an interception warrant would be appropriate, given it would have to remain in place for an indefinite period. For Edwards and Urquhart it 'remains an open problem if an interception warrant could appropriately be issued after a social media post had been read and perhaps replied to'.[447] This could have further impact on an individual's right to privacy and data protection, particularly for those not suspected of criminal activity. Access to this type of data is invaluable to the UK's policing and security agencies. It has been shown that the intrusive power of communication interception is one of the most important techniques that can be used, by only a small number of policing agencies for specific purposes, in the investigation of terrorism.[448] It is in this sense that interception of communications data, OSINT and SOCMINT, supports criminal investigations by providing pivotal intelligence.[449] The Director-General of the Office of Security and Counter-Terrorism (OSCT) pointed out the importance this power permits:

> Intelligence [from interception] has led *directly* to the prevention of terrorist attacks and serious crime, the success of operations aimed at countering the proliferation of weapons of mass destruction and the saving of lives. Overall, RIPA interception is a *critical tool* in

---

[447] L. Edwards and L. Urquhart (2015) Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence? *Social Science Research Network*, p.18

[448] Intercept as Evidence, The Office for Security and Counter-Terrorism, (Cm 8989, December 2014), A report by a Committee of Privy Counsellors led by the Rt. Hon. Sir John Chilcott, at p.4

[449] *Ibid*

> investigations into the full range of threats to national security.[450] [My emphasis]

In Anderson's 2015 report, policing and security agencies in the UK laboured the point that inception was vital to the success of their work. Of this the Security Service said that interception powers were crucial where intelligence gained is unique to electronic communications data.[451] According this would be hard to replicate.[452] The National Crime Agency (NCA) went further and confirmed that the intelligence gathered from interceptions electronic communications data assisted them in prioritising their work. They continued:

> …For some areas of NCA activity…there are *no practical alternatives* to using…interception…In 2013-14, interception played a *critical role* in investigations that resulted in…Over 2,200 arrests; Over 750kg of heroin and 2,000kg of cocaine seized; Over 140 firearms seized; and Over £20,000,000 seized. Police impressed upon [Anderson] that intercepted material may be useful in other types of cases, ranging from corruption investigations to domestic murder.[453] [My emphasis]

The Director General of the Security Service in response to Rifkind's 2013 report into access to communications data stated:

> …access to communications data of one sort or another is very important indeed. It's part of the backbone of the way in which we would approach investigations. I think I would be accurate in saying there are no significant investigations that we undertake across the service that don't use communications data because of its ability to tell you the who and the when and the where of your target's activities. It tends to be relatively reliable. It's relatively accessible at the moment in a number of areas, and from our point of view it's a very, very important capability…[454]

---

[450] *Supra* as per D. Anderson Q.C. (2015) p.126

[451] *Ibid* at, p127

[452] *Ibid*

[453] *Ibid* at, p127

[454] The Rt. Hon. Sir Malcolm Rifkind MP (2013), Intelligence and Security Committee, Access to communications data by the intelligence and security Agencies, February 2013, Cm8514, p.9

Whilst it is accepted there are issues and concerns over citizens' data protection and privacy rights, the key points raised here and in Chapter Two, highlight the fact that in today's communications culture and issues related to law enforcement having to carry out surveillance, these powers are essential. Safeguarding a citizen's right to life must be law enforcements primary concern. Data protection and privacy rights must at these times take a back seat. In order to access some types of communications data, such as emails that have not been sent but rather simply saved on the server, or on a note taking application on the smartphone device, law enforcement argue they need the power to interfere, or otherwise hack into the equipment.

BULK EQUIPMENT INTERFERENCE: COMPUTER NETWORK EXPLOITATION

Bulk equipment interference is currently provided for under the section 176 of the IPA and sections 5 and 7 of ISA. According to the UK Government, equipment interference is used increasingly by law enforcement to mitigate the inability to acquire intelligence through conventional bulk interception, and to access data directly from computers and other devices, which may never have otherwise have been obtainable. Alongside the proposed power comes another draft code of practice made pursuant to the IPA.[455] These types of warrants are only available

[455] Equipment Interference Draft Code of Practice, Home Office, Spring 2016, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504238/Equipment_interference_draft_code_of_practice.PDF accessed 30 December 2016

for operations overseas, whereby an example put forward illustrating the use states:

> Intelligence suggests that a [Islamic State]-inspired cell in a particular location in the Middle East is plotting an imminent bomb attack against UK interests in the region. Little is known about the individual members of the terrorist cell. However, it is known that a particular software package is commonly – but not exclusively – used by some terrorist groups. After using equipment interference to obtain equipment data from a large number of devices in the specified location, analysts apply analytical techniques to the data, starting with a search term ('selector') related to the known software package, to find common factors that indicate a terrorist connection. A series of refined searches of this kind, using evolving factors that are uncovered during the course of the analytical process, gradually identify devices within the original 'pot' of data collected that belong to the terrorist cell. Their communications (including content) can then be retrieved and examined. As the cell members can only be identified through a series of refined searches that cannot all be assessed in advance at the time the warrant is issued, second stage access controls are required to govern all of the data selection within the operation. Accordingly, a bulk equipment interference warrant is suitable.[456]

For Anderson however, the UK Government has failed in this instance to make its case evidencing the need for this bulk power.[457] He goes onto emphasise, the differences between the targeted equipment interference power and the bulk, where he notes his concerns lie 'particularly in relation to equipment interference, in that, if one looks at the so-called targeted power and, in particular, at its potential thematic use, it is quite extraordinarily broad'.[458] 'The code of practice indicates that the power is very broad indeed and that matters because the

---

[456] *Ibid*

[457] First sitting Committee Debate Session 2015-16, Investigatory Powers Bill, Publications on the Internet, Column 6, 24 March 2016 available at http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160324/am/160324s01.htm accessed 30 August 2016

[458] *Ibid*

safeguards on the targeted power are less than the safeguards on bulk. For a start, you do not need to be aiming only at somebody outside the UK, or people outside the UK. You can quite properly target it inside the UK'.[459]

Bulk Equipment Interference: 'Legalised hacking'

Following the *R v Coulson* authority, procedurally utilising Computer Network Exploitation (CNE) or Equipment Interference, the UK policing and security agencies can legitimately hack into Internet servers, such as cloud storage systems, and view the content without the person affected knowing.[460] Martin raises two complaints that were made by Privacy International and a global coalition of Internet Service Providers (ISP) claiming the UK's GCHQ lacked clear lawful authority to conduct specifically CNE operations.[461] Since Martin's assessment, the enactment of the IPA and the *Coulson* case, the government has introduced the Equipment Interference Code of Practice 2016, which confirms that an application must be made under s5 or s7 of the Intelligence Services Act 1994:

> …a warrant under section 5 of the [ISA] should be sought wherever members of the Intelligence Services, or persons acting on their behalf or in their support, conduct equipment interference in relation to equipment located in the British Islands that would be otherwise unlawful…If the equipment is located outside the British Islands, and the interference would be otherwise unlawful, the Security Service should seek a warrant under section 5 of the 1994 Act. In the case of SIS [Secret Intelligence

---

[459] *Ibid*

[460] *R v Coulson* [2013] EWCA Crim 1026

[461] A. J. Martin (2105) GCHQ v Privacy International: Computer hacking tribunal showdown begins, The Register, 1 December 2015, available at http://www.theregister.co.uk/2015/12/01/gchq_privacy_international_investigatory_powers_tribunal/ accessed 13 May 2016

> Service/MI6] and GCHQ, an authorisation under section 7 may be obtained instead of a warrant under section 5.[462]

Bulk equipment Interference introduces in essence legalised hacking and is perhaps one of the most intrusive powers available to law enforcement. The fact these powers can be used on mass potentially places a camera into people's homes by hacking into their personal computers and smartphones, and activating them. The 21st Century citizen, for the main part at least, is totally reliant of their use of technology. The amount of sensitive data people store on their smartphones and other devices continually increases, and at the same time the sophistication and fortitude of cyber criminals has increased. In order to facilitate access to people's smartphones and other devices, the IPA sets the scene introducing two new powers, the national security notice and the technical capabilities notice. Both these elements target applications providers and encryption. In contrast, two points are prevalent. Firstly it would be logistically impossible, in terms of law enforcement resources to hack into every citizen's piece of digital equipment, and secondly as pointed out in Chapter Two, terrorists are using encryption to hide their electronic communications data.[463] This means that smartphones and other smart devices, once decrypted, may hold vast quantities of, and quality intelligence essential to law enforcement.

---

[462] Equipment Interference Code of Practice, Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000, January 2016, Home Office, London: TSO, paragraphs 4.1 and 4.2, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf accessed 30 December 2016

[463] See http://www.telegraph.co.uk/news/uknews/1494190/MI5-we-did-not-receive-a-warning.html accessed 30 December 2016

The Equipment Interference Code of Practice has been introduced to also assist those working in counterterrorism to understand the procedure.[464] This code is one of many newly introduced by the Government that clearly show the authorisation processes that must be taken by the policing and security agencies. It worth mentioning here that the Security Service is governed by the Security Service Act 1989 and is primary concerned with internal threats to the UK's national security. The Secret Intelligence Service (more commonly referred to as MI6) is governed by the Intelligence Services Act 1994, and are primarily concerned with external threats by obtaining and providing information relating to the actions or intentions of persons outside the British Islands, and to perform other tasks relating to the actions or intentions of such persons in the interests of national security.[465] Under the same authority, GCHQ's functions are to monitor or interfere with electromagnetic, acoustic and other emissions, and to obtain and provide information derived from or related to such emissions or equipment, and from encrypted material in the interests of national security, or in support of the prevention or detection of serious crime.[466] The service's role here is essential, particularly in the 21st Century and when analysing the issues highlighted in Chapter Two, with regards the monitoring of electronic communications data.

---

[464] *R v Coulson* [2013] EWCA Crim 1026, see also Equipment Interference Code of Practice, Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000, January 2016, Home Office, London: TSO, paragraphs 4.1 and 4.2, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf accessed 30 December 2016

[465] *Ibid*

[466] *Ibid*

Broad Powers with Restricted Use and Access: Evidence of necessity

Within this broad yet restricted framework, according to the security agencies, accessing communications data or other information saved on computers or other devices, plays a pivotal role in gaining valuable information, allowing them to build an accurate picture of the suspect, and serves to make up for the loss of intelligence that may otherwise be unobtainable through other surveillance techniques, such as end to end encryption.[467] Therefore 'it can sometimes be the only method available by which the security services can acquire the data'.[468] The Rt. Hon. Sir Malcolm Rifkind's research findings into the murder of Fusilier Lee Rigby on the 22nd May 2013, found that such bulk powers allow the security services to see what the suspect has been looking at and downloading from the Internet.[469] One of the terrorists, Adebowale in fact came under the security services gaze following his interest in online extremist material.[470] Although parts of Rifkind's report has been sanitised, it appears rather clear that in addition to the many extremist publications available online, Adebowale had been looking at 'Inspire' magazine, created by al-Qaeda in the Arabian Peninsula (AQAP) to disseminate extremist information on the internet in English.[471] According to the Security Service in 2012-13:

---

[467] *Ibid*

[468] *Ibid*

[469] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) p.59

[470] *Ibid* at p.59

[471] *Ibid* at p.59-60

> Inspire seeks to promote home-grown *lone actor* attacks, providing the ideological backing and *practical* instruction for users to commit attacks... [It] presents a variety of risks to the UK, including providing *** [sanitized text] instruction for violent attacks…we can now say that Inspire has been read by those involved in at least *seven out of the ten attacks* planned within the UK since its first issue [in 2010]. We judge that it significantly enhanced the capability of individuals in four of these ten attack plots…[472] [My emphasis]

Despite these findings, it is interesting to note that the Security Service would not carry out any intrusive surveillance on of individual if they had only read the Inspire or Dabiq magazine. This is where we see the term proportionality added to necessity, as the Security Service confirm it would not be sufficient to qualify for intrusion.[473] Some individuals may well simply look at the material to satisfy their curiosity or perhaps have extremist views and enjoy reading it. However, there is no precise way at that stage of knowing if they are using the material in an instructive way to plan and carry out an attack. The Security Service confirmed:

> That whilst there is a potential risk posed by those who access extremist media, they also caution that it does not follow that everyone who does so then engages with violent extremism.[474]

Through the IPA authorities, law enforcement must evidence that the action required is necessary and proportionate.[475] Both are international human rights principles that must be applied to electronic communications data surveillance. Representing an ECHR mechanism, any interference with a qualified right, in this case Article 8 the right to privacy must be 'necessary in a democratic society'.

---

[472] *Ibid* at p.60

[473] *Ibid* at p.60-61

[474] *Ibid* at p.61

[475] Investigatory Powers Act 2016, s 227

This means that law enforcement must show a 'pressing social need', in addition to showing that the action required is proportionate. When reviewing these essential elements it becomes quite clear that the threshold is reasonably high, in terms of authorising state action. The disparity between those who merely read a terrorist publication and intend no violent action, to those that intend to carry out violence is limitless. It is therefore questionable as to whether merely engaging with online extremist material such as Inspire or Dabiq, should be considered as sufficient grounds to justify intrusive action.[476]

The End of Encryption: National security and technical capabilities notices

Towards the end of the IPA lies perhaps one of the most intrusive powers ever placed on the statue book. The 'national security notice' places an operator under an obligation to carry out any conduct, including the provision of services or amenities, facilitating anything done by the intelligence service.[477] Comparable to the provision of bulk powers, the Secretary of State must make the order based on proportionality, which then must be approved by an independent Judicial Commissioner.[478] Should the action be proportionate and necessary, there is in essence no time limit applicable within the IPA, simply what the Secretary of State feels is reasonable.[479] This means that any notice could last three days, or three months or three years. However, judicial authority will be required, which

[476] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) p.61

[477] Investigatory Powers Act 2016, s 252(3)

[478] Investigatory Powers Act 2016, s 252(1)

[479] Investigatory Powers Act 2016, s 252(7)

should safeguard this power from any type of abuse. Likewise, under s252 of the IPA, the Secretary of State can give any relevant service operator a 'technical capability notice'. Following a Judicial Commissioners approval, should the Secretary of State consider the necessity of the notice is required and proportionate; he may impose an obligation onto the operator to remove any electronic protection applied.[480] Otherwise known as encryption, this power places the operator under the obligation to decrypt the communication or device, permitting law enforcement agencies' unrestricted access as per the conditions of the notice. This power can be imposed extra-jurisdictionally, which places many operators in a difficult position in terms of privacy protection requirements.[481] It also has the potential to weaken the security model of many device and applications providers.

Dealing with the latter point, as discussed in Chapter Two encryption is as ubiquitous as computing itself, and many people and companies rely on it for security. Apple in particular noted their concern that removing encryption will put law-abiding citizens' at risk from cyber criminals, rather than actually affect the cyber criminals who can continue to access other means of encryption.[482] As with ICR, equipment interference could also impede the operation of smartphones

[480] Investigatory Powers Act 2016, s 253(5)(c), and s 254

[481] Investigatory Powers Act 2016, s 253(8)

[482] Apple Inc. and Apple Distribution International—written evidence (IPB0093) submitted to the Joint Committee on the Draft Investigatory Powers Bill, available at https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf accessed 24 November 2016

and other devices, rendering that particular device or server easier for criminals to access. Apple states that, 'surely such an intrusive power, if allowed at all, should only be targeted at the most serious of criminal suspects', rather than on mass that overwhelmingly and inevitably includes innocent people.[483] Apple in fact made a formal submission to the UK Joint Committee saying:

> We believe it would be wrong to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat. In this rapidly evolving cyber-threat environment, companies should remain free to implement strong encryption to protect customers.[484]

It could also affect their position in the international sense given many Internet service providers are located overseas, meaning they are put in the impossible position of choosing which law and which authority to follow, and which to disregard. Apple for example has offices registered in Ireland, meaning they are subject to EU data protection laws, and the USA where US law controls access to that data by law enforcement. Any failure to follow requirements under Title III of the US Omnibus Crime Control and Safe Streets Act, would subject Apple to criminal sanctions for any unauthorised interception of content in transit.[485] What must be remembered here of course is that the EU has been instrumental in

---

[483] *Ibid*

[484] Joint Committee on the Draft Investigatory Powers Bill (2016) Report of Session 2015-2016, 11 February, HL Paper 93 and HC 651 available at http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm. See also http://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/

[485] Apple Inc. and Apple Distribution International—written evidence (IPB0093) submitted to the Joint Committee on the Draft Investigatory Powers Bill, available at https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf accessed 24 November 2016

forming UK data protection law since 1995, so it may be likely that the IPA powers are compatible.[486] These issues will be returned to when assessing the IPA's legitimacy with EU law.

Bulk Personal Datasets

For now it is important to discuss the issue of bulk personal datasets facilitated by section 199 of the IPA, that have created quite a lot of criticism surrounding the authorisation and safeguards, and the storage of such information, along with the legitimate security risks of illegal hacking. The datasets represent information that includes personal data relating to a number of individuals. As with all proposed bulk powers, initially an automated computer programme processes the data, filters out the unnecessary and unwanted information, and effectively serves to profile individuals.[487] Lynskey contends that this may be abused if adequate safeguards are not placed correctly, and 'that decisions based on processing such datasets may profoundly affect individuals without their knowledge or consent' falling within the data protection scope.[488] Accordingly the IPA is antithetical towards data protection, conflicting with an individual's autonomy and personality-enhancing aspects, by facilitating profiling.[489] The IPA distinguishes

---

[486] R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [6]-[8], [11]

[487] O. Lynskey (2015) Beyond privacy: the data protection implications of the IP Bill, LSE Law Department Briefings on the Investigatory Powers Bill, LSE Law Policy Briefings, 15, Social Science Research Network, available at http://ssrn.com/abstract=2704299

[488] *Ibid*

[489] *Ibid*

between ‘specific’ and ‘class’ bulk data sets.[490] For Lynskey, ‘specific’ could mean for instance the national insurance number database, and the ‘class’ could be ‘all information held by football clubs about their season ticketholders, or CCTV data held by local borough councils’.[491] The proposed introduction of these powers caused political concern with regards access to health records. Section 206 of the IPA does introduce additional safeguards for such information, where an explicit reason for such collection and access be made by a statement from the head of the intelligence service.

Additionally, this type of mass surveillance profiling sits uneasy with rights such as the presumption of innocence and freedom from discrimination.[492] This is simply because the profiling computer programme used, authorised by the initial warrant, effectively singles out an individual based on the fact he is part of a group or has particular characteristics, ‘that correlate to suspects or persons of interest to the security and intelligence agencies, and cannot therefore have negative freedom’.[493] According to Lynskey, the individual, ‘may not know they a part of a group, or why this group is set apart from others, and he also may not know what future impact this categorisation might have on him. This Kafkaesque scenario shall become a reality for some UK residents under the IPA’.[494]

---

[490] Investigatory Powers Act 2016, s 204 Class BPD warrants, and s 205 Specific BPD warrants

[491] *Supra* as per O. Lynskey (2015)

[492] *Ibid*

[493] *Ibid*

[494] *Ibid*

According to the Security Service, the personal datasets are held for analysis whereby analysts will 'only look at the data relating to the minority who are of intelligence interest'.[495] Therefore, although a large number of individuals may have personal information stored, for the majority of cases this will never actually be looked at. They form an essential element in the identification of subjects of interest, or other individuals who 'surface during the course of an investigation'.[496] This assists the Security Service to establish communicational links between terrorist groups and potential terrorists, allowing them to filter out innocent citizens' as quickly as possible, focusing instead on those that pose a threat. According the Security Service confirm:

> The analysis of BPD is a critical part of our response to the increasingly complicated and challenging task of defending the UK's interests and protecting its citizens' in a digital age.[497]

The main aim is to protect citizen's lives and ultimately, this is what the bulk powers are trying to achieve. This is not a new power and the Security Service has been carrying out this function since the enactment of the SSA 1989. At this point it is perhaps relevant to discuss positive case studies illustrating these powers in the practical sense.

---

[495] See https://www.mi5.gov.uk/bulk-data accessed 12 December 2016

[496] *Ibid*

[497] *Ibid*

Financially, these powers have made an impact on the amount of fraud committed in the UK, whereby the, 'HMRC started using interception to support investigations into MTIC fraud. As a result the level of attempted fraud has reduced substantially from an estimated high of £5 billion in 2005/2006 to an estimated current figure of £750 million'.[498] Moving back to the terrorist threat in the late 2000s, bulk data enabled GCHQ to trigger a manhunt for a known terrorist linked to previous attacks on UK citizens'. At a time when other intelligence sources had gone cold, GCHQ was able to pick up the trail by identifying patterns of activity online believed to be unique to the suspect. Follow-up searches of bulk data provided further leads for the investigation. This work in turn highlighted links to extremists in the UK. Through a series of arrests, the network was successfully disrupted before any attack could place'.[499] Similarly in 2010 a UK 'intelligence operation identified a plot, which came from the top of al-Qaida's leadership structure, to send out waves of operatives to Europe to act as sleeper cells and prepare waves of attacks' using a unique communications method.[500] Working with international partners, GCHQ was able to identify operatives by querying bulk data collection for these distinctive communicative patterns.[501]

---

498 D. Anderson, (2015) *A Question of Trust: Report of the Investigatory Powers Review* London: The Stationary Office, p337

499 *Ibid*

500 *Ibid*

501 *Ibid*

It has been said by the UK's intelligence community that the nature of the international Islamist terror threat means that bulk data is the, 'first and last line of defence'.[502] The same has been said for the retention of such data collected where the studies have shown they can be put to great use in preventing and detecting serious crime.[503] One particular case study highlighted that:

> 'UK authorities received intelligence from US authorities that an individual using email had sent a movie file of a woman sexually abusing a four-month-old girl. The log-on IP address for this account was registered to a male from Northampton. Further enquiries established that a girlfriend of the individual had three children all less than four years old. After investigation both were convicted of the serious sexual abuse of the children'.[504]

This shows the necessity for bulk powers in terms of pre-empting crime and terrorist activity.

Terrorist Communication: The Rationale for Bulk Powers

Due to the terrorist group IS's propaganda and marketing campaign, coupled with the encryption capabilities, leads to a situation whereby it has become difficult to distinguish friend from foe. Determining who is and who is not a potential terrorist has become increasingly difficult in the 21st Century. Porous borders within the EU, and terrorist attacks committed within the EU and the UK, by EU and UK citizens', also known as 'home-grown', or 'lone jihad', mean it has become increasingly difficult for the law enforcement agencies' to make this

---

[502] *Ibid*

[503] *Ibid*

[504] *Ibid* at pp339-340

determination.[505] Friend or foe is now the question and conjoined with the fact terrorists lack a specific typecast has led to the EU and UK adopting risk management strategies to pre-empt and thereby prevent a terrorist attack.[506] This is because this type of threat is posed from individuals outside of any terrorist organisational structure or franchise, and they could be relatively anyone within the UK and EU population, and could attack at any given moment. In identifying potential terrorists, the UK Security Service highlighted this difficulty as explained to Sir Malcolm Rifkind:

> In order to maximise our chances of detecting such individuals, we use a set of factors identified as being common, but not unique, to many lone actors: an inability to cope with stress and anxiety; a pre-existing history of violence; mental health issues; blaming others for (personal or group) grievances; an immediate need to act to rectify grievances; social isolation; and significant interest in extremist material encouraging lone actor attacks. We use the factors, drawing on psychologists in our Behavioural Science Unit (BSU) where appropriate, in conjunction with other intelligence to inform risk assessments.[507]

Traceability and Typecasting

The key problem facing the UK is the traceability and typecasting of potential terrorists. This threat is not exclusive to the UK and is reflective of a larger international problem. Moeckli and King propose that the main problem facing policing and security agencies is the overall lack of the traceability of the terrorist threat to a clearly defined group, such as ETA, or the many factions of the Irish

---

[505] C. Walker (2008) Know Thine Enemy as Thyself: Discerning Friend from Foe under Anti-Terrorism Laws, *Melbourne University Law Review*, Vol. 32, 275-301, 276. See also https://azelin.files.wordpress.com/2016/07/al-qacc84_idah-in-the-arabian-peninsula-e2809cinspire-guide-2-nice-operatione2809d.pdf

[506] *Ibid*

[507] The Rt. Hon. Sir Malcolm Rifkind MP, Report on the intelligence relating to the murder of Fusilier Lee Rigby, Intelligence and Security Committee of Parliament, HC 795, 2014 at p.81

Republican Army (IRA) based in Northern Ireland and the Republic of Ireland.[508] The 21st Century international terrorist threat emanates from stateless organs, ubiquitous in nature, aimed at threatening the value systems of the Western world, rather than showing a particular grievance aimed at a specific State.[509] Carter moves the analysis away from stateless groups and traces a new evolution of tactics, and subsequent growth in prevalence of the 'self-radicalised' terrorist, which commenced following al-Qaeda's successful attack on the United States on 11 September 2001.[510] Following this analytical line, Carter goes on to postulate that the current terrorist threat comes from individuals whom lack formal ties to international terrorist groups, such as al-Qaeda and al-Shabaab.[511]

Although terrorism emanating from foreign citizens' tasked by a stateless international terrorist organisation remains a threat, it is UK and EU citizens' that have been influenced or otherwise radicalised, who then go on to commit acts of terrorism within their home country, more commonly known as home-grown terrorists, or lone wolves or Islamists, that poses the most tangible menace. As above, it is important to note that the UK and EU are not the only western countries facing this type of threat. Carter and Carter furnish evidence for the transnational nature of this home-grown threat when they conclude that the same

---

[508] D. Moeckli & T. King (2010) Human Rights and Non-discrimination on the "War on Terror", Publication Review, *European Journal of International Law* 1109-1111, 1109. For ETA see https://thebluereview.org/rise-fall-eta/ and for the IRA see http://terrorism.about.com/od/groupsleader1/p/IRA.htm accessed 18 April 2016

[509] *Ibid*

[510] G. Carter and D. L. Carter (2012) Law enforcement intelligence: implications for self-radicalized terrorism, Police Practice and Research, 13:2, 138-154, 139

[511] *Ibid*

risks are posed to the USA.[512] Although beyond the ambit of this thesis, to better understand the nature of the home-grown terror threat it is important to briefly note the radicalisation process brought about by terrorist communication. According to Gartenstein-Ross and Gossman *et al*, is believed to involve four stages:

1. Pre-radicalisation: an individual alters their lifestyle prior to radicalisation, such as relationships, employment and social life;
2. Self-identification: an individual is influenced by internal and external push/pull factors, attributing to the exploration of extremist philosophies, ideologies and values;
3. Indoctrination: an individual intensifies their beliefs and adopts extreme philosophies, ideologies and values with no exceptions;
4. Soldier: accepting their duty to participate in the struggle as a warrior fighting those who oppose the ideology in an attempt for the ideology to achieve realisation.[513]

State powers of surveillance can lead to those individuals within this process, at almost any stage, coming to the attention of the security services. However, this does depend on a number of factors. It is proposed the home-grown terrorist threat be broken down into two subdivisions to aid the thesis.[514]

The Self-Starting Terrorist

Firstly, there are the self-starting terrorists who are in contact with other like-minded extremists, seek inspiration and encouragement from them, but who have not been tasked by a stateless terrorist organisation to commit a violent act (such

---

[512] *Ibid,* 138

[513] D. Gartenstein-Ross and L. Grossman (2009) Homegrown terrorists in the U.S. and U.K. An empirical examination of the radicalisation process, Washington DC: Foundation for Defense of Democracies Press. See also M. D. Silber and A. Bhatt (2007) Radicalisation in the West: The homegrown threat, New York: Police Department, Intelligence Division. See also *Ibid*, 140

[514] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) p.80

as IS and al-Qaeda).[515] These types of start-ups are made much more effortlessly, and ensure a decent level of safety from electronic communications data surveillance capture for the would-be-terrorist, due to the amount of commercial encryption available on the open market, and the darknet. They are however, more likely to come to the attention of the policing and security agencies, somewhat due to their online presence, but more so because they may be socialising and meeting other persons whom are already known to the agencies, and may already be a 'Subject of Interest'.[516] Sir Malcolm Rifkind MP, former Chairman of the UK's Intelligence and Security Committee (ISC) highlighted this in the 2013 Committee report into the killing of Fusilier Lee Rigby.[517] This report highlights further how the UK's Security Service in particular works in practice, when identification of the would-be terrorist is essential. The issue surrounding finitely of resources faced by the UK agencies is also highlighted jointly in this report, which results in the UK Security Services need to prioritise their investigations, enabling the allocation of resources. They do this by ascribing a priority level determined on the available evidence at the given time:

- Priority 1 (P1a and P1b) is the highest, meaning there is intelligence to suggest attack planning;
- Priority 2 (P2H and P2M) is used when there is intelligence to suggest a high or medium risk such as terrorist training;
- Priority 3 (P3) is used when intelligence is uncorroborated;
- Priority 4 (P4) is assigned to those individuals where there is a risk of re-engagement with extremist activity.[518]

---

[515] *Ibid*

[516] *Ibid*

[517] *Ibid*

[518] *Ibid*, p13

The importance of this priority system cannot be overlooked, given that P3 and P4 cases are often paused or suspended in favour of concentrating on the higher levels. This is emphasised by Rifkind findings when questioning the Security Service as to the delay in identifying the terrorist Adebowale, which took the Digital Intelligence Team (DIGINT) five months.[519] The average for P3 cases is 69 days, but the Director General of the Security Service confirmed:

> If there was a P1 case that meant that we had significant urgency behind it, then we could do it much, much quicker. We have a finite amount of resource and we need to focus it on the highest priority work. No delay is desirable, but it is the reality of what we do that we carry delays in lower priority casework.[520]

It is accepted that P1 cases must take priority; after all they bear a more significant immediate risk, however, as evidenced the timescales surrounding the lower level cases must be improved. Particularly P4 cases given Carter and Carters research findings showing radicalisation is in essence resocialisation, coupled with the high levels of recidivism in the UK and the issue of radicalisation in prisons, though beyond the ambit of this thesis.

In addition to the priority of the overall investigation, Subjects of Interests are identified and placed into a tier system dependent upon their level of engagement.[521] As per the written evidence submitted to Rifkind's report, as of

---

[519] *Ibid*, pp.63-64

[520] *Ibid*, p.64 and p.88

[521] A Subjects of Interest is an individual who is being investigated because they are suspected of being a threat to national security.

October 2014 the Security Service were investigating several thousand individual Subjects of Interest with links to Islamist extremist activity in the UK:

- Tier 1: Main targets of an investigation, likely to be involved in all aspects of the investigated activities;
- Tier 2: Key contacts of the main targets, likely to be involved in a significant portion of the investigated activities;
- Tier 3: Contact with other Tier targets and likely to be only marginally involved with the investigated activities.[522]

This is where the importance of the intelligence-led policing framework and philosophy for preventing acts of terrorism come to fruition. The idea here is to allow for the collection and analysis of electronic communications data and other information related to terrorism, which results in actionable intelligence aiding law enforcement to develop tactical responses to the threats, or emerging threats.[523]

The Lone-Actor Terrorist

The second types of home-grown terrorist proposed are 'self-radicalising lone-actors', sometimes referred to as 'lone-wolves' or 'lone Islamist'. They have often been influenced and thereby radicalised at home via the Internet and terrorist communication, indirectly in some circumstances, and consequently inspired to commit an act of terror, doing so outside of any command type stateless structure, and without direct material assistance from any group.[524] The

---

[522] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) pp.13-14

[523] *Supra* as per D. L. Carter and J. G. Carter (2009) Intelligence led policing: Conceptual considerations for policy, *Criminal Justice Policy Review*, 20, 310-325, 317

[524] C. Bockstette (2010) Terrorists Exploit Information Technologies: Use of Strategic Communication Calls for United Response, in *Pre Concordiam, Journal of European Security and Defense Issues*, Terrorism, Volume 1, Issue 3, p.11

differences between the subdivisions become important when looking through the UK security agencies lens. Simply put, the lone-actor subdivision allows the individual to remain under the securities radar, entirely in some cases, whereby the person's identity poses a real challenge for the UK's law enforcement agencies'.[525] Examples of lone-actors are:

- Anders Behring Breivik on 22 July 2011, Norway, killed 77 people in two consecutive terrorist attacks. Firstly, he killed eight people with a car-bomb placed at the Norwegian government headquarters in Oslo. Then an hour later, he went to the summer camp of the Worker's Youth League (the youth organisation of the Labour Party) where he shot and killed 69 people;[526]
- In Nice on Bastille Day, Mohamed Lahouaiej Bouhlel drove an articulated lorry into a crowd or people killing at 84 people. Although the IS terror group claimed responsibility it has been insinuated he was in fact a lone-actor, with no known direct association to the group;[527]
- Omar Mateen in June 2016 entered a homosexual club in Orlando, Florida, and killed 50 people by shooting them. Shortly before the attack he pledged allegiance to IS;[528]
- Ahmad Khan Rahami in September 2016 carried out four bombings or bombing attempts in Seaside Park, New Jersey, Manhattan, New York, and Elizabeth, New Jersey. As law enforcement were apprehending him he shot and injured three police officers. According to the US policing agencies, Rahami was not part of any terrorist group or cell, but was simply motivated and inspired by the communications of al-Qaeda's Osama bin Laden and Anwar al-Awlaki;[529]

---

[525] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) p.5

[526] See http://www.telegraph.co.uk/news/2016/07/22/anders-breivik-inside-the-warped-mind-of-a-mass-killer/ accessed 30 December 2016

[527] B. Henderson and R. Sabur (2016) Nice terrorist attack on Bastille Day: everything we know so far on Monday, The Telegraph, 18 July, http://www.telegraph.co.uk/news/2016/07/15/nice-terror-attack-on-bastille-day-everything-we-know-so-far-on/ accessed 30 December 2016

[528] H. Tsukayama, M. Berman and J. Markon (2016) Terror in Orlando: 50 killed in shooting rampage at gay club, gunman pledged allegiance to ISIS, The Washington Post, 13 June 2016, available at https://www.washingtonpost.com/news/post-nation/wp/2016/06/12/orlando-nightclub-shooting-about-20-dead-in-domestic-terror-incident-at-gay-club/?hpid=hp_hp-top-table-high_orlando-banner%3Ahomepage%2Fstory&utm_term=.8adec967a5ff. See also http://www.reuters.com/article/us-florida-shooting-mateen-idUSKCN0YY0SY accessed 20 November 2016

[529] M. Santora, W. K. Rashbaum, A. Baker and A. Goldman (2016) Ahmad Khan Rahami Is Arrested in Manhattan and New Jersey Bombings, The New York Times, 19 September 2016, available at http://www.nytimes.com/2016/09/20/nyregion/nyc-nj-explosions-ahmad-khan-rahami.html?_r=0. See also M. Santora and A. Goldman (2016) Ahmad Khan Rahami Was Inspired by Bin Laden, Charges Say, The New York

- In 2016 Adel Kermiche and Abdel Malik Petitjean went into a Roman Catholic Church in Rouen, France, and killed the Priest. The two terrorists had only met in person a few days before the attack but had communicated through the encrypted messaging application 'Telegram'.[530]

It is clear from this list that it is not only Islamist terrorism that poses a risk to UK security. In the UK there has been an increase in far-right extremism, with new groups being created such as National Action, and Britain First.[531] Although such right-wing groups have not be defined by the UK as terrorist, the threat posed has been assessed more harmful and dangerous than that posed by lone-Islamist actors.[532] In 2016 Thomas Mair, who according to evidence presented had some connections to far right groups, killed Jo Cox MP utilising a knife and an illegally held firearm, and according to reports repeatedly shouted 'Britain First' during his attack. Despite claims to the contrary, it has been dealt with as a terrorist incident and Mair was sentenced accordingly.[533] As with Fusilier Lee Rigby's killing, the defendants were tried for murder contrary to UK Common Law, and terrorism was a sentencing factor in both trials. Also in Mair's trial a substantial quantity of

---

Times, 21 September 2016, available at http://www.nytimes.com/2016/09/21/nyregion/ahmad-khan-rahami-suspect.html accessed 20 November 2016

[530] See http://www.bbc.co.uk/news/world-europe-36892785. See also K. Willsher (2016) Powerful tributes at funeral of priest killed in Frnace terrorist attack, The Guardian, 2 August 2016, available at https://www.theguardian.com/world/2016/aug/02/thousands-expected-funeral-priest-killed-in-france-terror-attack accessed 21 November 2016

[531] https://www.rt.com/uk/347581-far-right-extremism-cox/. See also http://national-action.info accessed 21 November 2016

[532] M. Bentham (2016) Lone right wing extremists 'kill and harm more people than lone Islamist terrorists', Evening Standard, 21 June 2016, available at http://www.standard.co.uk/news/uk/lone-right-wing-extremists-kill-and-harm-more-people-than-islamist-terrorists-a3276876.html accessed 21 November 2016

[533] G. Greenwald (2016) Why is the Killer of British MP Jo cox not being called a 'Terrorist'? The Intercept, 17 June 2016, available at https://theintercept.com/2016/06/17/why-is-the-killer-of-british-mp-jo-cox-not-being-called-a-terrorist/ accessed 21 November 2016

evidence was produced showing his links to far right extremism.[534] As covered in Chapter One, the UK's definition of terrorism changes when a firearm is used, too:

> …the use or threat of action, involving firearms or explosives, made for the purpose of advancing a political, religious, racial or ideological cause.[535]

Clearly from Rifkind's report findings in 2014, both types of home-grown Islamist terrorists pose a significant challenge for the UK law enforcement agencies'. Another issue that must be considered is the fact that both self-starters and lone-actors show an increase in independent operational abilities, which simply compounds this issue further.[536] This sudden increase in independent operational abilities, along with the issue of resources finitely, has led Rob Wainwright head of Europol to assert that the EU currently faces the highest terror threat since the US attack by al-Qaeda in 2001.[537]

---

[534] See http://www.bbc.co.uk/news/uk-38076755 accessed 30 December 2016

[535] Terrorism Act 2000, s 1(3)

[536] V. Dodd, 'Europe faces highest terror threat since 9/11, MPs told', The Guardian, 13 January 2015, http://www.theguardian.com/uk-news/2015/jan/13/europe-highest-terror-threat-911-europol-fighting-overseas accessed 1 June 2015. For Paris terrorist attack see: http://www.bbc.co.uk/news/world-europe-30708237 accessed 30 April 2015. For Copenhagen terrorism attack see: http://www.theguardian.com/world/2015/feb/14/copenhagen-blasphemy-lars-vilks-prophet-muhammad-krudttonden-cafe accessed 1 June 2015. For Belgium terrorist attack please see: http://www.theguardian.com/world/2014/may/24/brussels-jewish-museum-attack-three-dead accessed 1 June 2015

[537] V. Dodd, 'Europe faces highest terror threat since 9/11, MPs told', The Guardian, 13 January 2015, http://www.theguardian.com/uk-news/2015/jan/13/europe-highest-terror-threat-911-europol-fighting-overseas accessed 1 June 2015

CONCLUSION

In the digital age most people do virtually everything online, including research, banking, shopping, finding new relationships, holiday planning and self-diagnosing health concerns. In conjunction with social media use, it has become almost impossible to separate people's lives in the real world, to their lives online. Likewise, people are increasingly becoming reliant on smartphones and other similar devices, storing private pictures and other personal data, such as calendars and reminders.

This means that bulk interception of communications data and bulk equipment interference are extraordinarily powerful tools to be wielded, having a much bigger impact upon individual privacy than traditional communications interception and surveillance might have had. Intercepting electronic communications data and content is not the same as intercepting a landline call as evidenced in this chapter. Additionally it is unhelpful and disappointing to note that the IPA does not expressly cover OSINT and SOCMINT collection, although the Government had plenty of time to implement such measures.

It has been argued that electronic communications data, by nature of its digital form, is ideal for analysis and profiling individuals. Data mining, or perhaps better-termed filtering arrangements as per section 62 of the IPA, will increasingly become autonomous as automated computer programmes carry out the first bulk interception step. Aimed at the population, who as a whole are not

suspected of being involved in any criminal or terrorist activity, these bulk powers have the potential to effectively destroy the privacy rights of millions of people, in order to find the elusive terrorist in the haystack. It has been substantiated that monitoring the whole population of the UK would be logistically impossible. However, in contrast it has been shown that due to the issues raised in Chapter 2, these powers are necessary. The balance between collective security and individual data privacy rights in the UK are fairly stable because of the role and importance of judicial review, judicial independence, and the over-arching scrutiny provided by commissioners and parliamentary committees.

CHAPTER THREE. PART TWO. THE UK'S LEGAL RESPONSE TO TERRORISM COMMUNICATION IN THE 21ST CENTURY: THE NECESSITY OF PRE-EMPTIVE LEGAL COUNTERTERRORISM MEASURES

INTRODUCTION

Adding more contention to the arguably unquantifiable threat posed is the sudden increase in independent operational abilities. These are gained through information attained on the Internet, or through the terrorist travelling to areas of conflict to receive the equivalent to military training.

Building upon the issues raised in Part One, Part Two will highlight further the requirement for mass data collection and pre-emptive legislative measures aimed at reducing the terrorist threat. The pre-emptive measures that will be focused on include temporary travel restrictions and the criminalisation of neutral behaviour, such as the collection of data deemed to be useful to a terrorist. Although the Chapter will highlight the interconnection between the risk society theory and predictive policing, it will remain within the legal research framework, discrediting terms used such as 'mass data surveillance' and 'pre-crime'. It will show that data retention is not the same as mass surveillance and that 'pre-crime' is a fabricated term used misleadingly, given that pre-emptive measures are in fact criminal offences.

The need for pre-emptive measures will be evidenced, highlighting that currently, counterterrorism legislation has failed to eradicate the terrorist groups' propaganda and infiltrate terrorist encrypted electronic communications data.

OPERATIONAL ABILITIES: ISLAMIST TERRORIST TRAINING

The sudden increase in independent operational abilities as alluded to in Part One of this Chapter, could be attributed to the amount of extremist material readily available through the Internet, or the individual could have travelled to another country to receive terrorist training, known within the UK's law enforcement services' as 'Jihadi tourism'.[538] Reports suggest approximately 5000 EU citizens' have been, and/or are currently engaged in terrorist related activities in conflict zones such as Somalia, Syria, Iraq, Libya and Yemen. Estimates suggest that one in 15 returning suspected of involvement in terrorist activities, potentially pose a threat to their respective national States upon return.[539] The methodology used to calculate these figures are unknown, mainly due to the difficulty in gathering such accurate data, and given they come from the UK security services and are deemed classified. It is argued therefore that these estimates could in actual fact be much higher, or indeed lower, rendering the terror threat unquantifiable. Adding to the issue finitely of resources, this serves to fashion an extraordinarily difficult if not

[538] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) p.6

[539] G. Buttarelli (2015) Counter-terrorism, De-Radicalisation and Foreign Fighters', Joint debate during the extraordinary meeting of the LIBE Committee. European Parliament, Brussels, 27 January 2015

impossible task of monitoring potential terrorists and suspects, thereby accurately managing the risk.

Islamist or Jihadi tourism purports its own danger, serving to not only increase independent operational abilities but also provide extensive hands-on military training in the use of firearms and explosives.[540] Although travelling to conflict zones increases the likelihood of the individual becoming known to the law enforcement agencies', the risk still remains somewhat unquantifiable. What is clear from Rifkind's 2014 report is that the independent operational abilities in conjunction with the methods used by lone actors and self-starting terrorists offer fewer opportunities for the security services to detect their activity.[541] Because of the changes in nature, 'the practices and policies necessary for prevention must change to reflect the threats'.[542] In recognising the type of threats, which according to the Director General of the Security Service, is mounting, 'diversifying and is increasingly complex', what can be seen is a sudden growth in risk management styles being employed by the police and security services when assessing intelligence.[543]

A point that must be made due to the successful marketing and promotion of IS, is that this has led to many foreign fighters traveling to Syria and Iraq. According to

[540] *Ibid*

[541] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) p.82

[542] J. G. Carter and D. L. Carter (2012) Law enforcement intelligence: implications for self-radicalized terrorism, Police Practice and Research, 13:2, 138-154, 138

[543] *Supra* as per The Rt. Hon. Sir Malcolm Rifkind MP (2014) pp.81-82

the National Counterterrorism Centre Director Nicholas Rasmussen, in October 2015 IS had 'attracted more than 28,000 foreign fighters, including at least 5000 westerners'.[544]

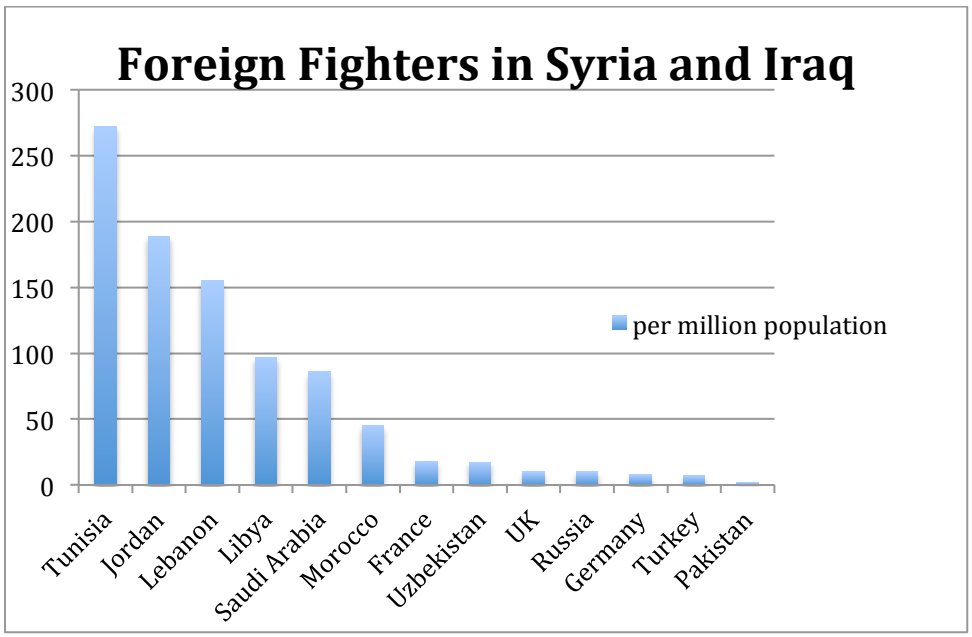

Table 2, Number of foreign fighters in Syria and Iraq, created from information attained at http://www.bbc.co.uk/news/world-middle-east-29052144 accessed 27 October 2016

Jihadi Tourism: Seizure of Passports and Travel Documents

In order to deal with and ultimately stop UK citizens' leaving the UK to engage in terrorist related activity, the Counter-Terrorism and Security Act 2015 (CTSA) introduced further pre-emptive measures. The CTSA also had to address and implement measures to halt the return of those citizens' returning to the UK after training and fighting with terrorist groups. The main pre-emptive power is found under Part 1 Chapter 1 of the CTSA, which allows law enforcement agencies' to seize passports and travel documents from persons suspected of involvement in

[544] See http://www.bbc.co.uk/news/world-middle-east-29052144 accessed 27 October 2016

terrorism. To this end Schedule One of the CTSA provides citizens' can have their passport retained for up to 14 days from the day after the initial seizure.[545] Although a short-term measure, this time allowance can be extend with judicial approval, to 30 days from the day after the initial seizure. Judicial approval is required whereby the Secretary of State must show that the relevant persons have been acting diligently and expeditiously in relation to the matters.[546] These provision were debated heavily during the enactment stages that led Lord Carlile to state:

> We heard some criticism of Clause 1, but I say… [Lordships] have got to get real about what Clause 1 is dealing with. Let me give you [a hypothetical] example…Suppose a suspicious travel agent who is public spirited telephones the police and says, 'I have just sold an air ticket in suspicious circumstances', and the authorities decide it is worth following the person who has bought the air ticket. That kind of incident can occur within an hour, and it does not leave the time to go off to a judge to get permission to seize that passport. We have to allow the authorities to deal with the urgent provisions made in Clause 1 and Schedule 1.[547]

Following this example and given that according to Rowley, the Metropolitan Police Assistant Commissioner, at the very least a total of 700 UK citizens' have travelled to Syria, with apparently more than half having returned to the UK, where they now pose a significant threat. The urgency and requirement for such emergency power can therefore be appreciated.[548] Whilst the time limitations are not too restrictive, there is still the issue of due process and the impact upon the

---

[545] Counter Terrorism and Security Act 2015, see paragraph 5(2) and (3)(a)

[546] Counter Terrorism and Security Act 2015 see paragraph 8(4), (5), (6) and (7)

[547] Lord Carlile of Berriew, Counter-Terrorism and Security Bill 2015, House of Lords Second Reading Stage, (13 January 2015: Column 722 7.27pm)

[548] P. Wintour (2015) *UK parents to get power to cancel children's passports over Isis fears*, The Guardian, 20 July 2015, available at https://www.theguardian.com/politics/2015/jul/20/uk-parents-power-cancel-childrens-passports-isis-fears accessed 24 July 2015

individual's privacy, and in particular their Article 45 right of the EU Charter, Freedom of movement and of residence.[549] Similar to that of the ECHR, any limitation on the exercise of the rights and freedoms under the Charter must be provided for by law.[550] Proportionality is the ultimate test of course and it must be deemed necessary in meeting recognised Union objectives, or to protect the rights and freedoms of others.[551] Ultimately these measures not only protect the public as a whole, but it also protects the vulnerable young adults and children from being further influenced and introduced to terrorist related activity should they be permitted to leave.

The provisions under Schedule One are wide in nature and define involvement in terrorism-related activity as:

> (a) the commission, preparation or instigation of acts of terrorism;
> (b) conduct that facilitates the commission, preparation or instigation of such acts, or is intended to do so;
> (c) conduct that gives encouragement to the commission, preparation or instigation of such acts, or is intended to do so;
> (d) conduct that gives support or assistance to individuals who are known or believed by the person concerned to be involved in conduct falling within paragraph; (a)

---

[549] Charter of Fundamental Rights of the European Union, see: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT accessed 1 June 2015. 'The free movement of persons is a fundamental right guaranteed by the EU to its citizens'. It entitles every EU citizen to travel, work and live in any EU country without special formalities. [Although the UK is not a member of Schengen]…Schengen cooperation enhances this freedom by enabling citizens' to cross-internal borders without being subjected to border checks. The border-free Schengen Area guarantees free movement to more than 400 million EU citizens', as well as to many non-EU nationals, businessmen, tourists or other persons legally present on the EU territory.' See http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm accessed 1 June 2015. And see also: 'Free movement of workers is a fundamental principle of the Treaty enshrined in Article 45 of the Treaty on the Functioning of the European Union and developed by EU secondary legislation and the Case law of the Court of Justice.' http://ec.europa.eu/social/main.jsp?catId=457 accessed 1 June 2015.

[550] Charter of Fundamental Rights of the European Union, Article 52(1)

[551] *Ibid*

> It is immaterial whether the acts of terrorism in question are specific acts of terrorism or acts of terrorism in general.'[552]

Should a constable or qualified officer have reasonable grounds to suspect a person is leaving the UK for the purposes of involvement in terrorism-related activity, or has arrived and is about to leave the UK to do so, then a number of powers are made available under Schedule 1, paragraph 2(5):

> (a) to require the person to hand over all travel documents in his or her possession to the constable or (as the case may be) the qualified officer;
> (b) to search for travel documents relating to the person and to take possession of any that the constable or officer finds;
> (c) to inspect any travel document relating to the person;
> (d) to retain any travel document relating to the person that is lawfully in the possession of the constable or officer.

In order to retain the travel documents for the specified length of times, authorisation from a senior officer must be attained.[553] The documents can then be retained whilst the Secretary of State considers the case.[554] They can also be retained whilst the authorities consider whether to charge the citizen with an offence, or subject them to further measures.[555] A person who fails to hand over all travel documentation, or obstructs the process, if found guilty of the offence may be liable to six months imprisonment.[556] The issue here of course is that the citizen may request a judicial review of the decision to retain his passport,

---

[552] Counter-Terrorism and Security Act 2015, Schedule 1, paragraph 1(10)

[553] Counter-Terrorism and Security Act 2015, Schedule 1, paragraph 4(1)(a)

[554] Counter-Terrorism and Security Act 2015, Schedule 1, paragraph 5(1)(a)

[555] Counter-Terrorism and Security Act 2015, Schedule 1, paragraph 5(1)(b)(c)

[556] Counter-Terrorism and Security Act 2015, Schedule 1, paragraph 15(1)(2)(3)

however, the intelligence and evidence gathered may be withheld from the suspect.[557] This makes it almost impossible for a citizen to in fact make a reviewable argument.

Temporary Exclusion Orders

The UK by way of Part 1 Chapter 2 of the CTSA fashions further intrusive pre-emptive measures aimed at preventing highly trained and militarily hardened terrorist from returning to the UK, who may then pose a direct or indirect risk to national security. Termed 'temporary exclusion orders' they state:

> (1) A temporary exclusion order is an order which requires an individual not to return to the United Kingdom unless-
> (a) the return is in accordance with a permit to return issued by the Secretary of State before the individual began the return; or
> (b) the return is the result of the individual's deportation to the UK.

Five conditions must be met before an order by the Secretary of State can be made and the order lasts up to two years.[558] Importantly, they require the Secretary of State to reasonably suspect that the individual is, or has been, involved in terrorism-related activity outside the UK, and reasonably considers that it is necessary, for purposes connected with protecting members of the public in the UK from a risk of terrorism, for a temporary exclusion order to be imposed on the individual.[559] Either the UK Court can grant the Secretary of State

---

[557] Counter-Terrorism and Security Act 2015, Schedule 1, paragraph 10(2), dealing with the extension period to 30 days.

[558] Counter-Terrorism and Security Act 2015, s 4(3)(b) limits the temporary exclusion orders to 2 years inclusive

[559] Counter-Terrorism and Security Act 2015, Chapter 2

permission to make an order under section 3, or the Secretary of State can show he considers the urgency of the case requires a temporary exclusion order to be imposed without obtaining permission.[560] The Act provides exceptionally wide powers to the executive, however, there is some protection afforded to the citizen by way of judicial supervision.

Firstly, the Secretary of State must include a statement outlining the urgency of the case and the requirement the order be imposed without obtaining the permission of the court.[561] Notice of the order must be provided to the court immediately after the temporary exclusion order is imposed, and the court must review the decision within 7 days of the order being made.[562] If the urgency of the order satisfies the court they must affirm the imposition, however, should the court determine the order is flawed they can quash it.[563] Judicial supervision, somewhat similar to that found in the IPA, is to be welcomed as a safeguarding development. Some other safeguarding clauses, such as the two-year limitation, was debated heavily during the enactment stages, leading Lord Carlile to state:

> I do not understand the two-year period contained in these amendments. The issue which we are dealing with and which is covered in this clause is, unfortunately, going to last for more than two years…having a two-year sunset clause…would send out a completely incorrect message to

[560] Counter-Terrorism and Security Act 2015, Chapter 2(7)(b)

[561] Counter-Terrorism and Security Act 2015, Schedule 2, paragraph 2

[562] Counter-Terrorism and Security Act 2015, Schedule 2, paragraph 3

[563] Counter-Terrorism and Security Act 2015, Schedule 2, paragraph 4

> those who are minded to go abroad and participate in jihad…We have to show some enduring determination over this issue.[564]

Although the ECHR rights and the EU Charter rights under Union law appear to have lacked discussion, the Marquess of Lothian raised a valid concern:

> …looking at the time factor here, what is the legal and international status of someone who has been subjected to a temporary exclusion order?[565]

International Status

This question has relevance given the legal and practical implications for the citizen subjected to this type of order. An important distinction must be made here, that the order is temporary, not indefinitely. In essence, this is not rendering that person stateless. There are two United Nations Conventions that the UK has long been a signatory, one of which serves to prevent a State from rendering a citizen stateless. The Convention relating to the Status of Stateless Persons 1954 and the 1961 Convention on the Reduction of Statelessness.[566] The 1961 Convention represents an international instrument safeguarding citizens' from inappropriate and unfair threats of statelessness. What is interesting however, is the Home Secretary, using Royal Prerogative power can already revoke UK citizenship entitlement, so long as the person concerned holds a dual nationality.[567] Taken in conjunction with the current terrorist threat, the

---

[564] Lord Carlile of Berriew, Counter-Terrorism and Security Bill 2015, House of Lords First Committee Stage, (20 January 2015: Column 1212)

[565] Marquess of Lothian, Counter-Terrorism and Security Bill 2015, House of Lords First Committee Stage, (20 January 2015: Column 1213)

[566] See http://www.unhcr.org/pages/4a2535c3d.html accessed 27 July 2015

[567]See http://www.findlaw.co.uk/law/government/constitutional_law/citizens_guide_to_government/500456.html accessed 21 July 2015

requirement for this genre of power to be on the statute book is clear. This is where the previous Prime Minister David Cameron's dexterity could be perused in his use of words, describing the actions of UK citizens' fighting for IS, as disloyal.[568] Articles 8 and 9 of the 1961 Convention expressly forbid the deprivation of nationality on racial, ethnic, religious or political grounds. Although the religious beliefs and political aspirations shown by members of IS are abhorrent, this would appear to satisfy the above definition.[569]

However, under the Convention, if a citizen has committed acts inconsistent with the duty of loyalty to the State, the State retains the right to deprive that citizen of nationality, even if this leads to statelessness. One could argue the actions of IS terrorists are certainly inconsistent with the UK. In addition, Article 19 of the EU Charter prohibits collective expulsion, or the expulsion of a person to a State where there is a risk of torture, the death penalty or other inhuman, degrading treatment. Although limited by law, it is argued this particular aspect of the UK's legislative measure will increasingly come under judicial scrutiny. The CJEU for example is not disinclined in striking down measures that are disproportionate in nature, particularly when such citizens' could be permitted to return to the UK and subjected to other forms of pre-terrorism sanctions, in accordance with other

[568] See http://www.ibtimes.com/uk-cannot-strip-returning-islamic-state-fighters-british-citizenship-cameron-clegg-1675618 accessed 21 July 2015

[569] See http://www.independent.co.uk/news/world/middle-east/who-are-isis-the-rise-of-the-islamic-state-in-iraq-and-the-levant-9541421.html accessed 23 July 2015

existing legislative measures.[570] Lord Macdonald of River Glaven appears to have at least recognised the impact of these measures and the potential for such friction between the executive and the courts:

> …we should not give away our freedoms in response to terrorism…[it] would be a good idea if [we] were to include a sunset clause…[because the] practicalities of this measure—how it will work in practice—…are most in doubt. Those practicalities will significantly impact on the rights of people on whom the orders are imposed…I support the idea of a sunset clause so that the House can thoroughly review how the legislation is working in practice.[571]

Mere suspicion that a citizen has engaged with terrorism-related activity is the required threshold. Considering the length of time the temporary exclusion order may be in place and the intrusive nature of these orders, the threshold should be raised and the executive be satisfied the citizen would pose a serious threat upon return. The decision made is reviewable and can be appealed by the citizen, however, the same rules with regards to disclosure exist as per the removal of passports and travel documents.[572] The potential repercussions for a citizen returning to the UK following the making of a temporary exclusion order, are severe should they be found guilty of an offence, sentenced for up to 5 years imprisonment.[573]

---

[570] Terrorism Prevention and Investigation Measures Act 2011, s 2, and the extension to these measures brought about by the Counter-Terrorism and Security Act 2015, s 16

[571] Lord Macdonald of River Glaven, Counter-Terrorism and Security Bill 2015, House of Lords First Committee Stage, (20 January 2015: Column 1214)

[572] Counter-Terrorism and Security Act 2015, Schedule 3, paragraph 4

[573] Counter-Terrorism and Security Act 2015, s 10

Clearly the UK Government is trying to reduce the terrorist risk posed, as is their duty to protect life and safeguard its citizens'. These powers are relatively new and therefore, data illustrating how they work in practice is short. In 2015 Germany took a similar approach to the UK in attempting to stop jihadi tourism.[574] According to the German Federal Ministry of the Interior, those traveling to join IS had increased dramatically in early 2015, which posed a direct threat to their nation state.[575] This new legislative Act followed an early Act in 2014 that provided authorities with the power to revoke or refuse an identity card for IS supporters, which included the proscription of the IS group and on all activity in support of IS in Germany.[576] In order to satisfy UN international norms, those persons who have been refused an identity card will instead be issues with a substitute identity document stating 'not valid for travel outside of Germany'.[577] Forming part of the risk management strategy inherent in the international and national response to the terrorist threat, some members of Germanys opposition party provided argumentation similar to that, as raised by UK MP's during the enactment stages of CTSA, in that the powers are unconstitutional as they criminalise neutral behaviour, because the moment of crime is far in advance of the actual crime.[578] In introducing such measures, the

---

574 See http://www.dw.com/en/german-cabinet-approves-bill-to-stop-radicals-traveling-to-middle-east/a-18233282 accessed 22 November 2016

575 See https://www.loc.gov/law/foreign-news/article/germany-new-anti-terrorism-legislation-entered-into-force/ accessed 22 November 2016

576 *Ibid*

577 *Ibid*

578 *Ibid*

state is simply trying to achieve good actionable intelligence, safeguarding citizens' lives.

CRIMINALISING NEUTRAL BEHAVIOUR: NEEDLES IN HAYSTACKS, RISK SOCIETY AND PRE-EMPTIVE MEASURES

Since the introduction of the various bulk powers and decryption under the IPA, it is highly likely that legislative pre-emptive measures introduced will increase in use. In attempting to manage the potential terrorist threats posed, the retention of electronic communications data for a period of 12 months and the bulk powers allowing such data to be screened by an algorithm, have proved essential in finding potential needles within the continually growing haystacks. As technology grows and the algorithms become more effective, the use of current pre-emptive measures will prove essential in the prevention of terrorist attacks. However, allowing such abilities to the state have resulted in academic debates surrounding mass surveillance, risk society, predictive policing and so called 'pre-crime' measures.

Mass Data Surveillance

According to Ratcliffe *et al*, in terms of CCTV camera use and its effects on crime reduction in the UK, citizens' are subjected to mass surveillance.[579] However, in terms of electronic communications data and ICR records that are retained for 12 months, and from the legal definition of surveillance under RIPA,

[579] J. Ratcliffe, T. Taniguchi and R. B. Taylor (2009) The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach, *Justice Quarterly*, 26:4

retention does not equate to mass surveillance. It would simply be impossible for UK law enforcement agencies' to actively conduct surveillance on the entire data pool. The algorithmic screening of the electronic communications data stored means that the majority of UK citizens' data would not come under the remit.[580]

Risk Society: The resulting increase in state powers

Collecting and storing vast amounts of data adds to the critical debate on the balancing of collective security with individual privacy, and essentially to the managing of risk. For Beck, the term 'risk' is a modern concept that:

> '…inherently contains the concept of control…presumes decision making [and involves] talking about calculating the incalculable'.[581]

According to Beck's conceptualisation in 2002, he suggests citizens' might increasingly become a paranoid 'risk society' as the international terror threat grows.[582] By linking prediction and risk, whereby fear of a potential terrorist attack leads to an increase in state law enforcements' capabilities, the result has arguably led to the development of computer algorithms to screen the vast amounts of data stored, in order to search out the needles in the haystacks autonomously and quickly.[583] According to Furedi's analysis, 'fear plays a key role in twenty-first century consciousness', which has inevitably led to citizens'

---

[580] I. Brown and D. Korff (2014) Foreign Surveillance: Law and Practice in a Global Digital Environment, *European Human Rights Law Review*, 3:243-251. See also A. S. Reid and N. Ryder (2010) For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000, *Information and Communications Technology Law*, 10:2, 179-201

[581] U. Beck (2002) The Terrorist Threat: World Risk Society Revisited, *Theory, Culture and Society*, 19:4, 39-55, 40

[582] *Ibid*

[583] *Ibid.* See also I. Kerr and J. Earle (2013) Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy, *Stanford Law Review Online*, available at https://www.stanfordlawreview.org/online/privacy-and-big-data-prediction-preemption-presumption/

acceptance of increased state monitoring and thereby, for Garland at least, control.[584] It is worth noting here that as citizens' increasingly accept state monitoring of stored data due to the risk society theory, conjoined with technological advancements, the automated computer algorithms used may become progressively effective at screening the vast amounts of data for potential terrorists. Leading of course to intelligence-led policing evolving into a type of predictive-led policing.

Predictive Policing and Pre-Emptive Measures: Pre-crime

Whilst the term predictive policing remains simply within the understanding of intelligence-led policing, it has nevertheless resulted in critics suggesting the UK is moving towards a 'pre-crime' scenario.[585] However, law enforcement cannot simply conduct surveillance or make an arrest without authorised legal powers, and a specific identifiable criminal offence being committed. As such, the term 'pre-crime' does not exist in legal terms. In fact it is simply a fabricated term used by Hollywood in the movie 'Minority Reports'. As discussed further below, collecting or disseminating terrorist related data through the Internet is a criminal offence.[586] The same can be said for encouraging another to commit an act of terrorism. These are not pre-crime measures, but pre-emptive criminal offences,

---

[584] F. Furedi (2007) The only thing we have to fear is the 'culture of fear' itself: How human thought and action are being stifled by a regime of uncertainty, available at http://frankfuredi.com/pdf/fearessay-20070404.pdf. See also D. Garland (2001) *The Culture of Control: Crime and social Order in Contemporary Society* (Oxford University Press)

[585] J. Richards (2016) *Needles in Haystacks: Law, Capability, Ethics, and Proportionality in Big Data Intelligence-Gathering*, in A. Bunnik, A. Cawley, M. Mulqueen and A. Zwitter, *Big Data Challenges* (Palgrave Macmillan) p74. See also L. Zedner (2007) Pre-crime and post-criminology? *Theoretical Criminology*, 11:2

[586] Terrorism Act 2000, ss 57, 58, and Terrorism Act 2006, ss 1, 2

aimed at preventing the would-be-terrorist from committing the physical act. They are a crime.

Following Beck's conceptualisation above, pre-emptive measures are littered throughout the UK's legal counterterrorism structure, simply because of the extraordinary terror threat.[587] As with the IPA, RIPA and the CTSA, there has been a growing tendency and common theme to address anticipatory risk.[588] For Walker, these measures have habitually been reactive to the politics of the last atrocity.[589] In response, the UK has enacted certain provisions aimed at criminalising the collection of terrorist material for terrorist purposes, and, at criminalising the encouragement and dissemination of terrorist publications. Again for Walker, the process of the radicalisation of young Muslim men became a primary focus following the terrorist attack on London on the 7th July 2005. In response to the gamut ferociousness and the devastating nature of recent terrorist acts, early State intervention is essential, before rather than after the attack.[590]

---

[587] *Supra* as per U. Beck (2002)

[588] C. Walker (2008) Terrorism: Terrorism Act 2000 s.57-direction to jury on defense of possession of items for defensive purposes, Case Comment, *Criminal Law Review* 72-80, 74

[589] *Ibid*

[590] For attack ion Turkey see http://edition.cnn.com/2016/03/13/world/ankara-park-blast/. For Ivory Coast attack see http://www.nytimes.com/2016/03/14/world/africa/gunmen-carry-out-fatal-attacks-at-resorts-in-ivory-coast.html?_r=0. For Northern Ireland terror attack see http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/, and http://www.bbc.co.uk/news/northern_ireland. For Paris attack 2016 see: http://www.bbc.co.uk/news/world-europe-34818994 accessed 15 March 2016

STATUTORY PREVENTATIVE MEASURES: POSSESSION OF ARTICLES AND COLLECTING MATERIALS AND INFORMATION FOR USE IN TERRORIST ACTIVITIES

Statutory preventative measures form part of this anticipatory risk management approach, although enacted prior to Walker's point made above, and not in direct response to a terrorist attack. Under section 57 of the Terrorism Act 2000 if a person possesses an article in circumstances that give a rise to a reasonable suspicion that such a possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism, they commit an offence. Similarly, under section 58 a person commits an offence if they collect or made a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or they possess a document or record containing information of that kind. This includes photographic and electronic communications data, both of which will increasingly become available to law enforcement by way of the IPA.

Although section 58 introduces measures requiring less proof of intent than section 57, both are designed to allow for the early prosecution of the would-be-terrorist, during the planning stage, rather than simply waiting for them to commit the physical act planned. Also known as anticipatory offences, these sections provide a correlative broad scope, meaning that more citizens' are potentially brought under the scope of terrorist activity, therefore providing law enforcement agencies' with an avenue to conduct surveillance, largely under the IPA and

RIPA. This has resulted in argumentation surrounding what exactly amounts to an article for the purposes of section 58.

In *R v K* the UK Court of Appeal made it clear that section 58 was not intended to criminalise possession of theological or propagandist material, and therefore must provide practical assistance.[591] The Court further made it clear that 'a document that simply encourages the commission of acts of terrorism' does not fall within the definition, thereby effectively curtailing the scope of section 58.[592] A year later in *R v G*, *R v J* the UK House of Lords appears to have built upon this judgement confirming that the defendant must be aware of the nature of the information contained in the article.[593] Ultimately, *J* then argued infringement of his ECHR Article 7 and 10 rights in the ECtHR, which failed.[594] According to Ackerman this judicial interpretation adds weight to the argument that the UK's counterterror legislation is overbroad and merely moderated by the judiciary, police and CPS restraint, possibly providing an excuse for executive excess.[595] Ackerman continues to argue the real threat to the public comes not from terrorism, but from counterterrorism measures such as these.[596] Gearty raises similar concerns, noting that the Convention rights are under 'sever attack from a

---

[591] [2008] EWCA Crim 185, [13]

[592] *Ibid*

[593] [2009] UKHL 13, [47]-[50]

[594] *Jobe v UK* [2011] 48278/09: ECHR Article 7 no punishment without law and Article 10 Freedom of Expression.

[595] B. Ackerman (2007) Before the Next Attack - Preserving Civil Liberties in an Age of Terrorism, *Public Law* 181-187

[596] *Ibid*

variety of sources'.[597] According to Imran, what is now clear is that many 'of the questions raised in *K* may be rendered superfluous by the intervention of alternative provisions that reduce the necessity for reliance on section 58'.[598]

Inciting Terrorism: Encouragement and glorification

A person commits an offence of incitement under section 59 of the Terrorism Act 2000, if they incite another to commit an act of terrorism, within or outside UK borders, if the act would constitute one of the following offences:

1) Murder (contrary to UK Common Law);
2) A s18 offence of wounding with intent under the Offences Against the Person Act 1861;
3) Administering poison to a person under s23 Offences Against the Person Act 1861;
4) Damage to property endangering life, as under s1 Criminal Damage Act 1971.

The issue here is that the offence of incitement is restricted to these four constitutions and evidentially it renders a high threshold, hence it can be quite difficult to prove. To fill the vacuum between incitement and encouragement, thereby serving to lower the threshold allowing UK law enforcement to broaden the net of suspicion, sections 1 and 2 of the Terrorism Act 2006 may serve to provide Imran's reduction, and provide ever more 'expansive possibilities for the prosecution and conviction'.[599] Enacted as a result of the terrorist attack on London, on 7th July 2005, and to reflecting the provisions of Article 5 of the 2005

---

[597] C. Gearty (2007) Rethinking civil liberties in a counter-terrorism world, European Human Rights Law Review (2), 111-119

[598] A. Imran (2011) Slaying the Monster: Sentencing, Criminal Law and Justice Weekly 175 JPN 151

[599] *Ibid*

Council of Europe Convention on the Prevention of Terrorism, section 1 makes it an offence to encourage an act of terrorism, and section 2 makes it an offence to disseminate terrorist publications. Section 1 in particular may have perhaps been enacted as a result of the earlier ruling in *R v K*.

ENCOURAGEMENT AND GLORIFICATION OF TERRORISM

The Terrorism Act 2006 was aimed at criminalising 'speeches at meetings, sermons at places of worship, chants and placards at demonstrations, broadcasts and material posted on the Internet', as discussed in Chapter Two.[600] A person will commit an offence of publishing a statement to directly encourage terrorism if:

> (a) he publishes a statement or causes another to publish such a statement; and
> (b) at the time he publishes it or causes it to be published, he
> (c) intends members of the public to be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare or instigate acts of terrorism or Convention offences; or
> (d) is reckless as to such and
> (e) the statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism or Convention offences.[601]

For Jones *et al*, the 'notion of direct encouragement causes little difficulty'.[602] The criminal act of publishing the material with intent is little different from the

---

[600] A. Jones QC, R. Bowers and H. D. Lodge (2006) *Blackstone's Guide to The Terrorism Act 2006*, (Oxford University Press) p.13

[601] Terrorism Act 2006, s 1(2)(b)(i)(ii)

[602] *Supra* as per A. Jones QC, R. Bowers and H. D. Lodge (2006) p.16

offence of incitement under the Terrorism Act 2000. The section 1 of the Terrorism Act 2006 offences can be committed with intent, or recklessly as to whether members of the public will be directly or indirectly encouraged or otherwise induced.[603] However, because this provides for indirect encouragement the breadth applicable of which is helpful to law enforcement agencies' in terms of scope.

Indirect Encouragement: Glorification

The glorification element posed one of the most contentious issues during the passage of the Terrorism Act 2006 through UK Parliament.[604] The main concern centred on how broadly the offence had been drawn and the possible implications on civil liberties and human rights, namely Article 10 ECHR the freedom of expression. The Third Report of the Joint Committee on Human Rights raised such concern in 2005. The Committee accepted on balance that a new law was required but considered:

> …that the offence of encouragement in clause 1 is not sufficiently legally certain to satisfy the requirement in Article 10 that interferences with freedom of expression be "prescribed by law" because of (i) the vagueness of the glorification requirement, (ii) the breadth of the definition of "terrorism" and (iii) the lack of any requirement of intent to incite terrorism or likelihood of such offences being caused as ingredients of the offence.[605]

---

603 Terrorism Act 2006, s 1(2)(b)(i) and (ii)

604 *Supra* as per A. Jones QC, R. Bowers and H. D. Lodge (2006) p.13

605 Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, House of Lords, House of Commons Joint Committee on Human Rights, Third Report of Session 2005–06, HL Paper 75-I HC 561-I, summary p.3

In order to render the new offence ECHR compatible, the Committee recommended the references to glorification be deleted, 'insert a more tightly drawn definition of terrorism' and ensure intent or at the very least a subjective recklessness test assessing the likelihood be inserted into the provision.[606] It was also recommended that a reasonable excuse or public interest defence be inserted to further satisfy ECHR standards.[607] However, the Government refused to implement the amendments suggested by the House of Lords and the then Labour Home Secretary Charles Clarke stated in Parliament that section 1 of the Terrorism Act 2006 intended to provide an exemplary description of what would constitute glorification.[608] As a result, under section 1 the statement made must glorify the commission or preparation, including past, future or in general terms, terrorist attacks, and is a statement that members of the public could reasonably be expected to infer that they should emulate the glorified conduct. Clarke however, made it clear that this description was not exhaustive.

Therefore a statement made that provides indirect encouragement is not limited to such glorification. Forming part of the UK's pre-emptive approach this section, coupled with section 5 creates a broader offence of preparation of terrorist acts, being closer to containing an offence of involvement, future intention, or even just espousal of the cause, rather than the commission of an established crime.[609] It

---

606 *Ibid*

607 *Ibid*

608 *Ibid*

609 *R v Rowe* [2008] Crim LR 72, see commentary

was argued this would appear to close off paths to enlightened discussion and debate utilising materials, as this could perceived as supporting acts of terrorism, rather than condemning it.[610] Given the gravity of the radicalisation problem outline above one can appreciate the political approach to the necessity of these powers. A similar approach is seen when looking at dissemination of terrorist materials.

Dissemination of terrorist publications

Following section 2 of the Terrorism Act 2006, a person engages in conduct falling within if he distributes or circulates a terrorist publication, including the sale or lending of a publication, or the offering for sale or loan, or provides a service to others that enable the obtainment of the publication, including the transmission of the publication electronically. The offence of dissemination is completed if he intends his conduct to directly or indirectly encourages, or provides assistance in, the commission, preparation or instigation of acts of terrorism, or is reckless as to such.[611] The Third Report of the Joint Committee on Human Rights raised the same concerns as those for the glorification of terrorism. They argued this provision 'suffers from some of the same compatibility problems as those identified in relation to the proposed encouragement offence'.[612] This included 'the lack of connection to incitement to

---

[610] Ibid

[611] Terrorism Act 2006 s 2(1)

[612] Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, House of Lords, House of Commons Joint Committee on Human Rights, Third Report of Session 2005–06, HL Paper 75-I HC 561-I, summary pp.3-4

violence and the absence of any requirement that such incitement be either intended, carried out with reckless indifference, or likely'.[613] Again the Committee suggested a reasonable excuse or public interest clause be inserted, primarily aimed at providing a defence and protection for legitimate activities of the media and academics.[614] The requirement for this power, on balance appears to be necessary given the amount of data disseminated through the Internet, within which section 3 of the Terrorism Act 2006 makes specific provision for the application of sections1 and 2 to Internet activity, thereby preventing terrorist material from making its way onto the Internet and attempting to halt terrorist communication. As highlighted, the enthused and encouraged would-be terrorist could potentially attempt to join terrorist groups currently fighting overseas.

These pre-emptive tools have proved to not be as effective as first hoped. In fact only three people have ever been successfully prosecuted under the Terrorist Act 2006. They could now be somewhat reinvigorated however, given the bulk powers under the IPA, and decryption methods. Taken as a whole, the legislation discussed to this point serves to provide severe human rights restrictions, specifically an individual's right to data privacy and to their freedom of expression, protected by both the ECHR and EU law.

---

613 *Ibid*

614 *Ibid*

CONCLUSION

In addition to the unquantifiable threat highlighted in Part One of this Chapter, Part Two has illustrated the frustrated scenario fashioned by sudden increases in independent operational abilities. This has resulted in the introduction of pre-emptive legislative measures and a risk management style of policing. To this end the Chapter has highlighted the interconnection between the risk society theory and predictive policing.

Such pre-emptive measures include temporary travel restrictions and the criminalisation of neutral behaviour. Taking a doctrinal approach, terms used such as mass data surveillance and pre-crime measures have been discredited. Indeed, it would be physically impossible for law enforcement to conduct surveillance on the whole of the UK populations' electronic communications data. It has further been shown that the term 'pre-crime' is simply a fabrication and misleadingly used, given that pre-emptive measures are in fact criminal offences.

The requirements for pre-emptive measures have been evidenced throughout both Parts of the Chapter, the second Part in particular, highlighting that currently counterterrorism legislation fails to eliminate the terrorist groups' propaganda and terrorist encrypted electronic communications data. Both of which play an integral part in increasing the security risks posed to the UK. It further fails to provide clarity in practical terms, given that the Terrorism Act 2006 appears to

have undercut ss57 and 58 of the Terrorism Act 2000, where it could be argued the latter merely provides 'a useful side-arm'.[615] Regardless, as with the balance between collective security and individual data privacy rights in the UK being fairly stable, that same can be said for the pre-emptive legislative measures examined. Again this is because of the role and importance of judicial review, judicial independence, and the over-arching scrutiny provided by commissioners and parliamentary committees. Since the passing of the IPA, an increase in the usage of these dedicated pre-emptive measures may increase, thereby serving to provide the state with positive outcomes.

[615] *Supra* as per A. Imran (2011)

CHAPTER FOUR. IMPLICATIONS OF THE UK'S LEGAL RESPONSE: STRIKING THE RIGHT BALANCE BETWEEN INDIVIDUAL PRIVACY AND COLLECTIVE SECURITY IN THE DIGITAL AGE

INTRODUCTION

This Chapter will assess if the bulk powers under the IPA can stand to legal challenges over breaches of data protection and privacy rights. The chapter starts by examining the EU's constitutional and legal influence on the UK legislature, specifically with regards to data protection and the rule of law. This is simply because the EU has led the UK's developments in terms of data protection and data privacy, and data retention of electronic communications data.

From the CJEU's ruling in *Digital Rights Ireland,* a new criterion will be developed from which to test new UK legislation, ensuring it remains within the limits set by EU law.[616] Applying this criterion specifically to the IPA, the chapter will illustrate that once tested by the CJEU, the initial bulk interception powers may be constrained. In addition, the new Judicial Commissioners role will be examined focusing on the available powers restricted to judicial review

[616] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* delivered on 8th April 2014 and reported at [2015] QB 127. Referred to as *Digital Rights Ireland*

rules. The overall aim of this chapter is to assess if the IPA strikes the right balance, between individual privacy and collective security in the digital age, and stand to CJEU and ECtHR judicial scrutiny.

UK DATA PROTECTION

The Data Protection Act 1998 (DPA) provides statutory control over how a citizen's personal information is used by organisations, private businesses and the Government.[617] Those responsible for using the data must abide by the data protection principles ensuring data is:

- used fairly and lawfully;
- use for limited and/or specific expressed purposes;
- accurate and used adequately;
- deleted when no longer required;
- kept secure;
- not transferred outside the European Economic Area without adequate protection.[618]

Should the data contain sensitive information, such as sexual health, criminal records, ethnicity and religious beliefs, then stronger protections must be in place.[619] When it was enacted, the impact of the DPA was felt right across the public and private sector. For the purposes of this Chapter, the seventh data protection principle relates to security, and it states that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing

[617] The Data Protection Act 1998, Introductory Text

[618] The Data Protection Act 1998, Schedule 1

[619] The Data Protection Act 1998, s2 and Schedule 3

of personal data and against accidental loss or destruction of, or damage to, personal data'.

This is particularly relevant to the issues raised in Chapter Two and three combined, where the use of Internet and e-mail raises issues when, private or public organisations, wish to monitor its use. Briefly, an organisation has a right and even a duty to monitor the use of the Internet and e-mails to prevent it being used for unlawful purposes or to distribute offensive material. However, running concurrent to this obligation is the fact an individual has a right to data privacy and protection. It is the duty of any organisation that provides access to e-mail and the Internet to balance these two conflicting principles. In specific policing terms section 29 DPA deals with crime and taxation exemptions that permit personal data to be processed and withheld from the individual concerned, for the purposes of the prevention or detection of crime. Such exemption must be proportionate, where the 'data controller' must record the data being processed. This means of course that a person may not be able to ascertain what information law enforcement has collected.

KEY HUMAN RIGHTS INSTRUMENTS: INFLUENCING THE UK'S APPROACH

The right to data privacy is enshrined in the EU at the constitutional level though Article 8 of the Charter of Fundamental Rights (CFR or Charter) and at the legislative level by way of two directives, namely the Data Protection Directive in

1995 and the e-Privacy Directive in 2002.[620] In the interests of fullness, the 2002 Directive repealed the earlier 1997 version aimed primarily towards the telecommunications sector, so it is no longer relevant.[621]

EU Constitutional Protection: The Treaty of Lisbon

As a result of the ratification of the Treaty of Lisbon 2007, which came into effect in 2009, the Charter of Fundamental Rights 2000 was given legal status. Therefore, constitutionally speaking, data privacy and protection is afforded by Article 8 of the Charter that states individuals have a right to the protection of personal data, where:

> Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.

The Charter also states compliance must be subject to control by an independent authority however, the right afforded here requires implementation into EU surveillance legislative instruments to make them effective. The EU's instruments have so far failed in this regard, inadequately providing sufficient oversight. Since the terrorist attack on the US on 11th September 2001, data protection appears to have been set aside almost as governments' focus on data

---

[620] European Union Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Also: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. See also *S and Marper v UK* [2008] 48 ECHR 1581, [66]-[67], the Court noted the concept of private life is a broad term not susceptible to exhaustive definition.

[621] European Union Directive 97/66/EC of the European Parliament and of the European Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

collection and mining.[622] Analysis illustrates that 'creating a stable and unequivocal system of data protection was not a priority'.[623]

EU Legislative Protection

The 1995 Directive was implemented in the UK by way of the Data Protection Act 1998, and the 2002 Directive was implemented by the Privacy and Electronic Communications (EC Directive) Regulations 2003. Following this in 2008, the EU adopted a Framework Decision aimed at providing similar legislative protection, but focused primarily on police and judicial co-operation when dealing in criminal matters.[624] The e-Privacy Directive in 2002 dealt with most aspects of protecting privacy in electronic communications, such as:

- Security: Article 4 requires the service provider to take appropriate technical security measures. Subscribers must be informed if there is a risk of a security breach;
- Confidentiality: Article 5 requires legislative assurance of confidentiality of communications made through public electronic communications services, or to such. Monitoring or storing communications is prohibited unless required for national security or crime prevention;
- Location data: Article 9 prohibits using location data unless it remains anonymous, or has the users consent. It can only be used to provide a value added service, such as local weather details. Article 10 however, permits the use of location data in life threatening circumstances, such as mobile contact with emergency services;
- Billing: Article 6 stipulates that billing data must be erased or made anonymous once the service providers' purposes for retention has expired (i.e.: the bill has been paid). Under Article 8, service users have a right to receive non-itemised billing;
- Automatic call forwarding: Article 11 provides service users the right to prevent automatic call forwarding by third parties;

---

[622] H. Hijmans and A. Scirocco (2009) Shortcomings in EU Data Protection in the Third and The Second Pillars, 46 *Common Market Law Review* 1485, 1496

[623] *Ibid*

[624] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

- Unsolicited marketing: Article 13 prohibits unsolicited communication unless consented to by the service user.[625]

For Hijman and Scirocco however, the protection afforded by way of these instruments lacked comprehensive cover for all data processing and thereby illustrate issues of practicality.[626] Balancing an individual's right to data privacy with the needs of national security has not been an easy task to complete, either within the UK or the EU. For example the DPA introduced safeguards applied to access to communications data. The problem is that law enforcement agencies' could only make use of electronic communications data for a limited period, and were thereby 'obliged to rely solely on data routinely retained by communications companies for their own purposes'.[627] This usually meant that the data was deleted following the payment of the last outstanding bill. In light of this, and the fact that no mandatory data retention regime existed, the EU introduced a number of Data Retention Directives. The first dealt with fixed networks and mobile telephony only, and was incorporated into UK law by way of the Data Retention (EC Directive) Regulations 2007 (S.I. 2007/2199). These were then superseded by the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859), 'which contained additional provisions relating to Internet access, Internet telephony and email'.[628]

---

[625] R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, summary

[626] H. Hijmans and A. Scirocco (2009) Shortcomings in EU Data Protection in the Third and The Second Pillars, 46 *Common Market Law Review* 1485, 1496

[627] R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [37]-[38]

[628] *Ibid*, [42]

The start of a new focus on data retention began when the EU's Council Action Plan on Combating Terrorism highlighted the emphasis to broaden security.[629] At this time, the EU focused on creating the next generation of Schengen, a visa information system and biometric passports, with a focus on information gathering, analysis and exchange.[630] In meeting this agenda, the EU's Action Plan paved the way for framework decisions aimed at simplifying information exchange between law enforcement agencies', Europol and Eurojust, and called for a Data Retention Directive.[631]

BULK RETENTION OF ELECTRONIC COMMUNICATIONS DATA: KEY HUMAN RIGHTS INSTRUMENTS

Mitsilegas follows this change in the use of EU level surveillance and notes five transformational trends, which are the linking of immigration with security and counterterrorism, increasing biometric data, a sharp shift towards prevention, broadening the access to data by law enforcement agencies' and taking a risk assessment approach.[632] These links and growth in the use of surveillance highlights a utilitarian logic where, 'information must be seen as a tool for collective benefits like fighting terrorism', ensuring, 'that information is available

[629] European Union Council, (2007) EU Action Plan on Combating Terrorism, Brussels, 9 March

[630] *Ibid*

[631] *Ibid*

[632] V. Mitsilegas (2010) The Transformation of Border Controls in an Era of Security: UK and EU Systems Converging? 24 *Journal of Immigration Asylum and Nationality Law* 233

when needed'.[633] This idea of the availability of data counters the EU's data protection principle, the aim of which is to limit the use of data to a specified purpose.

For Murphy, surveillance represents the broadest counterterrorism action taken by the EU.[634] In the 21st Century, national surveillance systems, such as the UK's IPA, subject to warrants and authorities can potentially affect a large section of the population and are not simply targeted towards immigrants, asylum seekers or suspected criminals. The EU's 2006 Data Retention Directive represents a classic example of targeting the whole population. For this reason, Murphy describes it as unpalatable.[635] The Directive:

> Aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.[636]

Prior to the terrorist attack in London on the 7 July 2005, the EU's earlier attempts to create such a measure failed due to heavy opposition from the European Parliament.[637] However, in the aftermath of this attack the UK

---

633 *Supra* as per H. Hijmans and A. Scirocco (2009), 1490

634 *Supra* as per C. C. Murphy (2015) p.147

635 *Ibid*

636 Article 1 of the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

637 Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose

effectively suppressed any opposition, arguing that mobile telephones were used in the coordination of the attacks, in addition to the earlier Madrid attack on 3 March 2004, and unsubstantiated claims were made confirming telecommunications information was vital to the investigation.[638] This Directive amended the earlier e-Privacy Directive and as such, following adoption of the Data Retention Directive on the basis of Article 95 EC (now Article 114 Treaty on the Functioning of the European Union (TFEU)), Ireland supported by Slovakia brought forward an application to have it annulled by the CJEU. In *Ireland v European Parliament and European Commission* the CJEU reached the decision that the amendment was within the legal scope under the now Article 114 TFEU.[639] In drawing a comparison to an earlier ruling concerning Passenger Name Record data, discussed in the next chapter, the Court confirmed the Directive merely aimed to harmonise the retention of data by private actors within the EU so that a distortion of competition within the internal market could be avoided.[640] Whilst the legality of the Directive is sufficient as it was adopted correctly, this further rationale represents a startlingly poor decision indeed. The reason behind the adoption in the first place was to provide lawful basis for the retention of data, both the traffic and location data of individuals, effectively

---

of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism 2004/0813/CNS

[638] Commission (EC) Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC COM (2005) 438 final, Brussels, 21 September 2005. See also: Euractiv.com, Data Retention: Parliament caves in to Council pressure, 14 December 2005, available at http://www.euractiv.com/section/digital/news/data-retention-parliament-caves-in-to-council-pressure/ accessed 11 July 2016

[639] [2009] ECR-I-593, [82]

[640] *Ireland v European Parliament and European Commission* [2009] ECR-I-593, [60]-[69]

permitting a total derogation from Article 7 and 8 CFR, which would require the deletion of such information once the billing purpose was satisfied.

The Breadth of the 2006 EU Directive

It is particularly concerning when one notes the sheer breadth of the 2006 Directive, which effectively includes a plethora of crimes for which the data may be utilised, to whom can access the data and the retention period. The 'excess of crimes' argument stems from the fact Member States cannot agree upon a definition of serious crime, and therefore Member States have implemented the directive in their own very personable way, contrary to EU law.[641] The same can be said for the different law enforcement agencies' permitted access to the data stored, with some Member States allowing not only security and policing agencies, but military services, tax and customs officials and border authorities.[642] Retention periods also fluctuate given the Directive allows for such divergence, permitting between six to 24 months.[643]

These facts prove inescapably the 2006 Directive derogated from the very purpose of EU directives. Even though the situation may have been improved given the previous total lack of uniformity, some divergence remains, illustrative

---

641 Council of the European Union, Document 9439/11, Brussels, 27 April 2011

642 Commission (EC) Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive 2006/24/EC COM (2011) 225 final, Brussels, 18 April 2011 at p.9

643 Article 6 Data Retention Directive, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

of the failure of the instruments claim to harmonise the internal market.[644] A rather peculiar clause within the Directive, although subject to EU Commission approval, allows the Member State to extend the retention period beyond the two years should particular circumstances exist.[645] It is startling to note that the Commission only review the Member States decision checking for compliance with the internal market, rather than data protection rights.[646] Coupled with the lack of clarity surrounding the necessity of this provision and the fact it has not been used deems it somewhat superfluous, and arguably unpalatable given the lack of focus on fundamental data protection.[647]

It terms of human rights infringements, the Directive directly reversed the requirements under the e-Privacy Directive 2002, which as per above required immediate deletion of traffic and location data once the billing process has been completed.[648] This was challenged through the judicial process where the CJEU dismissed the first claim that was based on the legality under what is now Article 114 TFEU, as discussed above.[649] However, in 2010 the Irish High Court granted

---

644 The Commission noted a wide range of retention periods existed prior to the Data Retention Directive, from 3 months to 4 years. Commission (EC) Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC COM (2005) 438 final, Brussels, 21 September 2005, p.1

645 Article 12 and Article 12(2) Data Retention Directive 2006/24/EC

646 M. Vilasau (2007) Traffic Data Retention v Data Protection: The New European Framework, *Computer and Telecommunications Law Review* 52, 58

647 Commission (EC) Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC COM (2005) 438 final, Brussels, 21 September 2005, p.13

648 Article 6 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

649 C-301/06 *Ireland v European Parliament and European Commission* [2009] ECR-I-593

a motion brought by a campaign group known as *Digital Rights Ireland*, where they specifically requested the CJEU look at the compliancy of the Directive with Article 5(4) Treaty on the European Union (TEU) and with certain fundamental rights protected under the CFR.[650] Additionally in 2012 a number of applicants brought an action in the Austrian Constitutional Court claiming the national law transposing the Directive infringed Article 8 CFR. The two claims were merged together by the CJEU where it was finally held that the Directive was invalid, overall, because the EU legislature had exceeded the limits imposed by Article 7, 8 and 52(1) of the CFR.[651]

They decided the Directive failed to provide sufficient safeguards against unlawful access to and the use of retained data, particularly by public authorities.[652] The CJEU, although noting the sheer breadth of the Directive and that in effect, no limits on the power to retain data existed, they failed to expressly lay down particular restraints or conditional requirements, should such retention be necessary.[653] Although it remains unclear, the Court did elucidate to what will be developed further below into the Digital Rights Criterion:

> 1. The protection of the fundamental right to respect for private life requires that derogations and limitations in relation to the protection of personal data *must apply only* in so far as is strictly necessary. Consequently the legislation in question must lay down *clear and*

---

650 *Ibid*

651 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others,* delivered on 8th April 2014 and reported at [2015] QB 127. Referred to as *Digital Rights Ireland*

652 *Digital Rights Ireland*, [57]-[59], [60]-[67]

653 *Digital Rights Ireland*, [58], [59]

precise rules governing the scope and application of the measure in question and imposing *minimum safeguards* sufficient to give effective protection against the risk of abuse and against any unlawful access to and use of that data;[654]

2. Any legislation establishing or permitting a general retention regime for personal data *must* expressly provide for access to and use of the data to be strictly *restricted* to the purpose of preventing and detecting *precisely defined* serious offences or of conducting criminal prosecutions relating to such offences;[655]

3. Above all, access by the competent national authority to the data retained *must* be made dependent on a *prior review by a court* or an independent administrative body whose decision seeks to *limit access* to the data and their use to what is *strictly necessary* for the purpose of attaining the objective pursued, and which intervenes following a reasoned request of those authorities.[656] [My emphasis]

Albeit the Court invalidated the Directive, a generalised rationale for the existence of such a data retaining measure was legitimised:

> '…the retention of data for the purpose of allowing the competent national authorities to have possible access to those data...genuinely satisfies an objective of general interest'.[657]

The impact of the CJEU's *Digital Rights Ireland* decision on the UK cannot be overstated, given if effectively neutered any national law giving effect to the Directive, which was transposed into UK national law by way of the Data Retention (EC Directive) Regulations 2009.[658] Immediately following the CJEU's landmark decision, the then Home Secretary Theresa May put before the

---

654 *Digital Rights Ireland*, [52], [54]

655 *Digital Rights Ireland*, [61]

656 *Digital Rights Ireland*, [62], this was also highlighted by Bean LJ in *R (on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [91]

657 *Digital Rights Ireland*, [44]

658 The Data Retention (EC Directive) Regulations SI 2009/859, adopted pursuant to the European Communities Act 1972 s 2(2). Regulations under the ECA 1972 depend upon the existence of a valid EU instrument. See also: A. Roberts (2015) Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications, *The Modern Law Review* 78(3) 522-548, 536

UK Parliament the Data Retention and Investigatory Powers Bill, specifying the UK must merely retain the powers under the invalid Directive, by fashioning such primary legislation.[659] This is made clear in the opening words of the statute, confirming:

> An Act to make provision, in consequence of a declaration made by the [CJEU] in relation to Directive 2006/24/EC, about the retention of certain communications data.[660]

To ensure *Digital Rights Ireland* had no bearing on the legislation, it did not purport to transpose any EU law.[661] It was introduced on the 14 July 2014 and rushed through UK Parliament as emergency legislation, receiving Royal Assent some four days later on 17 July 2014.[662] A sunset clause was applied to alleviate MP's fears surrounding rushed and under-debated, far reaching powers under the legislation, repealing it on 31 December 2016.[663]

As a result and following the enactment Ministers David Davis and Tom Watson brought a judicial review action to the UK High Court, arguing the provisions were incompatible with the EU law, namely the CFR and CJEU's decision in *Digital Rights Ireland*, and additionally the ECHR.[664] Lord Justice Bean

---

659 *Supra* as per D. Anderson QC (2015) p.16. See also V. Mitsilegas (2015) *The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law* (London: Springer, 2015) p.39

660 R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [44]-[46]

661 A. Roberts (2015) Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications, *The Modern Law Review* 78(3) 522-548, 537

662 *Supra* as per D. Anderson QC (2015) p.15

663 Data Retention and Investigatory Powers Act 2014, s 8(3)

664 R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092

discussed the *Digital Rights Ireland* cases, specifically referring to the CJEU's interpretation of Articles 7 and 8 of the CFR. Bean LJ replied in part on an earlier decision reached by Lord Kerr in the UK Supreme Court, in *Rugby Football Union v Consolidated Information Services Ltd*., confirming the CFR has direct effect in UK national law, when implementing EU law.[665] Given UK data protection law has been within the scope of EU law since 1995, Bean LJ really had no option but to illustrate the fact he was dealing with the implementation of EU law.[666]

Referring to the ruling in *Digital Rights Ireland* rendering the Directive invalid, Bean LJ went on to say:

> The invalidation of the Data Retention Directive by the CJEU put in doubt the legal basis for requiring the continued retention of communications data under the [UK's Data Retention (EC Directive)] 2009 Regulations. Although the 2009 Regulations remained in force, they had been made under s. 2(2) of the European Communities Act 1972 to implement the Data Retention Directive and were already subject to a legal challenge that had been stayed pending the outcome of the Digital Rights Ireland case. We were told that following the Digital Rights Ireland judgment, some CSPs [Crown Prosecution Service] expressed the view that there was *no legal basis* for them to continue to retain communications data, and indicated that they would start to delete data that had been retained under the 2009 Regulations.[667] [My emphasis]

Therefore, in the absence of a clear legal power to retain electronic communications data, the UK's law enforcement agencies' ability to use the Data Retention (EC Directive) Regulations 2009 was endangered. In disseminating the

---

[665] See *Rugby Football Union v Consolidated Information Services Ltd., (formerly Viagogo Ltd)* [2012] 1 WLR 3333, [27]-[28]

[666] *R (on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [6]-[8], [11]

[667] *R (on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [44]-[46]

CJEU's judgement in *Digital Rights Ireland*, Bean noted the Court's failure to stipulate possible conditions however, following the ratio it is clear that 'legislation establishing a general retention regime for electronic communications data infringes rights under Articles 7 and 8 of the CFR unless it is accompanied by an access regime which provides adequate safeguards for those rights'.[668]

The claimants' application for judicial review succeeded and the High Court declared that section 1 of the DRIPA was inconsistent with EU law in so far as:

> a) it does not lay down *clear and precise rules* providing for access to and use of communications data retained pursuant to a retention notice to be *strictly restricted* to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences; and
> b) access to the data is not made dependent on a *prior review* by a court or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued.[669] [My emphasis]

The High Court therefore made an order suspending section 1 of DRIPA postponed until 31 March 2016 to give Parliament time to consider their judgement and introduce measures consistent with EU law.[670] The High Court's decision is not surprising given that inherently, bulk collection of evidence has

---

[668] R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [89]

[669] R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [114]

[670] R *(on the application of David David MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v The Secretary of State for the Home Department* [2015] EWHC 2092, [121]

not been particularly welcomed or upheld, quite separately from constitutional EU law principles, within the jurisprudence of the ECtHR.[671]

European Court of Human Rights Jurisprudence

The ECHR and the ECtHR provides an additional layer of judicial accountability of UK statutes. Although the examples illustrated below do not cover electronic communications data, they do concern the state retaining data of persons neither charged nor convicted of a criminal offence. The jurisprudence of the ECtHR has illustrated that the state cannot simply retain the information for future use, or as a 'just in case measure'.[672] This has been evident for some time, and by way of example, under section 64(1A) Police and Criminal Evidence Act 1997 (PACE), the state was permitted to keep on file DNA and fingerprints evidence of those either not charged or convicted of the crime suspected for. This also included DNA from those who volunteered to give samples for elimination. Challenged by way of *R (S) v Chief Constable of South Yorkshire Police* in the House of Lords, it was held the Association of Police Officers (ACPO) policy allowing retention of DNA and fingerprints was lawful.[673] Later the case became known as *S and Marper v UK* where the ECtHR decided that a blanket and indiscriminate policy amounted to a breach of Article 8 ECHR.[674] This particular case highlights the clash between the UK judiciary and the jurisprudence of the ECtHR, where Lord

---

671 *R (GC) v Commissioner of the Metropolis* [2011] 1 WLR 1230

672 *Ibid*

673 [2004] UKHL 39

674 [2008] (Application Numbers 30562/04 and 30566/04), [67], and see also [2008] 48 EHRR 1169

Steyn in dismissing the appeal affirmed, whilst accepting the necessity that the Court interpret the ECHR in a harmonious way with the ECtHR's jurisprudence:

> The whole community, as well as the individuals whose sample was collected, benefits from there being as large a database as it is possible…The benefit to the aims of accurate and efficient law enforcement is thereby enhanced.[675]

The dichotomy is interesting here, given Lord Steyn favoured the interests of the wider community over the individual, and the ECtHR ultimately favoured the opposite, highlighting particular areas of concern:

> …have due regard to the specific context in which information at issue is recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.[676]

In light of the final ECtHR ruling, ACPO decided to do nothing, believing it should follow the earlier ruling in the House of Lords. This inevitably led to the database being further challenged in *R (GC) v Commissioner of the Metropolis* in the UK Supreme Court.[677] It held that the ECtHR's decision should be followed and therefore retaining the database was unjustified interference with Article 8 ECHR. Although the decision was welcomed, the Supreme Court did not make a declaration of incompatibility under the Human Rights Act 1998 with regards section 64(1A) PACE, stating Parliament had intended discretion be used as to what could be kept on the database. The Court did however, clarify that should Parliament not remedy the situation within a reasonable time then citizens' would have viable public law challenges. As a result Parliament introduced the

---

[675] [2004] UKHL 39, [78]

[676] [2008] (Application Numbers 30562/04 and 30566/04), [67]

[677] [2011] 1 WLR 1230

Protection of Freedoms Act 2012, where section 1 brought about the removal of DNA and fingerprints being stored on the database for those citizens' not convicted.

Considering the ECtHR's approach and particular emphasis in *S and Marper*, that in order for the powers to be in accordance with the rule of law, and ECHR compatible, there must be adequate legal protection against arbitrariness and sufficiently clarify the discretionary scope, given to authorities with a focus on the way the powers are exercised.[678] The Court findings are not that surprising given their earlier ruling in *Klass v Germany* where they emphasised proportionality and a focus on the individual's rights.[679] It is clear that blanket policies do not sit well within the ECHR framework, and where the ECtHR see the dignity of the individual prevailing over the interests of the wider community. Whilst the ECtHR disapproves of blanket policies the CJEU appears to be somewhat in favour, providing that minimum safeguards are put in place. It was evident from the *Digital Rights Ireland* Case that the collection of data was not the main issue, rather the safeguards surrounding the access to it.

More recently however, in *Zakharov v Russia* the ECtHR held that any authorisation for the use of surveillance powers must be capable of:

> '…verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for

[678] [2008] (Application Numbers 30562/04 and 30566/04), [95]

[679] [1978] (Application number 5029/71), [68]

> suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security'.[680]

Accordingly, the ECtHR here has made it quite clear that privacy, and the freedom of expression are important principles. Therefore, the ECtHR opinion would be that it is unjustifiable for a Government to collect the private communications data of potentially millions of people that it does not suspect in criminal involvement or terrorist related activity.[681] Ensuring restrictive laws provide for data protection and privacy may become increasingly important when the UK leave the EU, in terms of intelligence exchange, as explored in the next Chapter.

CREATING A NEW DATA RETENTION LAW: THE DIGITAL RIGHTS CRITERION

Returning to EU law, in order for UK legislation to fit with constitutional EU law and the jurisprudence of the CJEU, and the ECtHR, the following criteria is proposed ensuring compatibility:

1. Primary legislation must lay down clear and precise rules governing the scope and application of the measure;
2. Minimum safeguards must be imposed sufficiently reducing the risk of abuse or unlawful access to the data;
3. Access to the data must be expressly provided for, limiting the number of persons authorised to have such access and restricted to the purpose of preventing and detecting precisely defined serious criminal offences;

[680] 47143/06, 4 December 2015, [260]

[681] *Ibid*

4. Access to the data will only be granted after a prior assessment has been made by an independent administrative body or court, with the primary focus on human rights and proportionality of the measure;
5. Retained data will be deleted after 12 months unless an independent administrative body or court decides otherwise, having weighed the evidence and conducted a proportionality test

Focusing on EU law, it could be argued the IPA is purely domestic legislation and thereby not subject to the CFR, namely Article 8 right to data protection. DRIPA was arguably different, enacted to give effect to a EU instrument. One could generalise and state that the EU lacks competence in legislating within the field of fundamental rights and Member States must only respect the CFR when implementing EU law. However, legally it is much more complex as the CJEU expansively magnify the term 'implementing EU law' particularly when Member States seek to rely on a derogation from EU law principles.[682] The IPA in fact specifies under Schedule 10 Part 1, that the Privacy and Electronic Communications (EC Directive) Regulations 2003 do not apply in relation to any personal data breach which is to be notified to the Investigatory Powers Commissioner in accordance with a code of practice.[683] Considering UK data protection laws have been founded on EU law, particularly the e-Privacy Directive, it is argued the IPA is based upon EU derogation and it will undoubtedly be classed as implementing EU law by the CJEU. For this reason, the Act must respect the CFR and implement the digital rights criterion.

[682] Case C-390/12 *Pfleger* EU:C:2014:281, Case C-418/11 Texdata Software EU:C:2013:588 [71]-[75]

[683] S.I. 2003/2426

The Investigatory Powers Act 2016: Striking the right balance

It has been recognised the IPA needs to strike the right balance between individual privacy and collective security in the digital age. It has been said that holding privacy and security concerns to be irreconcilable is unhelpful and constraining given 'we all share an interest in maximising both our individual privacy on the one hand and collective security on the other.[684] Particularly since *Digital Rights Ireland*, it is vital any new intrusive surveillance powers that are passed are done so with due regard to the CFR.[685] Although the IPA was written to last, not just for the remaining time the UK is within the EU, the importance that UK counterterrorism legislation meets the CFR will still be important, in securing and maintaining intelligence exchange. Accordingly, the right to data protection includes data security and was described in *Digital Rights Ireland* as the essence of this right.[686]

BULK POWERS: DIGITAL RIGHTS CRITERION

In the previous Chapter it was shown that the bulk powers of interception, retention and equipment interference have been instrumental, and sometimes pivotal in preventing acts of terrorism and other serious crimes. The idea is to

---

[684] House of Commons Second Reading, 15 March 2016, Column 824, available at http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0001.htm#16031546000001

[685] A. Murray and B. Keenan (2015) Ensuring the Rule of Law, LSE Law Department Briefings on the Investigatory Powers Bill, LSE Law Policy Briefing Series, 12, *Social Science Research Network*, available at http://ssrn.com/abstract=2703806

[686] O. Lynskey (2015) Beyond privacy: the data protection implications of the IP Bill, LSE Law Department Briefings on the Investigatory Powers Bill, LSE Law Policy Briefings, 15, Social Science Research Network, available at http://ssrn.com/abstract=2704299

gather large volumes of data, which is then subject to stringent controls, used to filter out irrelevant material so the security services can simply focus on the small fraction that provides intelligence on known and potential threats.[687] The issue here is regardless of the filtering process many innocent citizens' electronic communications data would have been collected in the course of the action. King argues that whilst there 'needs to be formidable intrusive powers for law enforcement agencies' to operate' they must be targeted only and proportionate, rather than catchall bulk powers.[688] The bulk powers are extraordinarily broad in scope and the 'catchall' part to the bulk collection does not sound proportionate however, the practical effect of the breadth is limited by what can follow after the device has been accessed, or the telephone line tapped. It has been put forward that this stage makes the former proportionate.[689]

The question is of course does the IPA meet the *Digital Rights* criterion. The IPA clearly satisfies the first test insofar as it forms primary legislation that lays down clear and precise rules government the scope and application of the measures. The many accompanying code of conducts, although not law, may perhaps go some way in further satisfying this test. The access to the data is expressly provided for, with the bulk powers in particular stating that only intelligence and

---

[687] House of Lords Second Reading 27 June 2016, Volume 773, Column1362, available at https://hansard.parliament.uk/lords/2016-06-27/debates/1606278000466/InvestigatoryPowersBill

[688] First sitting Committee Debate Session 2015-16, Investigatory Powers Bill, Publications on the Internet, Column 14, 24 March 2016 available at http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160324/am/160324s01.htm accessed 30 August 2016

[689] *Ibid* at Column 6, 24 March 2016

security agencies can apply for the necessary warrants. This therefore limits the number of persons authorised to have such access and it is restricted to the purpose of preventing and detecting precisely defined serious crime.

In order to pass the digital rights criterion, measures must introduce minimum safeguards that sufficiently reduce the risk of abuse or unlawful access to the data, and that the access to the data will only be granted, after an independent administrative body or court has made a prior assessment, with the primary focus on human rights and proportionality of the measure. It is clear the UK Government has listened to the recommendations made, and perhaps learned from past mistakes, by taking a human rights approach highlighted by the opening Part to the IPA that imposes certain duties, and introduces general privacy protections and safeguards.[690]

The intrusive powers can only be used when it is necessary and proportionate to do so, and requires an independent judicial commissioner to review the Secretary of State decision before the warrant is valid.[691] IPA's new double lock system creates a number of new posts, including judicial commissioners and an Independent Investigatory Powers Commissioner.[692] This new position brings

---

[690] Investigatory Powers Bill 2015

[691] Investigatory Powers Bill 2015, s19 and s23; See also House of Commons Second Reading, 15 March 2016, Column 815, available at http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0001.htm#16031546000001

[692] *Ibid* at Column 813

together the responsibilities of the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner.[693] Additionally, the commissioners will be provided with inspectors, technical experts and independent legal advisers, and should an individual suffer as a result of an error the IPC will have the power to inform them.[694] These provisions certainly increase the difference between the IPA and all other surveillance legislation including RIPA.

Judicial commissioners, in deciding whether the warrant is necessary on relevant grounds and whether the conduct authorised is proportionate, must apply the same principles as would be applied by a court on an application for judicial review.[695] The meaning of judicial review was discussed during the First sitting Committee stage of the IPA and criticised by Sara Ogilvie from Liberty as being inherently limited in terms of jurisdiction.[696] In response Suella Fernandes confirmed that the double lock involves, 'an intensive analysis of necessity and proportionality'.[697]

---

[693] *Ibid* at Column 822

[694] Investigatory Powers Bill 2015, s19 and s23; See also *Ibid*

[695] Investigatory Powers Bill 2015, s23 (1)(2)

[696] First sitting Committee Debate Session 2015-16, Investigatory Powers Bill, Publications on the Internet, Column 17, 24 March 2016 available at http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160324/am/160324s01.htm accessed 30 August 2016

[697] *Ibid*

Checks and Balances: Judicial Commissioners and other mechanisms

In labouring the point Ogilvie argued that the level of judicial review would naturally be less intensive due to the 'national security' argument. Although Fernandes did offer some assurance in that the process, is not meant to be a 'rubber-stamping' exercise, it certainly appears that way considering section 229(6) confirms that judicial commissioners must not act in a way that is contrary to the public interest, or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK.[698] Adding further contention is the fact a judicial commissioner must not jeopardise the success of an intelligence or security operation, compromise the safety of those involved, or unduly impede the operational effectiveness of an intelligence service.[699] Although these particular sections are not to be applied when performing the 'double-lock' function, it does place a peculiar intent on the role, effectively requiring the commissioner to either agree or disagree with the Secretary of State.[700]

David Davis MP and Shami Chakrabarti both voiced similar concerns, referring to where the IPA specifies the judicial commissioners have to make their decisions based on judicial review principles, rather than based on the evidence.[701] Both Davis and Chakrabarti do have an agenda however, with the latter having been the

---

[698] *Ibid*

[699] Investigatory Powers Act 2016, s 229(7)

[700] Investigatory Powers Act 2016, s 229(8)

[701] See http://www.theguardian.com/politics/blog/live/2015/nov/04/surveillance-internet-snoopers-charter-may-plans-politics-live

director of Liberty for some years.[702] For Murray *et al*, it seems relatively clear from the IPA, that 'the judicial commissioner will be asked to review the Secretary of State's action in issuing a warrant on judicial review principles alone, this is whether the action was illegal, unfair (illegitimate), irrational or disproportionate'.[703] This is simply another layer of accountability on state action by the judiciary. Although the IPA does not appear to read this way, it could be further argued that the judicial commissioners position would be untenable, if the access to the data and evidenced put forward to the Secretary of State remain unavailable to them. Murray remains concerned that this lack of evidential transparency 'does not offer judicial independence required by the rule of law', and is not representative of an independent judiciary supposedly at the 'heart of the warrant process'.[704]

Notably, in terms of English public law, this new judicial position may challenge the doctrine of separation of powers, as the commissioners will be asked to, 'cross the waterline between secrecy and transparency', and effectively draws judges into 'the realm of executive decision-making, thereby threatening the impression of impartiality on which the legal system ultimately depends'.[705] Prior independent judicial authorisation however, is a new measure, so it is perhaps not

---

[702] See https://www.liberty-human-rights.org.uk accessed 30 December 2016

[703] A. Murray and B. Keenan (2015) Ensuring the Rule of Law, LSE Law Department Briefings on the Investigatory Powers Bill, LSE Law Policy Briefing Series, 12, *Social Science Research Network*, available at http://ssrn.com/abstract=2703806

[704] *Ibid*

[705] *Ibid*

possible to know with absolute certainty how it will work in practice. Inescapably and to balance this view, the result of judicial approval means that public bodies do not simply have unlimited power to 'intrude upon the privacy of citizens' without proper justification and authorisation'.[706]

Governmental Committees: Holding law enforcement to account

The ISC simply adds another additional layer to state and law enforcement agencies' accountability. It was first established by the ISA to, 'examine the policy, administration and expenditure of the Security Service, Secret Intelligence Service, and the Government Communications Headquarters'.[707] Since then the Justice and Security Act 2013 has increased the ISC's remit, including the oversight of operations, and has been granted greater powers.[708] The ISC can now look at other intelligence related work carried out by the Cabinet Office and Defence Intelligence for the Ministry of Defence, and the Office of Security and Counter Terrorism. The members of this Committee are appointed by Parliament, who then reports back to Parliament and to the Prime Minister, often dealing with sensitive information.

The ISC members, drawn from both the House of Commons and House of Lords, are able to hear classified material, meaning they can hold the intelligence agencies to account. On the 7th November 2013 the ISC held its first ever open evidence session with the heads of the Security Service, GCHQ and SIS. Although the

[706] House of Lords Second Reading 27 June 2016, Volume 773, Column 1363, available at https://hansard.parliament.uk/lords/2016-06-27/debates/1606278000466/InvestigatoryPowersBill

[707] See Intelligence and Security Committee of Parliament website, available at http://isc.independent.gov.uk

[708] *Ibid*

sessions are closed when assessing information that is deemed highly classified, the Committee intends to hold further public sessions in future.[709] In the ISC's latest 2015-2016 Annual Report, headed by the Chair the Rt. Hon. Dominic Grieve, the members confirmed they are of the view that the agencies' powers provided by the IPA are justified. In November 2015, a Joint Committee was appointed to commence pre-legislative scrutiny of the IPA. Given the role of the ISC in overseeing the intelligence agencies and its ability to take evidence on classified matters, the Committee provided the pre- legislative scrutiny focusing on 'those aspects of the draft Bill which relate primarily to the agencies' investigatory powers'.[710] In addition to the ISC report, the Joint Committee on the draft IPA made a total of 86 recommendations.[711] Whilst the former report focused on the overseeing arrangements surrounding the policing security agencies, due to its ability to take evidence on classified matters, the latter report focused on issues of clarity, judicial oversight and the justification for the various powers.

The Home Affairs Select Committee is another mechanism use to hold Government and law enforcement agencies' to account. This was seen on 6th December 2016, where David Armond the Deputy Director General of the NCA was questioned on

---

[709] *Ibid*

[710] Intelligence and Security Committee of Parliament, Annual Report 2015-2016, HC444, paragraph 5, available at http://isc.independent.gov.uk/committee-reports/annual-reports

[711] Joint Committee on the Draft Investigatory Powers Bill (2016) Report of Session 2015-2016, 11 February, HL Paper 93 and HC 651 available at http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm

EU policing and security issues.[712] This hearing led on from the earlier October 2016 focusing on UK policing after the UK's exit from the EU.[713]

In response to the issues raised by the various Committees, according to Prime Minster Theresa May, the IPA starts with a presumption of privacy, where privacy protections form the 'backbone' of the Act, and safeguards introduced further 'bolster' this in ensuring that high thresholds exist when sanctioning the most intrusive powers, and it limits the public authorities that can use the powers.[714] The questions of trust between the citizens' and the State are important ones.

PRIVACY AND TRUST: BALLANCING INDIVIDUAL PRIVACY AND COLLECTIVE SECURITY

The previous chapter has made it clear that powers of surveillance, particularly the proposed bulk powers, impinge upon individual privacy. Goold states:

> A public that is unable to understand why privacy is important-or which lacks the conceptual tools necessary to engage in meaningful debates about its value-is likely to be particularly susceptible to arguments that privacy should be curtailed.[715]

---

[712] See http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news-parliament-2015/161202-europol-ev/ accessed 9 December 2016

[713] See http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-subcommittee/news-parliament-2015/counterterrorism-lead-evidence-brexit/ accessed 9 December 2016

[714] House of Commons Second Reading, 15 March 2016, Column 814, available at http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0001.htm#16031546000001

[715] B. J. Goold (2009) Surveillance and the Political Value of Privacy, *Amsterdam Law Forum*

Whilst different perspectives and theories exist with regards the term 'privacy', this chapter has focused on the terms legal meaning. Privacy is important as it not only allows individualised expression and autonomy, but the concept can empower citizens' to challenge state decisions. In *R v Spencer* the Supreme Court of Canada described the protection of privacy as a prerequisite to individualised security, autonomy and self-fulfilment, which is essential in maintaining a thriving democratic society.[716] Privacy is not an absolute right as per the ECHR or the EU's CFR, but rather qualified and limited. On the one hand the State must protect the qualified rights insofar as possible, but on the other it must has a duty to protect the lives of it citizens' and keep them safe from criminality. In order to achieve this, the state must intrude on the privacy of individual citizens', usually of course as part of targeted intelligence-led policing, where proportionate, necessary and lawful to do so.

In terms of balancing individual privacy rights and maintaining collective security, debates turn on the level of individual privacy verses the level of State powers of surveillance. This focal point is unhelpful and dismisses less tangible aspects such as the individual's horizontal and vertical relationships, forming their perspectives on the social norm of privacy.[717] Sir Thomas Erskine May rather poetically captures the issue, stated in 1863:

---

[716] *R v Spencer* [2014] 2 SCR 212, [15]

[717] Britain is surveillance society (2006) The threat of sleepwalking into a surveillance society was thought to be a reality by the Information Commissioner, introducing his Report on the Surveillance Society, 2 November 2006, http://news.bbc.co.uk/1/hi/uk/6108496.stm accessed 9 May 2016

> Men may be without restraints upon their liberty: they may pass to and fro at pleasure but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators-who shall say that they are free? Nothing is more revolting to Englishmen than the espionage that forms part of the administrative system of continental despotisms. It haunts men like an evil genius, chills their gaiety, restrains their wit, casts a shadow over their friendships, and blights their domestic hearth. The freedom of this country may be measured by its immunity from this baleful agency.[718]

Modern attitudes towards surveillance are perhaps not as robust as during May's time, however, an element of mistrust exists.[719] It is also relevant that attitudes towards privacy depend heavily on the citizen's own perspective, informed by history, experience, environment, education and development.[720] Research has illustrated such positions are exceedingly contextual.[721]

Fears of the Surveillance Society: The Snowdon revelations

Anderson insinuates societal vertical relationships depend heavily on trust.[722] He leads the reader to what he calls is the 'Snowden effect', referring to the leaking of classified and sensitive US National Security Agency (NSA) documents by Edward Snowdon in 2013.[723] The documents emphasised the relationship between the NSA and the UK's GCHQ, whereby intelligence exchange ensued initiating widespread trepidation over the potential violations of human rights,

---

[718] T.E. May (1963) *Constitutional History of England since the Accession of King George III*, vol. 2, 1863, p.275

[719] *Supra* as per D. Anderson Q.C. (2015), pp.32-33

[720] *Ibid* at pp.32-33

[721] *Ibid* at p.33

[722] D. Anderson Q.C. (2015) p.34

[723] *Ibid*

arguably flouting legal protection for individual data privacy.[724] The documents highlighted the fact that a programme called 'PRISM' allowed US Federal agencies direct access to Internet servers, infiltrating Internet firms such as Microsoft, Apple, Facebook and Google.[725] Hopkins reports that between May 2012 and April 2013, 197 PRISM programme intelligence reports were passed to the UK's counterterrorism law enforcement agencies'.[726] The NSA, according to the leaked documents, was additionally recording millions of telephone conversations of US citizens' despite the fact they were not under any suspicion of unlawful behaviour.[727] Snowden having passed secret documents to a Glen Greenwald, a Guardian employee, Greenwald in the first of a series of following reports revealed that since April 2013 and under PRISM, confirmed that the NSA was collecting and retaining indiscriminately the telephone records of millions of US customers.[728] Although initially sanctioned to collect the communications records of foreign nationals, Greenwald confirms that it moved very quickly to concentrate on domestic communications.[729] As Greenwald continues with the series, he reported that the GCHQ had gained access to the intelligence, including

---

[724] D. Lowe (2014) Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty, *Terrorism and Political Violence*, 13 August 2014, 1

[725] *Ibid,* 4

[726] N. Hopkins (2013) UK Gathering Secret Intelligence via Covert NSA Operation, The Guardian, 7 June 2013, http://www.theguardian.com/technology/2013/jun/07/uk-gatheringsecret-intelligence-nsa-prism accessed 9 May 2016

[727] G. Greenwald (2013) NSA Collecting Phone Records of Millions of Verizon Customers Daily, The Guardian, 6 June 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order accessed 9 May 2016

[728] *Ibid*

[729] *Ibid*

sensitive personal information, which it then shared with the NSA.[730] Additionally it was also reported that the US Government had paid GCHQ over £100 million to secure access to the UK's intelligence gathering programmes.[731]

This is where the legal and cultural differences between the EU and US become quite prevalent, in that the Snowden revelations had the potential to damage diplomatic relationships, not only between the EU and US but the EU and the UK. This could have also affected international intelligence exchange between all parties as discussed further below. In light of this danger, UK and US politicians were somewhat forced to provide honest information, and defend the actions of the NSA and GCHQ. The then UK Foreign Secretary William Hague MP confirmed that both the UK and US had operated within the rule of law and used the intelligence obtained to protect citizens' freedoms.[732] Despite UK and US officials' assurances, the actions taken by the NSA and GCHQ reverberated even further when reports indicated that EU politicians were also spied on, in particular Angela Merkel the German Chancellor.[733]

---

[730] E. MacAskell, J. Borger, N. Davies and J. Ball (2013) GCHQ taps fibre-optic cables for secret access to world's communications', The Guardian, 21st June 2013 http://www.theguardian.com/uk/2013/jun/21/gchq-cablessecret-world-communications-nsa accessed 22 November 2016

[731] N. Hopkins and J. Borger (2013) Exclusive: NSA Pays £100m in Secret Funding for GCHQ, The Guardian, 1 August 2013, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden accessed 9 May 2016

[732] See http://www.bbc.co.uk/news/uk-politics-23053691 accessed 22 November 2016

[733] G. Greenwald (2014) *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, (Metropolitan Books: New York) p.141

In terms of the public trust, despite assurances the UK public's reaction has evidenced a suspicious attitude.[734] In light of Snowden, an Austrian citizen and privacy advocate, Maximillian Schrems took action against the Data Protection Commissioner.[735] His argument turned on the fact that Facebook Ireland has transferred his personal data to the US, and that the US did not ensure sufficient protection of his personal data.[736] Referring to NSA's practices as reported by Greenwald and leaked by Snowden, he claimed the NSA and other US agencies could have retained his personal data.[737] The US's Foreign Intelligence Services Act 1978 permits the NSA access to personal data held on US servers. Therefore, because Facebook Ireland is a subsidiary of Facebook US, *Schrems'* details had in fact been transferred. The CJEU noted that the US Foreign Intelligence Surveillance Court did not offer a judicial remedy to EU citizens' and declared the 2000/520/EC Decision invalid, bringing an end to the Safe Harbour Agreement.

Article 25 of the 1995 Data Protection Directive (discussed in Chapter Five) was critical to the CJEU, particularly concerning the Commissions responsibility to ensure adequate personal protection of transferred data.[738] The CJEU confirmed that the level of protection provided need not be identical to the EU's, but must

---

[734] A. Travis (2015) Snowden leak: governments' hostile reaction fuelled public distrust of spies, The Guardian, 15 June 2015, available at https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies accessed 22 November 2016

[735] *Maximillian Schrems v Data Protection Commissioner* [2015] C-362/14

[736] *Ibid*

[737] *Ibid*

[738] Data Protection Directive 1995, 95/46/EC, Article 25

evidence adequacy at the very least, ensuring they have a high level of fundamental rights protection in place, equivalent to which is afforded by Article 25.[739] The leaking of this information and GCHQ's actions regarding the allegation of conducting mass surveillance, led to the German Justice Minister, Sabine Leutheusser-Schnarrenberger's request from UK ministers', for reassurance that actions taken were legal and if they affected German citizens', stating further:

> In our modern world, the new media provide the framework for a free exchange of opinions and information. Transparent governance is one of the most important prerequisites that a democratic state and the rule of law requires.[740]

The legal director of Liberty also accused GCHQ of violating citizens' Article 8 rights to privacy, commenting on the then proposed IPA:

> Those demanding the [Investigatory Powers Act, also termed as the] Snoopers' Charter seem to have been indulging in out-of-control snooping even without it - exploiting legal loopholes and help from Uncle Sam [USA]. No one suggests a completely unpoliced Internet but those in power cannot swap targeted investigations for endless monitoring of the entire globe.[741]

In light of such reports and adversarial commentary, the EU's Justice and Home Affairs Council (JHAC) showed concern for the level of protection of EU citizens' constitutional right to privacy, which resulted in Viviane Reding the EU Justice Commissioner stating:

---

[739] *Maximillian Schrems v Data Protection Commissioner* [2015] C-362/14, [73], [141], [142], [147]

[740] Germany Seeks UK Surveillance Assurances, BBC News, 25 June 2013, http://www.bbc.co.uk/news/uk-23048259 accessed 9 May 2016

[741] *Ibid*

> The European Commission is concerned about the possible consequences on EU citizens' privacy. The Commission has raised this systematically in its dialogue with the U.S. authorities, especially in the context of the negotiations of the EU-U.S. data protection agreement in the field of police and judicial co-operation…[742]

It is interestingly to note the dichotomy between the civilian and the State when discussing powers of surveillance and personal data privacy. Representing somewhat of a paradox, citizens' seem less concerned with sharing information freely in a horizontal fashion, by means of social media for example where people seem quite happy for others to know everything about them, but become quite aggrieved when information is viewed vertically, by the State.[743] To this regard the previous chapters have shown the importance of personal privacy, being paramount in the minds of citizens' with a generalised fear of a Big Brother State, given weight by the law enforcements agencies use of OSINT and SOCMINT data. Many fear the UK is moving towards a surveillance society, given that what follows a terrorist act or perceived threat usually takes the form of new legislation introducing more restrictive measures. The fluid relationship between terror threats and new legislative prowess has been emphasised throughout this thesis, in addition to proposed new legislation dealing with extremism.

---

[742] N. Watt (2013) PRISM Scandal: European Commission to Seek Privacy Guarantees from U.S., The Guardian, 10 June 2013, http://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees accessed 9 May 2016

[743] K. D. Ewing (2010) *Bonfire of the Liberties: New Labour, Human Rights, and the Rule of Law* (Oxford University Press) p.54

CONCLUSION

Part One of the IPA could be equated to simply paying 'lip service', because for some, overall, the introduction of bulk powers under the IPA fails to extend human rights protections, specifically related to the right to privacy, protection of personal data and freedom of expression. Whilst these bulk powers may pass the digital rights criterion and could be described as necessary in finding would-be-terrorists, it may ultimately come to fail the CJEU and ECtHR jurisprudence when testing the proportionality of the measures.

In terms of checks and balances, the IPA does introduce a double lock system whereby a judicial commissioner must agree with the Secretary of State, in line with judicial review influences, that the powers permitted under the warrant are necessary and proportionate. The ISC and the Home Affairs Committee, both independent Governmental scrutiny mechanisms, with the former able to see classified information relating to intelligence operations, provide another form of checks and balances. Additional safeguards are currently provided by the office of the Interception Commissioner, currently the Rt. Hon. Sir Stanley Burnton, who oversees the security agencies arrangements for access to the data.[744] The new double lock system under the IPA however, creates a number of new posts

[744] See https://www.mi5.gov.uk/interception-of-communications accessed 29 April 2016, and http://www.iocco-uk.info accessed 29 April 2016

including judicial commissioners and an Independent Investigatory Powers Commissioner.[745]

It has been stipulated in the IPA that judicial commissioners must apply judicial review principles. Whilst this is not particularly concerning, given the commissioners will undoubtedly view the evidence used by the Home Secretary in approving the authority, it is a new element and until it is seen working in practice it would be difficult to make any firm statements. It will also be interesting to see if the bulk powers under the IPA will survive in their current form given legal challenges will undoubtedly come from human rights organisations such as Liberty. Even if the UK has left the EU prior to any future CJEU ruling on the subject, it must still keep within current criterions to ensure international intelligence exchange with the EU continues.

The EU has led data protection and data privacy initiatives, legally and constitutionally. However, looking forward it may be the case that the ECtHR takes the lead, given the EU's focus on data retention. Should the UK's bulk powers under the IPA be challenged in the ECtHR, who historically do not approve of blanket policies, or the keeping of data of innocent civilians, it may not survive. This would be detrimental however, and it is argued the CJEU and ECtHR should accept that terrorism in the digital age means the Internet must be monitored, allowing for bulk analysis of electronic communications data.

[745] *Ibid* at Column 813

The Chapter found however that the balance between collective security and individual data privacy rights in the UK are fairly stable because of the role of judicial review; judicial independence, and the over-arching scrutiny provided by commissioners and parliamentary committees. It is further argued that a blanket approach to retaining electronic communications data is necessary in finding the terrorist in the ever growing haystacks', because sometimes privacy rights and data protection must be curtailed to ensure the state can protect citizens' rights to life.

CHAPTER FIVE. THE INTERNATIONAL NATURE OF THE 21ST CENTURY TERROR THREAT: PRESERVING INTERNATIONAL INTELLIGENCE EXCHANGE AND THE IMPLICATIONS OF THE UK LEAVING THE EUROPEAN UNION

INTRODUCTION

The chapter will explore the relationship between the EU and the UK following the UK's exit. International intelligence exchange is an essential element to national security illustrating an international terror threat requires an international response. Particularly since al-Qaeda's terrorist attack on the US on 11th September 2001, the EU and the US have sought to co-operate through sharing internal security data. Of course the UK being a part of the EU has been party to this agreement.

The EU's legislative landscape has been shown in the previous chapter to be cluttered with many measures aimed at data surveillance and counterterrorism action. In addition to collecting, storing and exchanging a greater volume of intelligence data within the EU, by means of using both targeted and bulk powers, there has been an increased emphasis on transnational data exchange.[746] It will be highlighted that these international trends have also been contrary to the EU's rule of law. Focusing on current intelligence exchange arrangements between the EU

[746] *Supra* as per C. C. Murphy (2015) p.149

and UK, particularly with regards Passenger Name Records (PNR) data exchange; this chapter will assess what the new relationship will look like post the UK's exit from the EU, using the US as a case study.

This should show that differing cultures surrounding privacy rights between the EU and the USA have created their own set of problems.[747] The protection of privacy, particularly data privacy is protected under EU law, but less clear in the US.[748] Based on eight key principles, the EU focuses on the dignity on the individual citizen, whereas the US focuses on the liberty.[749] Not forgetting that the protection of privacy forms the safeguarding role of the rule of law within the EU, thereby requiring compliance with EU constitutional and legislative standards, the position is exasperated by the US lacking any formally expressed data protection law.[750]

THE UK AND EU: THE EXIT

As at December 2016, it has been reported that the UK's current Government appear to be playing with their cards close to their chest when it came to releasing

[747] S. Sottiaux (2008) *Terrorism and the Limitation of Rights: The ECHR and the US Constitution* (Oxford: Hart Publishing 2008) pp.265-322

[748] *Ibid* pp.266-268

[749] J. Q. Whitman (2004) The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal 1151-1221, 1219

[750] *Supra* as per H. Hijmans and A. Scirocco (2009) Shortcomings in EU Data Protection in the Third and The Second Pillars. 46 *Common Market Law Review* 1485, 1487-1489

the details of the exit plan.[751] The position remains extremely unclear and it will therefore not be possible to make any firm statements. What is clear however is that the UK will certainly be leaving the EU, and Prime Minister Theresa May might be working towards remaining within the single market, and Foreign Secretary Boris Johnson has affirmed his position that the UK would remain part of a 'dedicated European power'.[752]

Although the Supreme Court is currently deliberating on one of the most important UK constitutional decisions since Lord Justice Law's decision in *Thoburn v Sunderland City Council*, following a vote in UK Parliament on 7th December 2016 it would suggest that Article 50 of the Treaty of Lisbon 2007 would be triggered in March 2017.[753]

EU Counterterrorism: Security and intelligence

In terms of counterterrorism laws, for Kaunert counterterrorism has been a driver in the EU's Area of Freedom, Security and Justice (AFSJ) construction.[754] Prior

[751] J. Elgot (2016) Brexit debate in parliament would give game away to Brussels, says minister, The Guardian, 16 October 2016, available at https://www.theguardian.com/politics/2016/oct/16/brexit-debate-iwould-give-game-away-to-brussels-priti-patel accessed 9 December 2016

[752] M. Dathan (2016) No room for Bojo among EU's foreign ministers! Top diplomats tease Boris and block him from joining photo –shoot as they begin process of excluding Britain from Brussels club, The Mail Online, 2 September 2016, available at http://www.dailymail.co.uk/news/article-3770744/Britain-continue-helping-EU-tackle-migrant-crisis-Brexit-Boris-Johnson-pledges-tours-European-capitals.html accessed 24 November 2016

[753] [2002] EWHC 195 (Admin). See also P. Dominiczak, G. Rayner, S. Swinford, K. McCann, M. Wilkinson and B. Henderson (2016) Theresa May secures Article 50 victory in the Commons as Parliament passes amended Brexit motion by 448 to 75 - latest reaction and analysis, The Telegraph, 7 December 2016, available at http://www.telegraph.co.uk/news/2016/12/07/brexit-article-50-mps-vote-supreme-court-pmqs-live/ accessed 9 December 2016

[754] J. Argomaniz, O. Bures and C. Kaunert (2015) A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment, Intelligence and National Security, 30:2-3, 191-206, 192

to the attack on the US in 2001, the EU did not have a definition of terrorism. Since that point however, the EU has become increasingly active on the world stage focused on creating and maintaining internal and external intelligence exchange structures.[755] The EU has also sort to harmonise Member States national legislation, as well as coordinating policies and offering support for operational work.[756] Through this medium, Member States have been encouraged to adopt the same conceptual precautionary and organisational measures and structures.[757] According to Boer and Wiegand, this relationship has resulted in a move from convergence to a deeply integrated legal counterterrorism arrangement.[758] This has allowed the EU, in terms of supranational governance, to approach counterterrorism initiatives through a convergence between national counterterrorism systems, rather than a top down method.[759] Harmonisation ensuring constitutional, institutional and cultural similarities allows for greater ease of communications and information exchange.[760]

Whilst this idea and approach has perhaps been useful for law enforcement agencies' in practical terms, particularly when accessing shared intelligence, research conducted by Wiegand suggests that significant differences remain

---

[755] See http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/ accessed 9 December 2016

[756] *Supra* as per J. Argomaniz, O. Bures and C. Kaunert (2015), 196. See also M. L. Wade (2014) The European Union as a counter-terrorism actor: right path, wrong direction? *Crime Law Soc Change*, 62:355-383

[757] M. D. Boer, and I. Wiegand (2015) From Convergence to Deep Integration: Evaluating the Impact of EU Counter-Terrorism Strategies on Domestic Arenas, *Intelligence and National Security*, 30:2-3, 377-401, 377

[758] *Ibid* at 387

[759] *Ibid* at 378

[760] *Ibid*

between the national counterterrorism approaches of the Member States, despite the best intentions of the EU.[761] The EU has focused on four difference areas of convergence have been highlights, political-strategic, organisational, procedural and legal. Within the legal spectrum the EU has pushed to integrate objectives by developing internationalised regulatory mechanisms and dividing the focal points into four subdivisions namely preparation and response, prevention, protection, and prosecution.[762] Following the 175 measures adopted by the EU in the immediate aftermath of the attack on the USA in 2001, Wiegand's study shows Member States were slow in implementing them resulting in a 'slow, slack and uneven' scenario.[763]

The UK's Exit Position

Regardless this level of integration means that because the UK's counterterrorism structure has been formed, largely by the membership with the EU, the effects of leaving on international intelligence exchange should be minimal. Given the UK will still be a member of the EU on 25th May 2018, the latest EU PNR Directive will be required to be implemented. However, when the UK leaves the EU, it may become necessary to renegotiate this agreement given the UK will essentially be classed as a third country. For Jenni, there is no current model or framework the UK could look towards to give an indication of what a post UK exit would

761 *Ibid* at 379

762 *Ibid* at 381 and 383

763 *Ibid*

look like.[764] The point being no Member State has ever left the EU before. The Swiss model for example is not a solution but may provide some slight suggestions.[765] It is important to note that post the UK's exit, the UK will still be exchanging intelligence with EU Member States, and here is a good example of the points raised below concerning *Schrems*.

The Swiss Lessons

Jenni argues there may be four lessons from the Swiss model applicable to the UK. The first is that it may take many years to negotiate agreements, which may be determined on an *ad hoc* basis.[766] The Swiss model has further shown that the UK will not be able to draw up an agreement dealing with one area of concern, rather that the EU deal in package type agreements including trade-offs.[767] The second lesson is that leaving the EU will not end the EU's influence on the UK's law making powers. Particularly in terms of maintaining international security and mutual recognition, the EU would effectively curtail the UK's decision making powers, albeit perhaps not directly. This process would also be important in terms of the UK remaining within the single market, which feeds into the third lesson whereby proposed legislation is assessed to ensure EU law compatibility. The final lesson proves that tailor-made agreements have become more difficult

---

764 S. Jenni (2016) Is the Swiss model a Brexit solution? The UK in a Changing Europe, 23 March 2016, available at http://ukandeu.ac.uk/is-the-swiss-model-a-brexit-solution/ accessed 24 November 2016

765 *Ibid*

766 *Ibid*

767 *Ibid*

to achieve.[768] Undoubtedly the current President of the EU Commission is Jean-Claude Juncker, who is openly pro-federalist, could potentially cause problems for the UK negotiations.[769] The EU can be uncooperative as evidenced by the Swiss model, whereby they simply refuse to agree upon the terms of a negotiation. In response to the Swiss affirming their position, their access to the electricity market was suspended and they were excluded from the EU's Horizon 2020 research funding.[770] In light of the fact the current threat requires international cooperation, this awkward postulated position by the EU could become rather problematic in terms of the UK's current cross-border counterterrorism capabilities. It could also be argued that the EU will purposefully make it rather difficult for the UK to negotiate a positive deal given the fact Juncker would not want more EU Member States to leave.

International Security: The European Arrest Warrant

The European Arrest Warrant (EAW) was introduced in 2004 to make extradition of those suspected of serious crime and terrorist swifter and simpler.[771] Although not specifically linked with surveillance of electronic communications data and intelligence exchange within the EU, with the UK leaving the EU in 2019 it may

---

[768] *Ibid*

[769] P. Popham (2014) Jean-Claude Juncker: The face of federalism, Independent, 6 June 2014, available at http://www.independent.co.uk/news/people/jean-claude-juncker-the-face-of-federalism-9504014.html accessed 24 November 2016. See also K. Mansfield (2016) 'It is crazy' that EU members would want to act 'individually' says federalist Juncker, Express, 15 September 2016, available at http://www.express.co.uk/news/politics/711181/Jean-Claude-Juncker-says-crazy-EU-members-would-want-to-act-individually accessed 24 November 2016

[770] *Supra* as per S. Jenni (2016)

[771] See European Commision website http://ec.europa.eu/justice/criminal/recognition-decision/european-arrest-warrant/index_en.htm accessed 9 December 2016

no longer continue. This measure does form part of the legal convergence mechanism aimed at the harmonisation of Member States laws within the EU. The EAW effectively removed central authorities from the extradition process, which is now dealt with by law enforcement agencies' and judicial authorities. It also meant that EU Member States could not refuse to surrender to another Member State their own citizens' who were suspected of committing a serious crime on nationality grounds.[772] It has been suggested the UK may lose some of these international counterterrorism capabilities upon leaving the EU. The EAW and the relationship with Europol and Eurojust are some prime examples. The EAW mechanism takes on average 48 days whereas prior to the EAW extradition used to take an average of one year.[773] This was used by the UK in apprehending Hussain Osman who went on to be prosecuted in the UK for his part in the planned, but failed, attempted terrorist attack on London 21st July 2005.[774] Equally, there are some however that would like to see the UK come out of the EAW arrangement.[775] Pollard cites a recent case involving Stuart Ramsay, an award winning Sky News correspondent who reported on an alleged firearm-

---

[772] *Ibid*

[773] European Commission (2011) Report from the Commission to the European Parliament and the Council On the implementation since 2007 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, Brussels, 11 April 2011, Com(2011), 175 final, p11, available at http://ec.europa.eu/justice/criminal/files/eaw_implementation_report_2011_en.pdf

[774] See http://www.dailymail.co.uk/news/article-467244/21-7-bombers-failed-kill-dozens-mastermind-maths.html accessed 24 November 2016

[775] S. Alegre and M. Leaf (2004) Mutual Recognition in European Judicial Cooperation: A Step Too Far Too Soon? Case Study—the European Arrest Warrant, European Law Journal, 10:2, 200-217. See also C. Kaunert (2007) Without the Power of Purse or Sword: The European Arrest Warrant and the Role of the Commission, Journal of European Integration, 29:4, 387-404. See also S. Molders, (2005) European Arrest Warrant Act is Void – The Decision of the German Federal Constitutional Court of 18 July 2005, German Law Journal, 7:1, 45-58

running network in Romania.[776] In response the Romanian Government have asserted the reporting was faked and charged Ramsay for spreading false information.[777] As part of the first step to issuing an EAW, they have requested the UK assist in the criminal investigation.[778]

Despite Kearney's assertion that the UK's exit would not affect the relationship with the EU because the UK has a unique and successful counterterrorism framework, this has been built upon the relationship within the EU.[779] For Peers the EAW remain an important aspect for the UK, and as a quick form of extradition is something the UK should keep. Without this it is possible that the UK may fall back on to an ECHR focused system, albeit similar to the EAW. According to Peers' oral evidence to the recent Home Affairs Committee, 'it would be something like the European arrest warrant, perhaps with exceptions, like Norway and Iceland have, but there might not be enough time to negotiate those exceptions, so we run the risk of falling back, rather than being able to negotiate something. The advantages of the European investigation order, which is not in force yet, might not be obvious for a few years, so we might end up falling out of that as well, rather than trying to stay part of it'.[780]

---

[776] S. Pollard (2016) The case that shows why we must not stay in the European Arrest Warrant, The Spectator, 3 September 2016, available at http://www.spectator.co.uk/2016/09/the-case-that-shows-why-we-must-not-stay-in-the-european-arrest-warrant/ accessed 9 December 2016

[777] *Ibid*

[778] *Ibid*

[779] J. Kearney (2016) The Security Implications of Brexit, Compas Breakfast Breifing Summary, available at http://www.compas.ox.ac.uk/media/160520-security-web-text.pdf accessed 24 November 2016

[780] Home Affairs Committee, house of Commons, EU Policing and Security Issues, 6 December 2016, HC806, Oral evidence by S. Peers, available at

The relationship with Europol is equally important especially in light if technological growth and the use of digital electronic communications by terrorists'.

International Cooperation: Europol

In essence Europol is a centralised computer hub that contains the shared intelligence of 28 EU Member States and 20 third countries including the US, Canada, Russia and Turkey.[781] Coming from the old third pillar of the TEU, it was envisaged Europol would be utilised as a system of information exchange. For Loader however, once confidence grew in the agency it was inevitable is would be promoted as a kind of US style FBI for Europe.[782] Since its foundation Europol has developed at quite a fast pace, evidenced by the 2003 Europol Annual Report which confirmed in 2003 there was a substantial increase in operational activities for the agency, and in 2002 the information exchange between Europol and the member states increased by 40%.[783] Europol has grown in external competences also, and now have external agreements with other agencies including Interpol, the United Nations Office on Drugs and Crime

---

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/eu-policing-and-security-issues/oral/44210.html

[781] See https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1, and https://www.europol.europa.eu/partners-agreements/strategic-agreements accessed 24 November 2016

[782] I. Loader (2002) Policing, securitization and democratization in Europe Criminal Justice, The International Journal of Policy and Practice, Vol 2(2), 125-153, 128

[783] Europol (2004) Annual Report 2003, available at www.europol.eu.int accessed 9 December 2016

(UNODC), and the World Customs Organisation (WCO).[784] Europol is also a support centre for law enforcement operations and provides expertise. Although at first glance there does not seem to be any difference between being an internal and external partner with Europol in terms of support or access to intelligence, for Guild the extent to which third countries are always at the demanding side of Europol is concerning.[785] Accordingly, 'they are always at the requesting side and they are never fully participating'.[786] Another concern is that, 'a lot of the measures relating to policing and criminal justice are subject to the data protection directive, which the UK has opted out of. As a member state that has opted out of the directive, the UK's position would be somewhat different'.[787]

In procedural terms Europol has a designated Europol National Unit (ENU) that serves as the liaison between the authorities in that country and Europol, although only seven third counties have opted to have them.[788] It would appear from news reports that the UK Government intends to remain within Europol despite the UK's exit from the EU.[789] Brandon Lewis the UK's Policing Minister appears to have recognised the reality that transnational crime will remain when the UK

---

[784] See https://www.europol.europa.eu/partners-agreements/other-agreements accessed 24 November 2016

[785] Home Affairs Committee, house of Commons, EU Policing and Security Issues, 6 December 2016, HC806, Oral evidence by E. Guild, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/eu-policing-and-security-issues/oral/44210.html

[786] *Ibid*

[787] *Ibid*

[788] See https://www.europol.europa.eu/partners-agreements accessed 24 November 2016

[789] K. McCann (2016) UK opts back into Europol despite Brexit vote, The Telegraph, 14 November 2016, available at http://www.telegraph.co.uk/news/2016/11/14/uk-opts-back-into-europol-despite-brexit-vote/ accessed 24 November 2016

leave the EU.[790] UK policing and security agencies do benefit from the level of expertise at Europol, which provides unique intelligence on cyber-crime in addition to terrorism. Operation Golf is one such example where the Metropolitan Police and the Romanian National Police set up a Joint Investigation Team, which led to the rescue of 28 children and the arrests of over 125 individuals for offences including trafficking human beings, money laundering, and child neglect.[791] More recently in May 2016 a similar operation took place involving France, Paraguay and Spain.[792] Specifically in terms of terrorism, Kearney argues Europol is largely irrelevant.[793] However, policing and security officials who deal with the UK's terrorist threat daily are of a different opinion, confirming Europol to an essential element in combatting the threat.[794]

Europol also produce an annual TE-SAT report, with the 2016 edition assessing the terrorist threat posed from Islamist, ethno-Nationalist and separatist, left-wing and right wing groups, including single-issue threats.[795] The report shows that:

> In 2015 the European Union (EU) experienced a massive number of casualties caused by terrorist attacks. By far the most affected Member State was France, which had to cope with losing 148 citizens' and seeing

---

[790] *Ibid*

[791] J. Taylor (2010) Police smash Romanian 'child trafficking ring', The Independent, 12 October 2010, available at http://www.independent.co.uk/news/uk/crime/police-smash-romanian-child-trafficking-ring-2104694.html accessed 24 November 2016

[792] See https://www.europol.europa.eu/newsroom/news/europol-supports-successful-operation-against-human-trafficking-network accessed 24 November 2016

[793] *Supra* as per J. Kearney (2016)

[794] J. Rankin (2016) Europol chief says Brexit would harm UK crime-fighting, The Guardian, 22 June 2016, available at https://www.theguardian.com/politics/2016/jun/22/europol-chief-says-brexit-would-harm-uk-crime-fighting accessed 24 November 2016

[795] *Supra* as per Europol (2016)

> more than 350 injured in attacks perpetrated in January and November. Murders and injuries in 2015 resulted from both unsophisticated lone actor terrorist attacks and well-coordinated, complex attacks by groups of militants. The carefully planned attacks demonstrated the elevated threat to the EU from a fanatic minority, operationally based in the Middle East, combined with a network of people born and raised in the EU, often radicalised within a short space of time, who have proven to be willing and able to act as facilitators and active accomplices in terrorism.[796]

The lasted figures to this regard are:

[796] *Ibid*

Figure 15, Terrorist attacks and arrests in the EU in 2015, taken from Europol (2016) EU Terrorism Situation and Trend report TE-SAT 2016, Hague: Europol

The difficulty the UK has in terms of negotiating a relationship to maintain access to Europol is three fold. Firstly for Guild it is a question of value, as in the value of the UK's contribution to intelligence. From the counterterrorism perspective, Guild confirms that from what he has seen in the 'documents of the perspective, concerns and worries, the contribution there is perhaps not so evidently enormous as it is in the cybercrime field'.[797] According to Peers however, it may come down to a matter of money, and the UK's level of personal data protection, as raised by Guild above.[798] Representing a further obstacle is that although the Council and the Commission may well confirm the UK's data protection is adequate in providing safeguards, the European Parliament may cause difficulties, particularly should they send it to the CJEU, or 'individuals might challenge it, as they have done in the United States, for instance, through information commissioners and national courts'.[799] Peers elaborates and states that:

> Europol is quite closely connected to other EU legislation on data sharing because Europol has access to the EU's databases and uses that as part of its analyses, so it might be difficult to think about a deal on Europol access in isolation, especially if we talking about a bespoke deal with different rights than other non-EU countries.[800]

---

[797] Home Affairs Committee, house of Commons, EU Policing and Security Issues, 6 December 2016, HC806, Oral evidence by E. Guild, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/eu-policing-and-security-issues/oral/44210.html

[798] *Ibid*, Home Affairs Committee, Oral evidence by S. Peers

[799] *Ibid*

[800] *Ibid*

In terms of personal data, there will undoubtedly be an assessment of how effective and strong the UK's personal data laws are, particularly in light of the IPA that has just passed, which for Peers will face legal challenges to it in the UK and in the ECtHR. There may be a problem in light of the CJEU's judgment in Tom Watson's case that will be decided on the 21st December 2016. Based on an appeal on the earlier challenge to DRIPA, this represent a parallel Swedish case where the Court may decide to 'set out a series of problems with the prior legislation' which can then be read across to see if those problems also exist within the IPA'.[801] Peers continues this point and states:

> [The UK] obviously offer more than other states do and that has a knock-on effect in terms of access to other databases as well, because of the connection with that and Europol. The downside in the UK Government's argument is the potential complaint that might be made about the [IPA]. We will know, first of all on the 21st, and then probably in January or February with the Canada case, exactly where we stand in terms of what it would take. Maybe some kind of carve-out might be possible—if there is a problem with the rest of the [IPA], we will treat the information that we receive from or give to the European Union in a different way to satisfy the adequacy standards.

Armond confirms Peers' assertion and goes further explaining that the UK's access to EAW's must continue because:

> Since [EAW's] have been linked to [the Schengen Information System] SIS II, over 2,000 offenders have been arrested in the UK, and 150 offenders wanted by the UK have been arrested in the EU. That is a 25% increase in a year. They are not individuals who are wanted for minor offences; those are serious offences. I would argue that we are not doing work for Europe; we are actually defending the citizens' of the UK by arresting criminals who present a threat to society and are present in our shores. Those are the things that I would put at the top of the list.

---

[801] *Ibid*

The Schengen Information System

The Schengen Information System (SIS) follows a similar story to that of Europol in terms of the UK's relationship and negotiation, and the exit may affect the UK's access. The SIS is a large-scale information system and database that supports external border control and law enforcement cooperation, thereby protecting internal security. Although the UK is not a member of the Schengen Area, it does have access to the SIS within the context of law enforcement cooperation.[802]

[802] See http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm accessed 25 November 2016

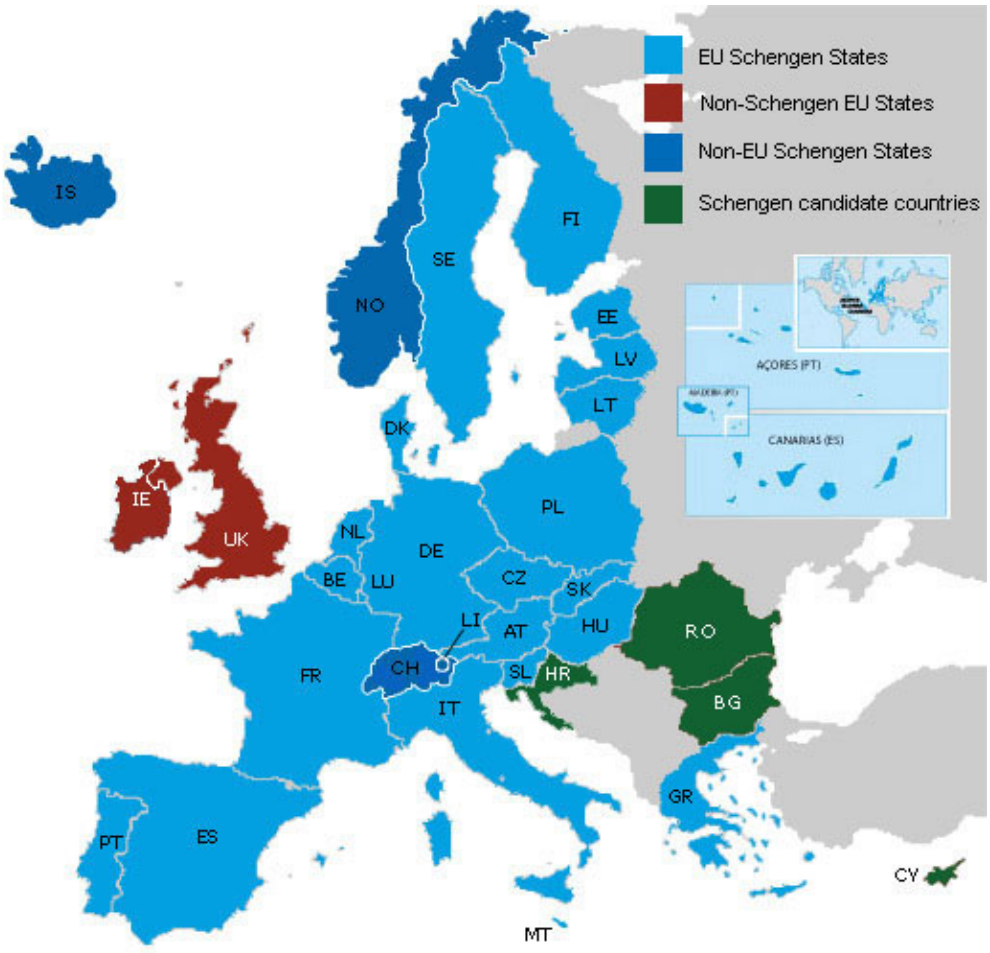

Figure 16, Map of Schengen Countries, taken from https://www.google.co.uk/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiOmZats-fQAhWLnBoKHfSZCF4QjhwIBQ&url=http%3A%2F%2Fec.europa.eu%2Fdgs%2Fhome-affairs%2Fwhat-we-do%2Fpolicies%2Fborders-and-visas%2Fschengen%2Findex_en.htm&psig=AFQjCNGqJrZlSbhJ02wVSBHPA9vAbw4BDQ&ust=1481382862154127 accessed 9 December 2016

SIS however still replied on a certain level of data protection, similar to the EU and Europol. There may have been some recent rules changes following their meeting on the 7th December 2016, however details of this meeting have not been released.[803] It is likely there will be an 'increase in the amount of information collected, access to it and purposes for which it can be used, particularly in

[803] See https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/CSIS accessed 9 December 2016

counter-terrorism'.[804] SIS is an important tool, used for 'facilitating European arrest warrants, which includes stolen vehicles, missing people, people wanted for discussion with the police and people under surveillance, maybe for counter-terrorism activities'.[805] Given the current relationship is somewhat removed from EU membership it is possible the UK's access will continue as a part of Europe. On 13th April 2015, UK law enforcement joined the SIS II increasing the sharing of intelligence.[806] Armond, Deputy Director General of the UK's National Crime Agency stated:

> SIS II has been a game-changer since it came online in April 2015, and access to it must remain…it is so important not only in terms of our border security, but in relation to work that police officers conduct every day on the street because 66 million records are available to them in the street via their radios and the police national computer. It is a very important function.[807]

The sharing of intelligence data not only takes place through SIS, but also other mechanisms, such as those dealing with airline passenger travel, the rules around which changed substantially following the 2001 attack on the USA.

---

[804] *Supra* as per Home Affairs Committee, Oral evidence by S. Peers

[805] *Ibid*

[806] See http://www.nationalcrimeagency.gov.uk/publications/european-arrest-warrant-statistics accessed 9 December 2016

[807] *Supra* as per Home Affairs Committee, Oral evidence by D. Armond

PASSENGER NAME RECORDS DATA AND ADVANCED PASSENGER INFORMATION: CASE STUDY IN RELATIONS BETWEEN THE EU AND THIRD COUNTIRES

Conducting a case study on intelligence data exchange is essential at this point given the UK is on course to leave the EU in 2019. It has been shown in the previous Chapter, that the EU takes data privacy protection seriously. Strict legislative controls are in place and the importance of remaining within the EU's ambit to this regard, in order to maintain intelligence data exchange will be illustrate below. Advanced Passenger Information (API) covers the basic details concerning the passenger that include name, date of birth, nationality and passport number.[808] PNR however, includes data usually submitted by the passenger at the time of making the travel arrangements, including details such as, credit card details, personal contact information, dietary information and sensitive data on ethnic origin, health, political views and sexual orientation.[809] Due to the fact API carries less personable data, the EU Directive ensuring data exchange within the EU for example was quickly adopted in 2004.[810] PNR agreements on the other hand have been controversial to say the least, impacting upon citizens' right to data protection, enshrined at the EU constitutional and EU law levels as discussed in the last chapter.

---

[808] M. Tzanou (2015) The war Against Terror and Transatlantic information Sharing: Spillovers of Privacy or Spillovers of Security? 31(80) *Utrecht Journal of international and European law*, 87-103, 96

[809] E. Brouwer (2009) The EU Passenger name record System and Human Rights: Transferring passenger data or passenger freedom, CEPS Working Document no.320/September 2009, p.3

[810] EU Council Directive on the obligation of carriers to communicate passenger data, 2004/82/EC, 29 April 2004, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:261:0024:0027:EN:PDF

An internal PNR agreement between the 28 Member States has been slow. The first attempt failed in 2011 due to the fact it did not have sufficient safeguards in place to protect individual data privacy.[811] The second attempt at a PNR Directive was passed in April 2016, giving Member States until the 25th May 2018 to implement it into national law.[812] Similar to the external PNR agreement with the US, this Directive has put various safeguards into place, such as a 'controller' who will oversee the processing and exchange of data, ensuring requests made are proportionate.[813] Member States must also provide a data protection officer, who will offer advice to the controller and other employees from the policing and security agencies, thereby monitoring compliance with the Directive.[814] Article 54 of the Directive also ensures that those citizens' affected by the provisions will have a judicial remedy. The rationale behind this heightened protection is the CJEU's decision in the *Schrems* and *Digital Rights* cases.[815] Member States have been encouraged to implementation the new PNR

---

811 European Commission (2011) Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, available at http://ec.europa.eu/homeaffairs/news/intro/docs/com_2011_32_en.pdf accessed 23 August 2016

812 Directive (EU) 2016/681 of the European Parliament and of the Council, of 27th April 2016, on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, available at http://eur-lex.europa.eu/eli/dir/2016/681/oj accessed 23 August 2016

813 *Ibid* at Article 3(8), 19 and 20

814 *Ibid* at Article 32 and 34

815 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others,* delivered on 8th April 2014 and reported at [2015] QB 127. Referred to as *Digital Rights Ireland*

directive urgently and not wait two years as the directive allows, and thereby harmonize the exploitation of the PNR data.[816]

The PNR data sharing agreement between the UK and the EU is another issue whereby the UK's continued access to it is essential. For Armond:

> [Access to PNR] is absolutely essential in terms of the profiling that we do to protect the UK. Of course, prior to recent agreements, it was long the case that because of free movement agreements in Europe, many European nations were not prepared to share passenger name record data with us. It is much more interesting, much more detailed and much more relevant than advance passenger information, and of course it gives us names, bank account details, phone numbers, details of previous travel and who people have travelled with. All of that material is really useful in terms of developing profiles and preventing the most dangerous people from coming to our country.[817]

As with the UK's continues access to Europol, any type of bulk data collection and retention must satisfy the Digital Rights Criterion developed in Chapter Three. Representing a further impact on EU law making, the EU's Directive must safeguard personal data and ensure it is protected, to in turn safeguard the Directive being invalidated by the CJEU. If UK is to maintain access to PNR within the EU, then the UK's legislation must still provide adequate protection. Ensuring that the Digital Right Criterion and the lessons learned from *Schrems* are employed fully should mean that the UK could maintain a relationship equal to the current standard. However, this is unknown territory for the UK and therefore

---

[816] Council of the European Union, State of play on implementation of the statement of the Members of the European Council of 12 February 2015, the JHA Council Conclusions of 20 November 2015, and the Conclusions of the European Council of 18 December 2015, Brussels, 4 March 2016, available at http://data.consilium.europa.eu/doc/document/ST-6785-2016-INIT/en/pdf

[817] *Supra* as per Home Affairs Committee, Oral evidence by D. Armond

one should look to how other third countries have agreed upon intelligence and data exchange.

THE PNR AGREEMENTS BETWEEN THE US AND EU: THE SNOWDEN EFFECT

For Kaunert and Zwolski the first international PNR agreement between the EU the US merely represented the EU's attempt to play a significant role in the war on terror, which did not involve military action that had proved divisive since the Afghan conflict following 9/11.[818] A noteworthy increase in EU-US counterterrorism cooperation was seen following the terrorist attack on the US on 9th September 2001.[819] Kaunert and Zwolski break this cooperation down into two areas, the Justice Dialogue and the Policy Dialogue on Borders and Transport Security.[820] Although the Justice Dialogue started in 1998 to ensure information was transferred to the US, it has become increasingly important since the development of 'new EU competences in criminal judicial and police cooperation'.[821] Particularly since 2002, the Dialogue has been essential for negotiating agreements on mutual legal assistance and extradition, including liaison issues with the newly continued enhancement of Eurojust and Europol.[822] During this time the US introduced several measures aimed at strengthening

---

818 C. Kaunert and K. Zwolski (2013) *The EU as a Global Security Actor: A Comprehensive Analysis Beyond CFSP and JHA*, Palgrave Macmillan, p.96

819 *Ibid*

820 *Ibid* at p.97

821 *Ibid*

822 *Ibid*

border security, including the Container Security Initiative, the collection of PNR and the use of biometric passports.

These measures are unsurprising given the international nature of the current terrorist threat; the point has been made in previous chapters that international security and national security carry the same weight in terms of importance.[823] By this border security extension however, the US Homeland Security policies, specifically surrounding intelligence, policing and law enforcement, the financing of terrorism and justice, had vast implications for the EU that resulted in reinforcing cooperation.[824]

Under the US Aviation and Transport Security Act 2001, all airline companies operating passenger flights to the US, must provide US authorities with electronic access to PNR.[825] This requirement caused a problem for EU airline companies, putting them under an obligation to disclose as per US law, and an obligation not to disclose as per EU law, placing them at risk of compromising EU data protection laws, which inevitably could result in EU financial fines of up to $6,000 (USD) per passenger.[826] This rock and hard-place scenario led to the EU Commission deciding to take on the challenge of negotiating with the US and

[823] *Supra* as per The RT Hon Lord Lloyd of Berwick (1996) Chapter 2 paragraph 2.4

[824] *Supra* as per C. Kaunert and K. Zwolski (2013) p97

[825] *Supra* as per C. C. Murphy (2015) p.158

[826] P. Pawlak (2009) Made in the USA? The Influence of the US on the EU's Data Protection Regime CEPS – Liberty and Security in Europe, Centre for European Policy Studies website http://aei.pitt.edu/15102/1/madeusa-influence-us-eus-data-protection-regime.pdf accessed 14 November 2016

they managed to delay the implementation of the measures on the grounds that the EU were required to comply with the 1995 EU Directive on the protection of personal data.[827] The 1995 Data Protection Directive orates that no personal data should be transferred to any third country unless the EU Commission has determined that its data protection system provides an, 'adequate level of protection of basic freedoms and rights of individuals'.[828] For Lowe, this represented the central obstacle for the EU in agreeing to a PNR data exchange agreement with the US.[829] The legal culture between the EU and the US is remarkably different, as the EU focuses on the dignity of citizens' in protecting fundamental human rights and the rule of law, in addition to the legislative data privacy protection, whereas the US focuses on liberty, and thereby has no explicit protection for data privacy under the Bill of Rights.[830] Rather legal scholars simply infer one from the specific rights in the First, fourth, Fifth and Ninth Amendments.[831] Because the US privacy framework did not meet EU standards the EU Commission developed a rather original solution, called the 'Safe Harbour' scheme.[832] This scheme was aimed at commercial practices and although the adequacy was challenged in 2002 and 2004, nothing changed. For Van Wasshnova, this scheme lacked basic adequacy being insufficiently clear and

---

827 *Supra* as per C. Kaunert and K. Zwolski (2013) p97

828 D. Lowe (2016) The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit For Purpose? *International Criminal Law Review*, 16:5, 856-884, 860

829 *Ibid*

830 *Supra* as per S. Sottiaux (2008) pp.265-322.

831 *Supra* as per J. Q. Whitman (2004) 1115-1221

832 EU Commission Decision 2000/520/EC

precise, hence why the EU Commission finally determined it was not possible for them to agree upon PNR with a US state department alone.[833] On the basis of the Commissions adequacy decision they agreed on the transfer of PNR intelligence, but required the US guarantee an adequate level of data protection for the transferred data.[834] This agreement received EU Council approval in 2004.[835]

Criticisms of this agreement came primarily from the European Parliament (EP), having been marginalised throughout the negotiation instigated proceedings through the CJEU, arguing the level of protection guaranteed by the US was below EU standards, and the agreement was based on the wrong law dealing with transport being Article 95 EU (now Article 114 TFEU). For Ilbiz *et al*, the latter point is much more prevalent given that that early PNR data agreements such as this, focused far too heavily on expanding and prioritising counterterrorism cooperation to the detriment of data protection rules.[836] The CJEU in 2006 focused on the former point and annulled the PNR agreement based on the fact they pertained to criminal justice co-operation and thereby the public security

---

[833] M. R. Van Wasshnova (2006-2008) Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange, 29 *Case Western Reserve Journal of International Law* 827, 832

[834] EU Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, (2004/496/EC), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004D0496

[835] *Ibid*

[836] E. Ilbiz, C. Kaunert and D. Anagnostakis (2015) The counterterrorism agreements of Europol with third countries: data protection and power asymmetry, *Terrorism and Political Violence,* 1-18, 2

framework, and not on the regulations of the internal market.[837] The CJEU made this clear in confirming that the now Article 114 TFEU was incompatible with Article 25 of the Data Protection Directive, which excluded the processing of personal data for 'public security, defence, state security and the activities of the state in areas of criminal law'.[838] As a result the PNR agreement was annulled on the basis that the Commission could not lawfully use the Data Protection Directive, and the Council was not competent to conclude the agreement on that foundation.[839]

Unfortunately, the adequacy of data protection under the Directive received very little discussion, which meant that any future PNR agreements must be based within the framework of the third pillar, in turn excluding the EP from the decision making process, arguable despite the future Treaty of Lisbon abolishing the old system and providing the EP with more decision making powers.[840] This meant that the second PNR agreement had to be based on the CJEU's findings, which Gilmore and Rijpma describe as a 'poisoned chalice' in terms of improving human rights and data protection compliance agreements.[841] For Murphy, this result could be termed perverse in that the 'constitutional role of the rule of law

---

[837] Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union and Commission of the European Communities* [2006] ECR I-4721

[838] Data Protection Directive 1995, 95/46/EC, Article 3(2) and 25

[839] Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union and Commission of the European Communities* [2006] ECR I-4721, [61], [70]

[840] *Supra* as per C. Kaunert and K. Zwolski (2013) p.98

[841] G. Gilmore and J. Rijpma (2007) Joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission*, Judgement of the Grand Chamber of 30 May 2006, [2006] ECR I-4721, 44 *Common Market Law Review* 1081, 1098

played a part in undermining the principle's safeguarding role'.[842] The EU Council therefore would lead the negotiations with the assistance of the Commission. In the meantime an interim PNR agreement was put in place to ensure continued intelligence sharing.[843] The second agreement was approved in 2007, creating two main issues where the adoption was based upon the Court's findings and properly under Police and Judicial Co-operation in Criminal Matters (PJCCM), and where it was agreed the US would receive less fields of data than under the first agreement that could be 'pulled' from the airline carriers database, 19 rather than 34.[844]

With regards the latter point, Papakonstantinou argues the reduction was not a reduction at all however.[845] Instead the original 34 fields of data were merged to merely give the appearance of a reduction.[846] As part of the negotiation and in exchange for reducing the fields of data, the EU agreed for the US authorities to share the data with an increased number of internal agencies, and to store the data for 15 years.[847] It was further agreed that the Department of Homeland Security be permitted to access 'sensitive data' where 'the life of a data subject or of others

---

[842] *Supra* as per C. C. Murphy (2015) p.162

[843] *Ibid* p.161

[844] EU Council Decision 2007/551/CFSP/JHA on the signing, on behalf of the European Union, or an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Records (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (hereafter, Second Agreement)

[845] V. Papakonstantinou and de Hert (2009) The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework of Either Side of the Atlantic, 46 *Common Market Law Review* 885, 914

[846] *Ibid*

[847] *Supra* as per C. Kaunert and K. Zwolski (2013) at p.99

could be imperilled of seriously impaired'.[848] For Murphy, this broad test renders sensitive personal data 'open to widespread use by US law enforcement authorities'.[849] With regards the former issue, concluding the agreement under the authority of PJCCM resulted in significant consequences for the regulatory framework within the operation. The roles of both the EP and national Parliaments, and CJEU in terms of oversight were therefore reduced.[850] Not surprisingly the EP criticised this second agreement, mainly based on the lack of democratic oversight within the PNR agreement, coupled with the fact that the US agreement took little to no account of the PNR agreement with other nation states, such as Canada and Australia, which for Kaunert provide an as surety of 'higher standards of protection of personal data'.[851] The Canadian agreement for example allows the PNR data to be held for six years, with the Australian model allowing for five years and six months.[852]

---

[848] Department of Homeland Security, US letter to the EU, III Types of Information Collected, OJL204/21, 4 August 2007, available at https://www.dhs.gov/sites/default/files/publications/privacy/pnr-2007agreement-usversion.pdf

[849] *Supra* as per C. C. Murphy (2015) p.163

[850] G. Gilmore and J. Rijpma (2007) Joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission*, Judgement of the Grand Chamber of 30 May 2006, [2006] ECR I-4721, 44 *Common Market Law Review* 1081, 1098

[851] *Supra* as per C. Kaunert and K. Zwolski (2013)

[852] EU Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service. And Council Decision 2006/230/EC of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data

Rather unmistakably this second PNR agreement was favourable towards the US, rather than towards the EU. This adds weight to Lehrke and Schomaker's hypothesis that because the EU is more embedded in its networks with the US, the US found itself able to exert influence on the EU Council and Commission.[853] According to Lowe, this hypothesis, 'builds on Pawlak's earlier study who states as the EU's security consciousness has not developed as rapidly as the US, the US has the opportunity to exert a big influence on the transatlantic agenda with the US dictating and shaping the EU's security agenda'.[854] This second agreement was in turn replaced with a third PNR agreement in 2012, following the adoption of the Lisbon Treaty 2007, which provided the EP with increased decision-making powers.[855] Introducing this third agreement the EU Council confirmed the legal framework for PNR data exchange would not only assist with border crimes, but it would greatly increase the capabilities inherent in the prevention and detection, investigation and prosecution of terrorist offences.[856] The third agreement resembles greatly the second in terms of broadness, retention periods and access to the data.[857]

---

[853] J.P. Lehrke and R. Schmaker (2014) 'Mechanisms of Convergence in Domestic Counterterrorism Regulations: American Influence, Domestic Networks and International Networks', 37(8) *Studies in Conflict & Terrorism*, 689-712, 693

[854] *Supra* as per Lowe (2016)

[855] C. Kaunert, S. Leonard and A. McKenzie (2012) The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT', 21(4) *European Security*, 474-496, 485.

[856] Council of the European Union, Council adopts new EU-US agreement on passenger Name Records (PNR), (2012) 9186/12, PRESSE 173, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf accessed 14 November 2016

[857] See Article 8 http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416915581157&uri=CELEX:22012A0811(01)

The Broadness of the External PNR Agreements: Access, crime and human rights

The CJEU added that legislation allowing public authorities' access to the stored electronic communications data on a 'generalised basis' must be 'regarded as compromising the essence of the fundamental right to privacy'.[858] In addition to the 15 years retention period and the so called reduced fields of data covered, the list of agencies permitted to access PNR data have been lengthy, including law enforcement agencies' not generally associated with counterterrorism. The first agreement included the Inland Revenue Service and Animal Plant Health Inspection Service for example.[859] The interim and second agreements included an infinite number of agencies with the addition of the Office of the Department of homeland Security and all entities that directly support it'.[860] The types of crimes listed under these agreements were also vast and broadly phrased to include other types of crimes' in addition to serious crimes and terrorism.[861] Article 4 of the third PNR agreement provides the same extremely broad provisions, including threats to commit crime, and 'other crimes' punishable by a sentence of three years or more.[862] During the PNR agreement negotiations, the EP, Article 29 Working Group, European Data Protection Supervisor, and

---

[858] *Supra* as per D. Lowe (2016) 860

[859] D. R. Rasmussen (2008) Is International Travel *Per Se* Suspicion of Terrorism? The Dispute Between the United States and the European Union over Passenger Name Record Data Transfers 26 *Wisconsin International Law Journal* 551

[860] *Ibid* at 585

[861] *Ibid*

[862] See http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416915581157&uri=CELEX:22012A0811(01)

national parliamentary organisations such as the UK House of Lords EU Committee have all conveyed severe trepidations relating to individual privacy protections.[863] These centred on the fact that transferring such data to the US may violate the EU's high-principled standards of data protection.[864] PNR data has been referred to as broader than what could be considered 'adequate, relevant and not excessive'.[865] It has been further argued that access to the data should be limited to reasons of terrorism and serious crime only, and that sensitive data should be abandoned entirely thereby ensuring compatibility with the Directive.[866]

Policing Cooperation: EU and US intelligence

EU and US policing cooperation has mainly been based on agreements reached by the EU and US. Following the terrorist attack on the US on 9th September 2001, the EU demonstrated eagerness to show solidarity with the US and asked the then Director of Europol to draft an intelligence exchange agreement.[867] Focusing on strategic and technical information concerning serious forms of international crime, the first agreement was adopted by the EU Council in December 2001.[868] This agreement provided for the identification of personnel named as points of

---

[863] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. See http://ec.europa.eu/justice/data-protection/article-29/index_en.htm. For information on the UK House of Lords EU committee see http://www.parliament.uk/hleu

[864] *Ibid*

[865] Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 13 June 2003, p.7

[866] *Ibid* at pp.7-8

[867] *Supra* as per C. Kaunert and K. Zwolski (2013) p.102

[868] Council (2001) Conclusions Adopted By The Council (Justice and Home Affairs) Doc. SN 3926/6/01 20 September 2001

contact, information exchange, mutual consultation, exchange of expertise and liaison officers, specifically for crimes committed or likely to be committed in the course of terrorist activity.[869] The second agreement took longer to negotiate as the EU's direction in terms of personal data protection had developed and changed in approach to that of the US. For Rees the EU had passed a significant amount of data protection legislation due to the fact member states had tended to keep large amount of data of their citizens', and in contract the US's approach to this was more *ad hoc* and somewhat relaxed, whereby relatively small amounts of data was held and kept.[870] Regardless the agreement was passed in December 2002 and although criticised by civil liberties campaigners the agreement contains many data protection safeguards including the principle of 'purpose limitation', whereby intelligence can only be used for the specific purpose under which it was obtained.[871] These agreements remain in place to date despite the Snowden revelations that could have potentially damaged this relationship.

CONCLUSION

The UK is in a unique position when it comes to the relationship with the EU as a Member State. This position will undoubted remain so given the legislative influence the EU has had on the UK since the enactment of the European Communities Act 1972. As a new third country to the EU, the UK may have to

---

869 *Ibid* at Article 3

870 W. Rees (2006) *Transatlantic Counter-Terrorism Cooperation: The New Imperative*, (Routledge) p.92

871 V. Mitsilegas (2003) The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data, *European Foreign Affairs Review*, 8, 515-536, 519

negotiate many provisions surrounds security, intelligence and data exchange, and future counterterrorism measures. On striking the balance between national security and human rights, it could be argued that the USA leans more to the interests of national security over individual human rights, whereas the EU Member States lean more towards the interests of human rights.

In order to maintain a relationship with the EU, and the many agencies the UK Government must retain its affiliation with human rights and preserve the data protection laws. It is for now; unclear whether or not the UK will continue to have access to Europol, the EAW or SIS II and PNR data. This chapter has shown that according to those who work within policing, the UK's continued membership and access to these are essential to keeping the UK safe. Four problems to the UK's successful negotiation to this end have been highlighted,

1. Money: The EU fund Europol and other measures, this will therefore cost the UK and may not be separated from other institutions;
2. Value of Contribution: The UK must evidence the level of contribution it could make to Europol;
3. Data Protection: Following the enactment of the IPA this may become a problem. For the time being at least the bulk powers provisions are untested, but the decision on the 21st December 2016 may provide an indication;
4. Uncooperative: Following the Swiss model, the EU can be very uncooperative. With Juncker in charge this may be more difficult.

CONCLUSION

The thesis begins with an examination of the UK's legal definition of terrorism under section 1 of the Terrorism Act 2000. This is important to the thesis because UK law enforcement agencies' and the courts use the definition when ascertaining that the activity they are dealing with is terrorism. It found that several elements of the definition, namely the lack of defined phrasing used and the resulting broadness, impact upon the rule of law and individual human rights. Through consideration two problems exist. The first concerns the proliferation of undefined causes that has resulted in some difficulty in deciding which to apply to a particular case, thereby effecting at least to some degree judicial application. The analysis found that the second issue is intrinsically linked to the first, but with an increased focus on the political currency attached to the term 'terrorism'. Both problems are not rectifiable due to both the extremely varied 21st Century terrorist threat and the political nature of international agreements. The analysis did however, find that a general criminal offence of terrorism may assist in taking the subject out of the political realm and firmly set into the legal. To this end, inserting exclusion clauses into this definition, covering actions taken by way of protest and industrial action and dissent, or during an international armed conflict in accordance with customary international law, would further assist.

Chapter Two concluded that the dynamics of private life have changed, following the advancements made in 21st Century communications technology, with people

living their lives increasingly online. To that end private conversations simply no longer take place in the citizens' home or through using a landline telephone, but rather online through the Internet, social media and through the ever-growing list of chat applications available on the smartphone, allowing encryption. What follows the legitimate use of technological advancements is criminal, or in this case terrorist exploitation. With terrorists using the Internet to communicate their propaganda and with each other, the resulting law enforcements investigatory capabilities gap must be filled. It highlights the growth in technology, which is estimated to double every two years, and using the Islamic State as a case study, they have used this to fashion an extraordinary threat level whereby law enforcement have difficulty in recognising friend from foe. It simply cannot continue to be the case, that law enforcement is denied investigatory powers within the realms of the Internet, when clearly there is a criminal exploitation and terrorist problem.

In fulfilling their task of protecting national security and protecting the citizens' right to life Chapter Three explores the vast powers of surveillance provided to law enforcement. In conjunction with the EU, the UK has enacted new laws and regulations over time to close the capabilities gaps as and when they appear, due to technological advancements are made. Allowing law enforcement to monitor Internet traffic has simply become an essential in the fight against terrorism, and in the States duty to protect its citizen's lives. To this end, the UK Government has recently enacted the IPA that introduces the ability to bulk collect and retain

electronic data communications, and to seek the operators' assistance in decryption. The examination highlighted the fact that although the IPA attempts to take a human rights approach, the main contentious elements in the Act are those in relation to the authorities' capabilities to intercept electronic communications data on mass, and to retain such data, and to legally hack into the populations equipment, again on mass, often using backdoors into encrypted online services.

The analysis went on to evidence that terrorist groups and self-starters have embraced modern communication technology, using it from marketing up to coordinating an attack. It also concluded that some legislative measures have failed to combat terrorism communication, such as the section 1 and 2 of the Terrorism Act 2006, and sections 57 and 58 of the Terrorism Act 2000. Chapter three continued to critically analyse the legalised pre-emptive measures, including temporary travel restrictions and the criminalisation of neutral behaviour. Utilising the doctrinal methodology, terms used such as mass data surveillance and pre-crime measures have been discredited. It was shown it would be physically impossible for law enforcement to conduct surveillance on the whole of the UK populations' electronic communications data. It has further been shown that the term 'pre-crime' is simply a fabrication and misleadingly used, given that pre-emptive measures are in fact criminal offences.

It was argued that a unique threat has been created, whereby the vertical effects of terrorist groups' communication influence others, then the horizontal effect that allows people to operate under an anonymity cloak. Concerning is the growth in the apparent advanced independent operational abilities of terrorists, with the potential access to explosives and firearms purchased on the darknet. It was made clear that legislation is required aimed at policing Internet traffic. A cooperative approach with ISP's is essential to this aim, ensuring the dark sides of the web are monitored and then removed should they be deemed to be providing illegal materials.

This in turn has resulted in new measures, providing bulk interception of communications data and bulk equipment interference, which have been deemed to be extraordinarily powerful tools to be wielded, having a much bigger impact upon individual privacy than traditional communications interception and surveillance might have had. Intercepting electronic communications data and content is not the same as intercepting a landline call as evidenced in this chapter. Additionally it is unhelpful and disappointing to note the IPA does not expressly cover OSINT and SOCMINT collection, although the Government had plenty of time to implement such measures. Chapter Three also showed that communications data, by the very nature of its digital form, is ideal for analysis and profiling individuals. Data mining will increasingly become autonomous as automatic computer algorithms carry out the first bulk interception step. Aimed at the population as a whole who are not suspected of being involved in any

criminal or terrorist activity, subject to authority these bulk powers have the potential to effectively destroy the privacy rights of millions of people, in order to find the elusive terrorist in the haystack. Although the IPA may pass through the digital rights criterion as highlighted in Chapter Four, and could be described as necessary in finding would-be-terrorists, it may ultimately come to fail the ECtHR jurisprudence when testing the proportionality of the retention of data and the bulk power measures.

Chapter Four further emphasised that fact that the EU has been the most influential on the UK's law making processes. The CJEU in particular has proved the most influential judicial body in terms of individual data protection, through its key judgements in *Digital Rights Ireland*.[872] The CJEU has achieved this by applying the EU's constitutional and legal prowess in protecting data protection, such as Article 8 of the Charter of Fundamental Rights and byway of two directives, namely the Data Protection Directive in 1995 and the e-Privacy Directive in 2002.[873] It was concluded that in order to keep the capabilities gap closed, the UK Government must ensure the law endures by safeguarding the cohesiveness with the jurisprudence of the CJEU and the European Court of Human Rights (ECtHR). These human rights focused courts do focus on different

---

[872] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and the conjoined case of Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*

[873] European Union Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Also: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. See also *S and Marper v UK* [2008] 48 ECHR 1581, [66]-[67], the Court noted the concept of private life is a broad term not susceptible to exhaustive definition.

elements, built around the Conventional rights, with the CJEU focused on data protection and the ECtHR on Article 8 right to privacy.

The level of data protection becomes even more important in Chapter Five, as in order to maintain, or indeed build new agreements with regards to data intelligence exchange; these must be protected to a level agreed by the EU. It is for now however, unclear whether or not the UK will continue to have access to Europol, the EAW or SIS II and PNR data. Chapter Four explores these issues and illustrates that according to those who work within policing, the UK's continued membership and access to these are essential to keeping the UK safe. EU levelled data privacy protection has been highlighted to be one of the three pre-existing conditions that must be met in order to assist in the UK's negotiation. Other issues potentially surround money and the value of contribution, and the UK's agreement to other measures. It was concluded that following the Swiss model emphasises the potential problems an uncooperative EU can be.

Using the US and EU's PNR agreement as a case study for the UK, demonstrates the importance the EU place on data privacy protection. Overall, should the UK law be considered as providing adequate protection, looking forward and perhaps focusing on some of the potential stumbling blocks to successful negotiation, the situation may not be as worse as first thought.

In terms of answering the question posed by the thesis, it has found that there are, and will perhaps always be, conflicting issues between collective security and upholding individual human rights protections, specifically regarding the gathering and retention of electronic communications data, the sanctioned use of the bulk powers under the IPA and the sharing of intelligence, both domestic and international. Following the analysis, the thesis found that this balance in the UK is fairly steady because of the role and importance of judicial review; judicial independence, and the over-arching scrutiny provided by commissioners and parliamentary committees. It must also be accepted that at times, individual privacy rights must be secondary to the absolute human right to life.

The value of these powers has been evidenced through the thesis, and particularly emphasised by the professionals working within the policing and security agencies. This point has also been given credibility by the many Governmental Committee hearings into law enforcements action. Continually reports suggest that there is no shortage of individuals mounting or attempting to mount terrorist attacks. This is further evidenced the 2015-2016 Europol TE-SAT report, which highlights during 2015, there were 103 terrorist incidents/plots in the UK resulting in 134 terrorist related arrests, with an additional 41 in the Republic of Ireland.[874] Throughout the EU, there were 211 terrorist attacks in 2015 and 1077 arrests made.[875] The figures for the UK in particular do seem to be lower, given that in

[874] Europol (2016) EU Terrorism Situation and Trend report TE-SAT 2016, Hague: Europol, p15

[875] *Ibid*

2014 there were 35 terrorist attacks and 77 arrests made. In 2012 there were 84 terrorist attacks but only 24 arrests. This perhaps highlights the fact that UK law enforcement is becoming more effective all round, and could also illustrate the importance increased powers play in countering the terrorist threat.

The consequences when terrorist acts are not prevented can be severe resulting in serious injury and death. On the 16th April 2013 in the USA bombs exploded at the finish line of the Boston marathon killing three people and injuring over 170. Many of those injured included loss of limbs resulting in permanent disability. In 2013 a British soldier, Lee Rigby, was hacked to death outside Woolwich Barracks, in London. The thesis has shown that the perpetrators were on security intelligence databases, but were not identified as major threats. Regardless of this, these incidents can still occur because terrorist methods have changed and continue to do so. The success in preventing complex plots is largely due to increased international co-operation between states however, the thesis reveals a major concern for intelligence and policing agencies, being the threat lone actors pose to the overall terrorist threat as they can go about undetected due to their low-level planning. This was seen recently on the 14th July 2016 in Nice, France where a lone actor influenced by the Islamist narrative drove a heavy goods vehicle into the crowds watching the firework display on Nice's promenade.

It is low-level attacks that largely justifies why state agencies require powers to conduct bulk surveillance in to aspects of citizens' lives where the need

necessitates it. The above examples show however, that even when citizens' are placed under a targeted surveillance authority, the lack of resources and financial pressures on law enforcement agencies' means that individual suspects must be prioritised and often intelligence is missed, and targets lost. It therefore follows that it would simply be impossible to monitor the entirety of Internet traffic and all UK citizens', all of the time, despite the media's portrayal of law enforcements' arbitrary use of surveillance and detention powers. In the EU, UK and the US the powers are not arbitrary. Powers to conduct surveillance of electronic communications must be applied proportionately and within the rule of law. These assertions, and increased powers of surveillance have resulted in an emphasis on privacy that has in turn resulted in the growth of commercial encryption; particularly in light of the fact lives are being increasingly lived online.[876] Privacy advocates have therefore campaigned for reduced state powers or enhanced safeguards, to protect the individual from what they judge to be a surveillance state.[877] In turn Governments seem to fear the possibility of the emergence of electronic communication channels they cannot monitor, and the possibility of losing intelligence powers. Both sides of the divide see a future in which they lose control, where 'privacy advocates look at a world in whichever more data is produced, aggregated and mined and the authorities fear

[876] See https://globenewswire.com/news-release/2016/10/31/884765/0/en/Encryption-Software-Market-Expected-To-Reach-2-16-Billion-By-2020.html accessed 22 November 2016

[877] See https://www.privacyinternational.org/node/917 accessed 22 November 2016

developments such as universal default encryption, peer-to-peer networks and the dark net'.[878]

The Government has the duty to protect and ensure citizens' absolute Article 2 ECHR right to life. In doing so they intimately interfere with the citizens' qualified Article 8 right to privacy under ECHR, and Article 7 and 8 under the CFR. It is impossible for a citizen to use and access qualified rights if their Article 2 right is not protected. Overall, the thesis evidenced that the balance in the UK between collective security and individual data privacy rights is properly stable because of the role of judicial review, judicial independence, and the scrutiny by commissioners and parliamentary committees.

[878] *Supra* as per D. Anderson Q.C. (2015) p.34

BIBLIOGRAPHY

A Strong Britain in an Age of Uncertainty: The National Security Strategy, HM Government, October 2010, Cm7953

Aas, K.F. (2007) *Globalisation and Crime* (Sage)

Ackerman, B. (2007) Before the Next Attack - Preserving Civil Liberties in an Age of Terrorism, *Public Law* 181-187

Alegre S. and Leaf M. (2004) Mutual Recognition in European Judicial Cooperation: A Step Too Far Too Soon? Case Study—the European Arrest Warrant, European Law Journal, 10:2, 200-217

Alonso, R. *et al* (2008) Radicalisation Process Leading to Acts of Terrorism. A concise Report prepared by the European Commission's Expert Group on Violent Radicalisation

Alston, P. and Weiler, J.H.H. (1999) *An 'Ever Closer Union' in Need of a Human Rights Policy: The European Union and Human Rights*, in Alston, *et al* (editors) *The EU and Human Rights* (Oxford University Press)

Anderson QC, D. (2012) The Terrorism Acts in 2012 London: The Stationary Office

Anderson QC, D. (2013) The Terrorism Acts in 2012 London: The Stationary Office

Anderson QC, D. (2014) The Terrorism Acts in 2013 London: The Stationary Office

Anderson QC, D. Independent Reviewer of Terrorism Legislation (2015) A Question of Trust: Report of the Investigatory Powers Review, June 2015

Anderson, M. (1998) *European Frontiers at the End of the Twentieth Century*, in Anderson, M. and Eberhard, B. *The Frontiers of Europe* (London: Pinter)

Andrews and Arnold Ltd. (2015) Written evidence (DIP0001) submitted to the Joint Committee on the Draft Investigatory Powers Bill, available at https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf accessed 24 November 2016

Argomaniz, J. (2012) *The EU and Counter-Terrorism* (Routledge)

Argomaniz, J., Bures, O. and Kaunert, C. (2015) A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment, *Intelligence and National Security*, 30:2-3, 191-206

Arreguin-Toft, I. (2002) Tunnel at the End of the Light: A Critique of US Counter-terrorist Grand Strategy, *Cambridge Review of International Affairs* 15(3), 549-563

Ashour, O. (2009) *The De-Radicalisation of the Jihadists: Transforming Armed Islamist Movements,* (Routledge)

Baker, C. (1998) *Membership Categorization and Interview Accounts*, in Silverman, D. (editor) *Qualitative Research: Theory, Method and Practice* (Sage)

Baldwin, F. N. & DiPerna, T. A. (2007) The rule of law: an essential component of the financial war against organized crime and terrorism in the Americas, *Journal of Financial Crime*

Ball, J. and Lewis, P. (2011) Twitter and the Riots: How the News Spread, The Guardian, 7 December, available at: http://www.theguardian.com/uk/2011/dec/07/twitter-riots-how-news-spread accessed 23 August 2016

Balzacq, B. et al (2006) Security and the Two-Level Game, CEPS Working Document No234/January 2006

Bamford, B. (2004) The United Kingdom's "War Against Terrorism", *Terrorism & Political Violence* 16(4), 737-756

Bamford, B.W.C. (2005) The Role and effectiveness of intelligence in Northern Ireland, *Intelligence and National Security*, 20:4, 581-607

Barker, J & Foster, S. (2010) The use of fatal force, article 2 of the European Convention and the Jean Charles de Menezes case, *Coventry Law Journal*, 15(2), 39-49

Barnidge, R P. (2008) *Non-State Actors and Terrorism: Applying the Law of State Responsibility and the Due Diligence Principle*, (Cambridge University Press)

Bartlett, J. Miller, C. Crump, J and Middleton, L. (2013) Policing in an Information Age, Centre for Analysis of Social Media, Demos, March, available at

http://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365 23 August 2016

Bartow, A. (2011) Facebook and the Fourth Amendment: Expecting Any Privacy May be Unreasonable, Jotwell (18 April) available at http://cyber.jotwell.com/2011/04/ accessed 30 December 2016

Bassiouni, M Cherif. (1988) *A Policy-oriented Inquiry of 'International Terrorism'* in: Bassiouni, M Cherif ed., *Legal Responses to International Terrorism: U.S. Procedural Aspects*, (London: Martinus Nijhoff Publishers, 1988)

Beck, U. (2002) The Terrorist Threat: World Risk Society Revisited, Theory, Culture and Society, 19:4, 39-55

Beinart, P. (2015) What Does Obama Really Mean by 'Violent Extremism'? The Atlantic, available at: http://www.theatlantic.com/international/archive/2015/02/obama-violent-extremism-radical-islam/385700/ accessed 9 February 2016

Bell, L. (2016) Millions of Apple devices at risk of attack due to a security bug, Wired Cyber Security, 22 July 2016, available at http://www.wired.co.uk/article/apple-security-bug-hackers-steal-your-password accessed 7 December 2016

Bentham, M. (2016) Lone right wing extremists 'kill and harm more people than lone Islamist terrorists', Evening Standard, 21 June 2016, available at http://www.standard.co.uk/news/uk/lone-right-wing-extremists-kill-and-harm-more-people-than-islamist-terrorists-a3276876.html accessed 21 November 2016

Berenskoetter, F. (2012) Mapping the Field of UK EU Policing, *Journal of Common Market Studies*, 50(1), 37-53

Berger, J. M. and Morgan, J. (2015) The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter, 20 March 2015, Centre for Middle East Policy at Brooking, available at http://webcache.googleusercontent.com/search?q=cache:nUpiATbv50wJ:www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf+&cd=1&hl=en&ct=clnk&gl=uk accessed 21 November 2016

Bergeron, J. (2013) Transnational Organised Crime and International Security, *The Rusi Journal*, 158(2), 6-9

Bernal, P. (2015) Supplementary written evidence (IPB0018) submitted to the Joint Committee on the Draft Investigatory Powers Bill, available at

https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf accessed 24 November 2016

Bertrand, N. (2015) ISIS is taking full advantage of the darkest corners of the Internet, Business Insider UK, http://uk.businessinsider.com/isis-is-using-the-dark-web-2015-7?r=US&IR=T accessed 5 December 2016

Bigo, D. *et al* (2013) Open Season for Data Dishing on the Web, CEPS Policy Brief No.293 18th June 2013

Bigo, D. *et al* (2015) The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda, CEPS in *Liberty and Security in Europe*, February 2015, No. 81,

Bockstette, C. (2010) Terrorists Exploit Information Technologies: Use of Strategic Communication Calls for United Response, in *Pre Concordiam, Journal of European Security and Defense Issues*, *Terrorism*, Volume 1, Issue 3

Boer, M D. (2002) Towards an Accountable Regime for an Emerging European Policing Governance, *Policing and Society: An International Journal of Research and Policy*, 12:4, 275-289

Boer, M. D. and Wiegand, I. (2015) From Convergence to Deep Integration: Evaluating the Impact of EU Counter-Terrorism Strategies on Domestic Arenas, *Intelligence and National Security*, 30:2-3, 377-401

Boer, M. D. (2015) Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis, *Intelligence and National Security,* 30:2-3, 402-419

Bogard, W. (2006) *Welcome to the Society of Control*, in Haggerty, K. D. and Ericson, R. V. eds, *The New Politics of Surveillance Visibility* (University of Toronto Press)

Bonino, S. (2012) Policing Strategies against Islamic Terrorism in the UK after 9/11: The Socio-Political Realities for British Muslims, *Journal of Muslim Minority Affairs*, 32:1

Bonner, D. (2006) Responding to crisis: legislating against terrorism, *Law Quarterly Review*, 122, 602-631

Booth, R. Dodd, V. and Parveen, N. (2016) Labour MP Jo Cox dies after being shot and stabbed, The Guardian 16 June, https://www.theguardian.com/uk-

news/2016/jun/16/labour-mp-jo-cox-shot-in-west-yorkshire accessed 24 December 2016

Borum, R. (2011) Radicalisation into Violent Extremism I: A Review of Social Science Theories, *Journal of Strategic Security*, 4:4 7-36

Boyne, R. (2000) Post Panopticism, *Economy and Society*, 29, 285.

Bradley, A. W. (2008) Relations between Executive, Judiciary and Parliament: an evolving saga? *Public Law*, 470-489

Bradley, A. W. and Ewing, K. D. (2011), *Constitutional and Administrative Law*, (15th Edition, Pearson Education Ltd)

Brodeur, J. P. (2007) High and Low Policing in Post-9/11 *Times Policing*, 1(1) 70-79

Brown, C. S. D. (2015) Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology, Vol 9, Issue 1, January-June 2015, available at http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf accessed 21 November 2016

Brown, I. and Korff, D. (2014) Foreign Surveillance: Law and Practice in a Global Digital Environment, *European Human Rights Law Review*, 3:243-251

Bulk Acquisition Draft Code of Practice, Published for consultation alongside the Investigatory Powers Bill, Home Office, Spring 2016, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/505412/Bulk_Acquisition_draft_code_of_practice.PDF accessed 22 December 2016

Bures, O. (2008) Europol's Fledgling Counterterrorism Role, *Terrorism and Political Violence*, 20(4), 498-517

Burke, J. (2007) *Al-Qaeda*, (Penguin Books)

Busuioc, M., Curtin, D. and Groenleer, M. (2011) Agency growth between autonomy and accountability: the European Police Office as a 'living institution', *Journal of European Public Policy*, 18:6, 848-867

Buttarelli, G. (2015) Counter-terrorism, De-Radicalisation and Foreign Fighters', Joint debate during the extraordinary meeting of the LIBE Committee. European Parliament, Brussels, 27 January 2015

Buxton, R. (2010) Terrorism and the European Convention, Case Comment, Criminal Law Review, (7), 533-542

Byman, D. (2015) *Al Qaeda, The Islamic State and the Global Jihadist Movement*, (Oxford University press)

Byrnes, A. (2002) Apocalyptic Visions and the Law: The Legacy of September 11, a professorial address by Byrnes at the ANU Law School for the Faculty's Inaugural and Valedictory Lecture Series, May 30, 2002, available at: https://law.anu.edu.au/CIPL/StaffPapersTalks&Submissions/Byrnes30May02.pdf accessed 12 December 2015

Campbell, D. (2010) The threat of terrorism: David Campbell responds to Clive Walker, *Public Law*, 459-463

Carpenter, J.S., Levitt, M. and Jacobson, M. (2009) Confronting the ideology of Radical Extremism, *Journal of National Security Law & Policy*, Vol. 3 301-327

Carter, D. L. and Carter, J. G. (2009) Intelligence led policing: Conceptual considerations for policy, *Criminal Justice Policy Review*, 20, 310-325

Carter, G. and Carter, D. L. (2012) Law enforcement intelligence: implications for self-radicalized terrorism, *Police Practice and Research*, 13:2, 138-154

Cassese, A. (2008) *International Criminal Law* (2nd Edition, Oxford University Press)

Chacos, B. (2013) Meet Darknet, the hidden, anonymous underbelly of the searchable web, PC World, http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html accessed 21 November 2016

Chadderton, C. (2012) UK secondary schools under surveillance: what are the implications for race? A Critical Race and Butlerian analysis, *Journal for Critical Education Policy Studies*, 76-92

Choi, S. W. and Luo, S. (2013) Economic Sanctions, Poverty, and International Terrorism: An Empirical Analysis, *International Interactions: Empirical and Theoretical Research in International Relations*, 39:2, 217-245

Choudhury, T. and Fenwick, H. (2011) The impact of counter-terrorism measures on Muslim communities, Equality and Human Rights Commission Research report 72, Durham University

Cini, M. (2003) European Union Politics, (Oxford University Press)

Clarke, R. (1991) *Information Technology and Dataveillance*, in Dunlop, C. and Kling, R. (eds), *Computerization and Controversy: Value Conflicts and Social Choices* (Academic Press, Inc. Waltham 1991).

Coates, S. (2015) PM: seven terror attacks in UK stopped in last year, The Times, 16 November 2015, available at http://www.thetimes.co.uk/tto/news/uk/article4615198.ece accessed 20 November 2016

Cockayne, J., Millar, A., Cortright, D. and Romaniuk, P. (2012) Reshaping United Nations Counterterrorism Efforts: Blue-Sky Thinking for Global Counterterroism Cooperation 10 Years After 9/11, Report for the Centre on Global Counterterrorism Cooperation

Coco, A. (2013) The Mark of Cain, *Journal of International Criminal Justice* 11(2) 425

Coleman, R. and McCahill, M. (2011) Surveillance & Crime, (Sage Publications)

College of Policing (2015) Intelligence collection, development and dissemination, available at: https://www.app.college.police.uk/app-content/intelligence-management/intelligence-cycle/ accessed 23 August 2016

Colvin, M. (1998) *Under Surveillance: Covert policing and human rights standards*, (London: Justice)

Comay, M. (1976) Political Terrorism, *Mental Heath and Society*, 3, 249-261

Commission (EC) (2007) Report from the Commission based on Art 11 of the Council Framework decision of 13 June 2002 on combatting terrorism, Brussels, COM (2007) 681 6th November 2007

Commission (EC) (2005) Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC COM (2005) 438 final, Brussels, 21 September 2005.

Commission (EC) (2011) Report from the Commission to the European Parliament and the Council On the implementation since 2007 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, Brussels, 11 April 2011, Com(2011), 175 final, available at

http://ec.europa.eu/justice/criminal/files/eaw_implementation_report_2011_en.pdf

Commission (EC) (2011) Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive 2006/24/EC COM (2011) 225 final, Brussels, 18 April 2011

Commission (EC) (2011) Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, available at http://ec.europa.eu/homeaffairs/news/intro/docs/com_2011_32_en.pdf accessed 23 August 2016

Commission of the European Communities, (2005) Communication from the Commission to the Council and the European Parliament – The Hague Programme: Ten priorities for the next five years, a partnership for renewal, Brussels; EU Commission

Commission of the European Communities, (2005) Communication of the commission to the Council and the European parliament: Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013, http://europa.eu.in/council accessed 23 August 2016

Commission of the European Communities, (2005a) Proposal for a Council Framework Decision on the exchange of information under the principle of availability, Brussels COM (2005) 490 Final 12 December 2005

Commission of the European Communities, (2005b) Proposal for a Framework Decision on exchange of information under the principle of availability, Memorandum MEMO/05/367 Brussels; EU Commission
Commission of the European Communities, (2005c) Communication From The Commission To The Council And The European Parliament, Brussels COM (2005) 124 Final 06 April 2005

Commission of the European Communities, (2005d) Communication from the Commission To The Council and the European Parliament – The Hague Programme: Ten priorities for the next five years, a partnership for renewal, Brussels: EU Commission

Commission of the European Communities, (2005e) Communication for the Commission to the Council and the European Parliament: Developing a strategic concept on tackling organised crime, Brussels EU Commission COM (2005) 232 Final 2 April 2005

CONTEST: The United Kingdom's Strategy for Countering Terrorism, HM Government, March 2013 Cm8583

CONTEST: The United Kingdom's Strategy for Countering Terrorism, HM Government, July 2016 Cm9310

Cook, A. H. and Lounsbery, M. O. (2011) Assessing the Risk Posed by Terrorist Groups: Identifying Motivating Factors and Threats, *Terrorism and Political Violence*, 23:5, 711-729

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

Council Framework Decision on combating terrorism 2002/475/JHA

Council of Europe, (2005) Special investigation techniques in relation to serious crimes including acts of terrorism: Recommendation Rec (2005) 10 and explanatory memorandum, Strasbourg: Council of Europe Publishing

Council of the European Communities (2005) Communication from the Commission to the Council and the European Parliament Brussels COM (2005) 124 6 April 2005

Council of the European Union (2005a) The European Union Counter-terrorism Strategy 14469/4/05 30 November 2005

Counter-Extremism Strategy, HM Government, October 2015, Cm9145

Counter-Terrorism and Security Bill London: The Stationary Office, November 2014, Bill 127

Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, Third Report of Session 2005–06, House of Lords, House of Commons, Joint Committee on Human Rights, HL Paper 75-I, HC 561-I

Countering International Terrorism: The United Kingdom's Strategy, HM Government July 2006, Cm 6888

Crawford, A. (2002) *Crime and Insecurity: The governance of safety in Europe*, (Willan Publishing)

Crish, P. (2016) Junior doctors' strikes will continue as minister plans to impose new contracts, CIPD available at:

http://www.cipd.co.uk/pm/peoplemanagement/b/weblog/archive/2016/02/12/junior-doctors-39-strikes-will-continue-as-minister-plans-to-impose-new-contracts.aspx accessed 13 February 2016

Crone, M and Harrow, M. (2011) Homegrown Terrorism in the West, *Terrorism and Political Violence*, 23:4, 521-536

Curtis, M. (2010) *Secret Affairs: Britain's Collusion with Radical Islam*, (Serpent's Tail)

Dathan, M. (2016) No room for Bojo among EU's foreign ministers! Top diplomats tease Boris and block him from joining photo –shoot as they begin process of excluding Britain from Brussels club, The Mail Online, 2 September 2016, available at http://www.dailymail.co.uk/news/article-3770744/Britain-continue-helping-EU-tackle-migrant-crisis-Brexit-Boris-Johnson-pledges-tours-European-capitals.html accessed 24 November 2016

Deen, T. (2005) U.N. Member States Struggle to Define Terrorism, Inter Press Service, available at http://www.ipsnews.net/2005/07/politics-un-member-states-struggle-to-define-terrorism/ accessed 2 September 2016

Deflam, M. (2006) Europol and the Policing of International terrorism: Counter-Terrorism in a Global Perspective, *Justice Quarterly*, 23(3), 336-35

Deflam, M. (2009) *The Policing of Terrorism: Organizational and Global Perspectives*, (Routledge)

Deleuze, G. (1992) Postscripts on the Societies of Control, October, Winter Ed 59:3, available at https://cidadeinseguranca.files.wordpress.com/2012/02/deleuze_control.pdf accessed 2 December 2016

Delmas-Marty, M. (2007) The paradigm of the war on crime: legitimating inhuman treatment? *Journal of International Criminal Justice*, 5(3), 584-598

Den Boar, M. Hillebrand, C. and Nolke, A. (2008) Legitimacy under Pressure: The European Web of Counterterrorism Networks, *Journal of Common Market Studies*, 46(1), 101-124

Diaz-Paniagua, C. F. (2008) Negotiating Terrorism: The negotiation dynamics of four UN counter-terrorism treaties, 1997-2005 City University of New York

Dixon, D. (1997) *Law in Policing, legal Rules and Police Practices: Legal Regulation and Police Practices*, (Oxford University Press)

Dobinson, I and Johns, F. (2007) Qualitative Legal Research in M. McConville and W. Chong Hui (eds), Research Methods for Law (Edinburgh University Press)

Dodd, V. 'Europe faces highest terror threat since 9/11, MPs told', The Guardian, 13 January 2015, available at: http://www.theguardian.com/uk-news/2015/jan/13/europe-highest-terror-threat-911-europol-fighting-overseas accessed 1 June 2015

Dodd, V. (2011) British Airways worker Rajib Karim convicted of terrorist plot, The Guardian, 28 February 2011, available at: https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim accessed 21 November 2016

Dodd, V. (2011) Police accessed BlackBerry messages to thwart planned riots, The Guardian, 16 August 2011, available at: https://www.theguardian.com/uk/2011/aug/16/police-accessed-blackberry-messages-thwart-riots accessed 10 November 2016

Dodd, V. (2016) Anjem Choudary jailed for five-and-a-half years for urging support for ISIS, The Guardian, 6 September 2016, available at https://www.theguardian.com/uk-news/2016/sep/06/anjem-choudary-jailed-for-five-years-and-six-months-for-urging-support-of-isis accessed 30 December 2016

Dodd, V. and Topping, A. (2010) Roshonara Choudhry jailed for life over MP attack, The Guardian, 3 November 2010, available at: https://www.theguardian.com/uk/2010/nov/03/roshonara-choudhry-jailed-life-attack accessed 30 December 2016

Dominiczak, P., Rayner, G., Swinford, S., McCann, K., Wilkinson, M. and Henderson, B. (2016) Theresa May secures Article 50 victory in the Commons as Parliament passes amended Brexit motion by 448 to 75 - latest reaction and analysis, The Telegraph, 7 December 2016, available at http://www.telegraph.co.uk/news/2016/12/07/brexit-article-50-mps-vote-supreme-court-pmqs-live/ accessed 9 December 2016

Donohue, L.K. (2005) *Terrorism and the counter-terrorist discourse*, in Ramraj, V. V., Hor, M. and Roach, K. eds, *Global Anti-terrorism Law and Policy* (Cambridge University Press)

Donohue, L. K. (2008) *The Cost of Counterterrorism: Power, Politics and Liberty* (Cambridge University Press)

Douglas, R. (2010) Must terrorists act for a cause? The motivational requirement in definitions of terrorism in the United Kingdom, Canada, New Zealand and Australia, *Commonwealth Law Bulletin*, 36(2), 295-312

Draft Enhanced Terrorism Prevention and Investigation Measures Bill London: The Stationary Office, September 2011, Cm 8166

Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism 2004/0813/CNS

Drury, I. (2015) Public schoolboy who quit City to fight ISIS returns home: Briton who spent five months alongside Kurdish forces says he can justify actions if questioned by police, Mail Online, 10 June 2015, available at http://www.dailymail.co.uk/news/article-3119071/ISIS-fighting-city-trader-returns-home-UK.html accessed 5 December 2015

Edwards, L. and Urquhart, L (2015) Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence? *Social Science Research Network*

Eijkman, Q. A. M. & Waggemans, D. (2011) Visual surveillance and the prevention of terrorism: What about the checks and balances? *International Review of Law, Computers & Technology* 25:3, 143-150

Elgot, J (2016) Brexit debate in parliament would give game away to Brussels, says minister, The Guardian, 16 October 2016, available at https://www.theguardian.com/politics/2016/oct/16/brexit-debate-iwould-give-game-away-to-brussels-priti-patel accessed 9 December 2016

Elliott, M. (2004) Parliamentary sovereignty and the new constitutional order: legislative freedom, political reality and convention, *Legal Studies* 22, 340-376

Elliott, M. (2007) The 'war on terror' and the United Kingdom's constitution, *European Journal of Legal Studies*, Issue 1

English, R. (2009) *Terrorism: How to respond*, (Oxford University Press)

Epstein, L. and King, K. (2002) The Rules of Inference, 69 U. Chi. L Rev. 1

Erlenbusch, V. (2013) How (not) to study terrorism, *Critical Review of International Social and Political Philosophy*

Equipment Interference Code of Practice, Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000, January 2016, Home Office, London: TSO, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf accessed 30 December 2016

Equipment Interference Draft Code of Practice, Home Office, Spring 2016, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504238/Equipment_interference_draft_code_of_practice.PDF accessed 30 December 2016

EU Council, (2002) Council Decision of 28th February 2002: setting up Eurojust with a view to reinforcing the fight against serious crime, Official Journal of the European Communities 6 March 2002, L63/1

EU Council, (2003) 2889th Council Meeting – Justice and Home Affairs, Brussels 27-28 February 2003, 6162/03 (Presse 42)

EU Council, (2004) 2579th Council Meeting – Justice and Home Affairs, Luxembourg 20 April 2004, 8694/04 (Presse 123)

EU Council, (2005a) 2642nd Council Meeting – Justice and home Affairs, Brussels 24 February 2005, 6228/05 (Presse 28)

EU Council, (2005b) Council Meeting – Justice and Home Affairs, Brussels 12 December 2005, 12645/05 (Presse 247)

EU Presidency, (2004) Presidency Conclusions, Brusssels 4-5 November 2004, Document 14292/04

European Union Council, (2007) EU Action Plan on Combating Terrorism, Brussels, 9 March 2007

European Union Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

European Union Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Union Directive 97/66/EC of the European Parliament and of the European Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Europol (2012) EU Terrorism Situation and Trend report TE-SAT 2012, Hague: Europol

Europol (2016) EU Terrorism Situation and Trend report TE-SAT 2016, Hague: Europol

Evans, J. (2012) The Olympics and Beyond, MI5 website https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html accessed 30 December 2015

Ewing, K. D. (1999) The Human Rights Act and Parliamentary Democracy, *The Modern Law Review*, Volume 62, 79-99

Ewing, K. D. (2004) The futility of the Human Rights Act, *Public Law*, 829-852

Ewing, K. D. (2005) The futility of the Human Rights Act – A Long Footnote, *Bracton Law Journal*, Volume 37, 41-47

Ewing, K. D. (2010) *Bonfire of the Liberties: New Labour, Human Rights, and the Rule of Law*, (Oxford University Press)

Feldman, D. (2005) Proportionality and Discrimination in Anti-Terrorism Legislation, *The Cambridge Law Journal*, 64:2, 271-273

Feldman, D. (2005) None, One or Several? Perspectives on the UK's Constitution(s), *Cambridge Law Journal*, 64:2, 329-351

Feldman, D. (2006) Human Rights, terrorism and risk: the role of politicians and judges, *Public Law*, 364-384

Feldman, D. (2010) Disclosure of information, torture and the 'special relationship', *Cambridge Law Journal*, 69(3), 430-433

Felsen, D. and Kalaitzidis, A. (2005) *A Historical overview of Transnational Crime*, in Reichel, P. (editor) *Handbook of Transnational Crime and Justice* (Sage)

Fenwick, H. (2008) Proactive counter-terrorist strategies in conflict with human rights International Review of Law, *Computers & Technology*, 22(3) 259-270

Fenwick, H. (2011) Preventative anti-terrorism strategies in the UK and ECHR: control orders, TPIMs and the role of technology, *International Review of Law, Computers and Technology*, 25:3, 129-141

First sitting Committee Debate Session 2015-16, Investigatory Powers Bill, Publications on the Internet, 24 March 2016 available at http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160324/am/160324s01.htm accessed 30 August 2016

Fischer, A., Oswald, M. E. and Seiler, S. (2013) Terrorists Among Us: Effects of a Suspect's Group Membership, Terrorist Past, and Knowledge on Lay Persons' Interrogation Severity Recommendations, *Swiss Journal of Psychology*, 72 (1), 13-23

Foreign Policy Aspects of the War Against Terrorism, Sixth Report of the Foreign Affairs Committee, Session 2004-05, June 2005, Cm6590

Foster, S. (2009) The fight against terrorism, detention without trail and human rights, Coventry Law Journal, 14(1), 4-20

Freedman, D. and Thussu, D. K. (2012) Media & Terrorism Global Perspectives, (Sage Publications)

Freeman, M. (2005) *Order, Rights and Threats: Terrorism and Global Justice*, in Wilson, R. A. (ed) *Human Rights in the War on Terror* (Cambridge University Press)

Freeman, M. (2011) The Sources of Terrorist Financing: Theory and Typology, *Studies in Conflict & Terrorism*, 34:461-475

Friedlander, R. A. (1983) *Terror Violence: Aspects of Social Control*, (Oceana Publications)

Fuch-Drapier, M. (2011) The European Union's Solidarity Clause in the Event of a Terrorist Attack: Towards Solidarity or Maintaining Sovereignty, *Journal of Contingencies and Crisis Management*, 19:4, 184-197

Fulford, A (2008) How have things changed since the IRA trials? *Medicine, Science & the Law*, 48:3, 185-188

Furedi, F. (2007) The only thing we have to fear is the 'culture of fear' itself: How human thought and action are being stifled by a regime of uncertainty, available at http://frankfuredi.com/pdf/fearessay-20070404.pdf

Fussey, P. (2007) Observing Potentiality in the Global City: Surveillance and Counterterrorism in London, *International Criminal Justice Review*, 17:171

Gale, C. J. S. (2006) The UK Response to Terrorism: Human Rights and a Wider Perspective, *Working Paper Series*, No 06/01

Gallagher, R. (2013) Software that Tracks People on Social Media Created by Defence Firm, The Guardian, 10 February, available at http://www.theguardian.com/world/2013/feb/10/software-trackssocial-media-defence accessed 23 August 2016

Ganor, B. (2002) Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? *Police Practice and Research: An International Journal*, 3:4, 287-304

Ganor, B. (2014) *Defining Terrorism: Is One Mans Terrorist Another Mans Freedom Fighter*? In Lowe, D. Turk, A. and Das, D. K. *Examining Political Violence: Studies of Terrorism, Counterterrorism and Internal War*, (CRC Press)

Garland, D. (2001) *The Culture of Control: Crime and social Order in Contemporary Society* (Oxford University Press)

Gartenstein-Ross, D. and Grossman, L. (2009) Homegrown terrorists in the U.S. and U.K. An empirical examination of the radicalisation process, Washington DC: Foundation for Defense of Democracies Press.

Gearty, C. (2005) Terrorism and human rights*, European Human Rights Law Review*, (1), 1-6

Gearty, C. (2007) Rethinking civil liberties in a counter-terrorism world, *European Human Rights Law Review*, (2), 111-119

Gearty, C. (2012) Is attacking multiculturalism a way of tackling racism – or feeding it? Relections on the Governments Prevent Strategy, *European Human Rights Law Review*, (2), 121-129

Geltzer, J. A. (2011) Taking Hand-Outs or Going It Alone: Nationalization versus Privatization in the Funding of Islamist Terrorist Groups, *Studies in Conflict & Terrorism*, 34:144-170

Gillespie, A. (2009) Regulation of Internet Surveillance, *European Human Rights Law Review*, 4, 552.

Gioia, A. (2006) *The UN Conventions on the Prevention and Suppression of International Terrorism*, in Nesi, G. ed., *International Cooperation in Counter-*

terrorism: The United Nations And Regional Organizations in the Fight Against Terrorism, (Ashgate)

Githens-Mazer, J. (2008) Causes of jihadi terrorism: beyond paintballing and social exclusion, *Criminal Justice Matters*, 73(1) 26-28

Goold, B. J. (2009) Surveillance and the Political Value of Privacy, Amsterdam Law Forum

Graham, R. (2016) How Terrorists Use Encryption, Combating Terrorism Centre, available at https://www.ctc.usma.edu/posts/how-terrorists-use-encryption accessed 21 November 2016

Gottlieb, S. (2010) *Debating Terrorism and Counterterrorism: Conflicting Perspectives on Causes, Contexts and Responses*, (Washington DC: CQ Press)

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, (Metropolitan Books: New York)

Greenwald, G. (2016) Why is the Killer of British MP Jo cox not being called a 'Terrorist'? The Intercept, 17 June 2016, available at https://theintercept.com/2016/06/17/why-is-the-killer-of-british-mp-jo-cox-not-being-called-a-terrorist/ accessed 21 November 2016

Greer, S. (2010) Anti-terrorist laws and the United Kingdom's "suspect Muslim community": a reply to Pantazis and Pemberton, *British Journal of Criminology*

Grierson, J. Dodd, V. and Rodrigues, J. (2016) Anjem Choudary convicted of supporting Islamic State, The Guradian, 16 August, available at https://www.theguardian.com/uk-news/2016/aug/16/anjem-choudary-convicted-of-supporting-islamic-state accessed 20 September 2016

Guille, L. (2010) Policing in Europe: An Ethnographic Approach to Understanding the Nature of Cooperation and the Gap between Policy and Practice, *Journal of Contemporary European Research*, 6:2, 257-271. Available at: http://www.jcer.net/ojs/index accessed 10 February 2015

Hacker, F. J. (1980) Terror and Terrorism: Modern growth industry and mass entertainment, *Studies in Conflict and Terrorism*, 4, 143-159.

Haggerty, K. (2006) *Tearing Down the Walls: On Demolishing the Panopticon*, in D. Lyon, *Theorizing Surveillance: The Panopticon and Beyond*, (Cullompton: Willan)

Haider, M. (2013) European Parliament identifies Wahabi and Salafi roots of global terrorism, available at http://www.dawn.com/news/1029713 accessed 8 February 2016

Hayes, B. (2002) The activities and development of Europol: towards an unaccountable FBI in Europe, London: Statewatch, available at: http://www.statewatch.org/news/2002/feb/eufbi.pdf accessed 20 January 2015

Head, M. (2010) Calling out the troops and the Civil Contingencies Act: some questions of concern, *Public Law*, 340-361

Henderson, B. and Sabur, R. (2016) Nice terrorist attack on Bastille Day: everything we know so far on Monday, The Telegraph, 18 July 2016, http://www.telegraph.co.uk/news/2016/07/15/nice-terror-attack-on-bastille-day-everything-we-know-so-far-on/ accessed 30 December 2016

Henne, P. S. (2012) The Ancient Fire: Religion and Suicide Terrorism, *Terrorism and Political Violence*, 24:1, 38-60

Hewitt, S. (2008) *The British War on Terror*, (London: Continuum Books)

Hijmans, H. and Scirocco, A. (2009) Shortcomings in EU Data Protection in the Third and The Second Pillars, 46 *Common Market Law Review* 1485

Hillyard, P. (1993) *Suspect Community: People's Experience of the Prevention of Terrorism Act in Britain* (Pluto Press)

HM Government, (2016) CONTEST: The United Kingdom's Strategy for Countering Terrorism London: The Stationary Office, Cm9310

Hoffman, B. (2006) *Inside Terrorism*, (2nd Edition, Columbia University Press)

Home Affairs Select Committee, A Surveillance Society? Fifth Report of Session 2007-2008 (HC 2008-2009 58-I)

Home Office, User guide to operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes and stops and searches, Great Britain, 6 March 2014

Hopkins, N. (2013) UK gathering secret intelligence via covert NSA operation, The Guardian 7th June 2013, http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism accessed 30 December 2016

Hopkins, N. and Ackermenn, S. (2013) Flexible laws and weak oversight give GCHQ room for manoeuvre, The Guardian 2nd August 2013, http://www.theguardian.com/uk-news/2013/aug/02/gchq-laws-oversight-nsa accessed 20 December 2016

Hopkins, N. and Borger, J. (2013) Exclusive: NSA pays £100m in secret funding for GCHQ, The Guardian 1st August 2013, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden accessed 30 December 2016

Hopkins, N. Borger, J. and Harding, L. (2013) GCHQ: inside the top secret world of Britain's biggest spy agency The Guardian, 2nd August 2013 http://www.theguardian.com/world/interactive/2013/aug/01/gchq-spy-agency-nsa-edward-snowden accessed 30 December 2016

Horgan, J. (2009) *Walking Away From Terrorism*, (Routledge)

Horne, A. & Walker, C. (2014) Lessons learned from political constitutionalism? Comparing the enactment of control orders and terrorism prevention and investigation measures by the UK Parliament, *Public Law,* 267-288

Hua, J. and Bapna, S. (2012) How Can We Deter Cyber Terrorism? *Information Security Journal: Global Perspective,* 21:2, 102-114

Hutson, R. Long. T. and Page. M. (2009) Pathways to Violent Radicalisation in the Middle East: A model for future studies of transnational jihad, *Rusi Journal* April 2009, 154(2) 18-26

Huq, A. Z., Tyler, T. R. and Schulhofer, S. J. (2011) Why Does The Public Cooperate With Law Enforcement? The Influence of The Purposes and Targets of Policing, *Psychology, Public Policy and Law*, 17:3, 419-450

Imran, A. (2011) Slaying the Monster: Sentencing, *Criminal Law and Justice Weekly* 175 JPN 151

Ingram, H. J. (2015) The strategic logic of Islamic state information operations, *Australian Journal of International Affairs* 69(6) 729-752, 732

Ingram, H. J. (2015) Three Traits of the Islamic State's Information Warfare, *The Rusi Journal* 159(6) 4-11

Ingram, H. (2016) Militant Islamist propaganda targeting Muslims in the West: comparing Inspire and Dabiq narratives, Terrorist Use of the Internet: Assessment and Response, Dublin City University, Ireland.

Innes, M .and Thiel, D. (2008) *Policing Terror*, in Newburn, T. (editor) *Handbook of Policing* (2nd edition, Willan)

Intelligence and Security Committee Annual Report 2011-2012, HM Government July 2012 Cm8403

Intelligence and Security Committee, Privacy and security: a modern and transparent legal framework, HC 1075 2014/15, 12 March 2015

Intercept as Evidence, The Office for Security and Counter-Terrorism, (Cm 8989, December 2014), A report by a Committee of Privy Counsellors led by the Rt. Hon. Sir John Chilcott

Jackson, R. (2008) An Argument for Terrorism, *Perspectives on Terrorism*, Vol. 2, No. 2, 1-12

Jackson, R., Jarvis, L., Gunning, J. and Smyth, M. B. (2011) *Terrorism: A Critical Introduction*, (Palgrave Macmillan)

Jackson, R. and Sinclair, S. J. (2012) *Contemporary Debates on Terrorism* (Routledge)

Jenni, S. (2016) Is the Swiss model a Brexit solution? The UK in a Changing Europe, 23 March 2016, available at http://ukandeu.ac.uk/is-the-swiss-model-a-brexit-solution/ accessed 30 December 2016

Joffe, G. (2008) The European Union, Democracy and Counter-Terrorism in the Maghreb, *Journal of Common Market Studies*, 46(1), 147-171

Joint Committee on Human Rights, Prevention of Terrorism Bill (2004-05) (2005), HL 68

Joint Committee on the Draft Investigatory Powers Bill (2016) Report of Session 2015-2016, 11 February, HL Paper 93 and HC 651

Joint debate during the extraordinary meeting of the LIBE Committee (European Parliament, Brussels, 27 January 2015)

Jones QC, A. Bowers, R. and Lodge, H. D. (2006*) Blackstone's Guide to The Terrorism Act 2006*, (Oxford University Press)

Jones, R. (2000) Digital Rule: Punishment, Control and Technology, *Punishment and Society* 2:5

Jones, S. G. (2014) A Persistent Threat: The Evolution of al-Qaida and Other Salafi Jihadists, RAND National Defense Research Institute.

Juergensmeyer, M. (2000) Terror in the Mind of God: The Global Rise of Religious Violence, University of California Press.

Kaczorowska, A. (2013) European Union Law (3rd Edition, Routledge)

Katselli, E. (2012) International peace ans security, human rights and the courts: a critical re-appraisal, *The International Journal of Human Rights*, 16:2, 257-277

Katz, R. (2015) How Islamic State is still Thriving on Twitter, 11 April 2015, InSite Blog on Terrorism & Extremism, available at http://news.siteintelgroup.com/blog/index.php/entry/377-how-the-islamic-state-is-still-thriving-on-twitter accessed 19 November 2016

Kaunert, C. (2007) Without the Power of Purse or Sword: The European Arrest Warrant and the Role of the Commission, Journal of European Integration, 29:4, 387-404

Kaunert, C. (2009) Liberty versus Security? EU Asylum Policy and the European Commission, *Journal of Contemporary European Research*, 5(2), 148-170

Kaunert, C. (2010) Europol and EU Counterterrorism: International Security Actorness in the External Dimension, *Studies in Conflict & Terrorism*, 33(7), 652-671

Kearney, J. (2016) The Security Implications of Brexit, Compas Breakfast Breifing Summary, available at http://www.compas.ox.ac.uk/media/160520-security-web-text.pdf accessed 24 November 2016

Keohane, D. (2008) The Absent Friend: EU Foreign Policy and Counter-Terrorism, *Journal of Common Market Studies*, 46(1), 125-146

Kepel, G. (2002) *Jihad: The Trail of Political Islam*, (Harvard University Press)

Kerr, I. and Earle, J. (2013) Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy, *Stanford Law Review Online*, available at https://www.stanfordlawreview.org/online/privacy-and-big-data-prediction-preemption-presumption/

Khan, A. (2014) What ISIL's English-language propaganda tells us about its goals, Aljazeera 20 June 2014, available at http://america.aljazeera.com/watch/shows/america-

tonight/articles/2014/6/19/how-isil-is-remakingitsbrandontheinternet.html accessed 20 November 2016

Khomami, N. (2015) Mohammad Emwazi: who were his victims? The Guardian, 13 November 2015, available at http://www.theguardian.com/uk-news/2015/nov/13/mohammed-emwazi-who-were-his-victims accessed 20 November 2016

Kirby, A. (2007) London Bombers as Self-Starters: A Case Study in Indigenous Radicalisation and the Emergence of Autonomous Cliques, *Studies in Conflict and Terrorism*, 30 (Winter 2007) 415-428

Klausen, J. (2009) British Counter-Terrorism After 7/7: Adapting Community Policing to the Fight Against Domestic Terrorism, *Journal of Ethnic and Migration Studies*, Vol. 35, No. 3, March, 403-420.

Klausen, J. (2015) Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq, *Studies in Conflict & Terrorism* 39(1), 1-22

Knight, C. J. S. (2011) Striking down legislation under bi-polar sovereignty, *Public Law*

Koops, B. J. (2013) Police Investigations in Internet Open Sources: Procedural Law Issues, *Computer Law and Security Review*, 29:654

Koops, B. J., Hoepman, J. and Leenes, R. (2013) Open source intelligence and privacy by design, *Computer Law and Security Review*, 29:676

LaFree, G and Dugan, L. (2007) Introducing the Global Terrorism Database, *Terrorism and Political Violence*, 19:2, 181-204

Lambert, D. (2010) Intelligence-Led Policing in a Fusion Center, FBI Law Enforcement Bulletin

Laqueur, W. (1987) *The Age of Terrorism* (Boston: Little, Brown and Company)

Laqueur, W. (1999) *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford University Press)

Lawther, C. (2010) "Securing" the past: policing and the contest over truth in Northern Ireland, *British Journal of Criminology*

Legislation Against Terrorism, A consultation paper (1998) The Stationary Office Cm 4178

Legislative Scrutiny: Counter-Terrorism and Security Bill, Fifth Report of Session 2014-15, House of Lords, House of Commons, Joint Committee on Human Rights, 12 January 2015, HL 86, HC 859

Leigh, I. (1986) A Tappers Charter? *Public Law*, 8-18

Leiken, R. S. (2005) Europe's Mujahideen: Where Mass Immigration Meets Global Terrorism April 2005, Centre for Immigration Studies

Leonard, S. and Kaunert, C. (2012) "Between a rock and a hard place?": The European Union's financial sanctions against suspected terrorists, multilateralism and human rights, *Cooperation and Conflict*, 47:473)

Lester, A. (2005) The utility of the Human Rights Act: a reply to Keith Ewing, Public Law, 249-258

Levi, M. (2010) Combating the financing of terrorism: a history and assessment of the control of "threat finance", *British Journal of Criminology*

Lewis, N., (2005) *Expanding surveillance: connecting biometric information systems to international police cooperation*, in Zureil E. and Salter, M.B. (editors) *Global Surveillance and Policing: Borders, security, identity*, (Willan)

Lewis, P. et al (2012) Reading the Riots: Investigating England's Summer of Disorder (Guardianshorts, London School of Economics and The Guardian, London 2012) available at: https://www.theguardian.com/info/2011/dec/15/reading-the-riots-ebook accessed 30 January 2016

Lewitt, G. (1986) Is Terrorism Worth Defining? *Ohio Northern University Law Review* 97

LexisNexis® Risk Solutions (2012) Survey of Law Enforcement Personnel and Their Use of Social Media in Investigations. www.lexisnexis.com/investigations available at https://www.lexisnexis.com/risk/downloads/whitepaper/Infographic-Social-Media-Use-in-Law-Enforcement.pdf accessed 10 November 2016

Loader, I. (2002) Policing, securitization and democratization in Europe Criminal Justice, *The International Journal of Policy and Practice*, Vol 2(2), 125-153

Lord Bingham (2007) The Rule of Law, *Cambridge Law Journal*, 66(1), 67-85

Lord Carlile of Berriew Q.C. (2007) Independent Reviewer of Terrorism Legislation, The Definition of Terrorism, March 2007, Cm7052

Lord Carlile of Berriew Q.C. (2007) Report on Proposed Measures for Inclusion in a Counter Terrorism Bill, Cm7262

Lowe, D. (2011) The lack of discretion in high policing, *Policing and Society: An International Journal of Research and Policy*, 21:2, 233-247

Lowe, D. (2013) *Radicalisation of Terrorist Causes: the 32CSM/IRA Threat to UK Security*, in Lowe, D., Turk, A. and Das, D. (editors) *Political Violence, Terrorism and Counter-Terrorism* (New York: Taylor & Francis)

Lowe, D. (2014) Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty, *Terrorism and Political Violence*, 13 August 2014

Lynch, O. and Ryder, C. (2012) Deadliness, organisational change and suicide attacks: understanding the assumptions inherent in the use of the term 'new terrorism', *Critical Studies on Terrorism*, 5:2, 257-275

Lynskey, O. (2015) Beyond privacy: the data protection implications of the IP Bill, LSE Law Department Briefings on the Investigatory Powers Bill, LSE Law Policy Briefings, 15, *Social Science Research Network*

MacAskell, E. Borger, J. Davies, N. and Ball, J. (2013) GCHQ taps fibre-optic cables for secret access to world's communications The Guardian 21st June 2013 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa accessed 30 December 2016

Macdonald, A. (2015) EU's Tusk warns against federalist push, treaty change, 7 September 2015, Reuters, available at http://www.reuters.com/article/us-eu-tusk-treaties-idUSKCN0R72C320150907 accessed 20 December 2016

Mahan, S. and Grist, P. L. (2013) *Terrorism in Perspective*, (3rd Edition, Sage)

Mandoza, I. (2012) What's in a name: Challenging the word "Islamist", The Chicago Monitor, critical perspectives on mainstream media, available at http://chicagomonitor.com/2012/05/whats-in-a-name-challenging-the-word-islamist/ accessed 9 February 2016

Mansfield, K. (2016) 'It is crazy' that EU members would want to act 'individually' says federalist Juncker, Express, 15 September 2016, available at http://www.express.co.uk/news/politics/711181/Jean-Claude-Juncker-says-crazy-EU-members-would-want-to-act-individually accessed 24 November 2016

Marong, C. (2012) Protecting the public? Challenging the indefinite preventive detention of non-citizens, UCL Journal of Law and Jurisprudence, 3(1), 115-143

Martin, G. (2004) *The New Era of Terrorism: Selected Readings*, (Sage)

Martin, G. (2011) *Essentials of Terrorism: Concepts and Controversies*. (2nd edition, Sage)

Martin, M. (2013) *Understanding Terrorism: Challenges, Perspectives, and Issues* (4th edition, Sage)

Martin, A. J. (2105) GCHQ v Privacy International: Computer hacking tribunal showdown begins, The Register, 1 December 2015, available at http://www.theregister.co.uk/2015/12/01/gchq_privacy_international_investigatory_powers_tribunal/ accessed 13 May 2016

Martyn, A. (2002) The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September Australian Law and Bills Digest Group, Parliament of Australia Web Site

Matlary, J. H. (2008) Much ado about little: the EU and human security, *International Affairs*, 84:1, 131-143

Matusitz, J. (2013) *Terrorism & Communication: A Critical Introduction*, (Sage)

McCann, K. (2016) UK opts back into Europol despite Brexit vote, The Telegraph, 14 November 2016, available at http://www.telegraph.co.uk/news/2016/11/14/uk-opts-back-into-europol-despite-brexit-vote/ accessed 24 November 2016

McCulloch, J. and Pickering, S. (2009) Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror", *British Journal of Criminology*, 49, 628-645

McKeever, D. (2010) The Human Rights Act and anti-terrorism in the UK: one great leap forward by Parliament, but are the courts able to slow the steady retreat that has followed? *Public Law*, 110-139

McKittrick, D and McVea, D. (2001) *Making Sense of the Troubles*, (Penguin Books)

Meisels, T. (2009) Defining terrorism – a typology, *Critical Review of International Social and Political Philosophy*, 12:3, 331-351

Middleton, B. (2013) Terrorism prevention and investigation measures: constitutional evolution, not revolution? *Journal of Criminal Law*, 77(6), 562-582

Miller, C. and Ginnis, S. et al (2015) The road to representivity (Centre for the Analysis of Social Media at Demos/IPSOS Mori, September 2015) at http://www.demos.co.uk/project/the-road-to-representivity/ accessed 12 July 2015

Milton, D. (2014) The Islamic State: An Adaptive Organisation Facing Increasing Challenges, in al-Ubaydi, Lahoud, Milton and Price (editors), The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State, December 2014, The Combatting Terrorism Centre at West Point, available at www.ctc.usma.edu accessed 20 November 2016

Mitsilegas, V. (2003) The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data, *European Foreign Affairs Review*, 8, 515-536

Mitsilegas, V. (2010) The Transformation of Border Controls in an Era of Security: UK and EU Systems Converging? 24 *Journal of Immigration Asylum and Nationality Law*, 233

Mitsilegas, V. (2015) *The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law* (London: Springer)

Moeckli, D. and King, T. (2010) Human Rights and Non-discrimination on the "War on Terror", Publication Review, *European Journal of International Law* 1109-1111

Molders, S. (2005) European Arrest Warrant Act is Void – The Decision of the German Federal Constitutional Court of 18 July 2005, German Law Journal, 7:1, 45-58

Monar, J. (2013) EU internal security governance: the case of counter-terrorism, *European Security*, 23:2, 195-209

Monar, J. (2015) The EU as an International Counter-Terrorism Actor: Progress and Constraints, *Intelligence and National Security*, 30:2-3, 333-356

Moran, J. (2010) Evaluating Special Branch and the Use of Informant Intelligence in Northern Ireland, *Intelligence and National Security*, 25:1, 1-23

Mosendz, P. (2014) How the head of ISIS got his name: Abu Bakr al-Baghdadi chose a name with historic resonance in the Muslim world, Europe Newsweek, http://europe.newsweek.com/abu-bakr-al-baghdadi-abu-dua-invisible-sheikh-awwad-ibrahim-ali-al-badri-al-282939?rm=eu accessed 27 October 2016

Moskalenko, S and McCauley, C. (2011) The psychology of lone-wolf terrorism, *Counselling Psychology Quarterly*, 24:2, 115-126

Muller-Wille, B. (2008) The Effect of International Terrorism on EU Intelligence Co-operation, *Journal of Common Market Studies*, 46(1), 49-73

Murphy, C. C. (2015) *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law*, (Hart Publishing)

Murray, A. and Keenan, B. (2015) Ensuring the Rule of Law, LSE Law Department Briefings on the Investigatory Powers Bill, LSE Law Policy Briefing Series, 12, *Social Science Research Network*

Mustapha, H. (2014) The al-Nusra Front: From Formation to Dissension, Policy Analysis Series, *Arab Centre for Research and Policy Studies*

Mythen, G. and Walklate, S. (2006) Criminology and Terrorism: Which Thesis Risk Society or Governmentality? *British Journal of Criminology*, 46(3) 379-398

Nagesh, A (2016) France is probably going to move our border back to Dover after Brexit, The Metro, 25 June 2016, available at http://metro.co.uk/2016/06/25/france-is-probably-going-to-move-our-border-back-to-dover-after-brexit-5966133/ accessed 28 December 2016

Nance, M. W. (2015) *The Terrorists of Iraq: Inside the Strategy and Tactics of the Iraqi Insurgency 2003-2014*, (CRC Press)

Napoleoni, L. (2004) The New Economy of Terror: How Terrorism is Financed, *Forum on Crime and Society*, 4:1, 4:2, 31-48

Netanyahu, B. (1985) *Terrorism: How the West Can Win*, (Farrar, Strauss and Giroux, New York)

Neuburger, L. D. C., and Valentini, T. (1996) *Women and Terrorism*, (Macmillan Press)

Neumann, P. R. opinion cited in Sedgwick, M. (2010) The Concept of Radicalisation as a Source of Confusion, *Terrorism and Political Violence*, 22:4

Newburn, T. Williamson, T. and Wright, A. (2008) *Handbook of Criminal Investigation* (2nd edition, Willan)

O'Carroll, L. and Norton-Taylor, R. (2013) David Miranda detention prompts outcry over 'gross misuse' of terror laws, The Guardian, 19 August 2013 http://www.theguardian.com/world/2013/aug/19/david-miranda-detention-outcry-terrorism-laws accessed 15 December 2016

O'Floinn, M. and Ormerod, D. (2011) Social networking sites, RIPA and Criminal Investigations, *Criminal Law Review*, 10:766

O'Neill, M. (2007) A Critical Analysis of the EU Legal Provisions of Terrorism, *Terrorism and Political Violence*, 20:1, 26-48

OFCOM, The Communications Market (2016), Telecoms and networks, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0026/26648/uk_telecoms.pdf accessed 21 November 2016

Ojanen, T. (2014) Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, *European Constitutional Law Review*, 10:3, 528-541

Oltermann, P. (2013) Britain accused of trying to impede EU data protection law, The Guardian, 27 September 2013 http://www.theguardian.com/technology/2013/sep/27/britain-eu-data-protection-law accessed 24 November 2016

Omand, D. (2012) #Intelligence, Centre for Analysis of Social Media, Demos, 24 April, available at http://www.demos.co.uk/project/intelligence/ accessed 22 August 2016

Omand, D. Bartlett, J. and Miller, C. (2012) Introducing Social Media Intelligence, *Intelligence and National Security Review*, 27:1

Omand, D. Bartlett, J. and Miller, C. (for UK Cabinet Office) (2010) A Strong Britain in an Age of Uncertainty: The National Security Strategy (HMSO 2010)

O'Neill, M. (2007) A Critical Analysis of the EU Legal Provisions on Terrorism, *Terrorism and Political Violence*, 20:1, 26-48

Ormerod, D. (2008) *Smith and Hogan Criminal Law* (12th Edition, Oxford University Press)

Orr, A. (2012) Terrorism: A Philosophical Discourse, *Journal of Applied Security Research*, 7:1, 93-106

Paganini, P. (2012) The good and the bad of the Deep Web, The Hacker New Magazine, 17 September 2012, available at http://securityaffairs.co/wordpress/8719/deep-web/the-good-and-the-bad-of-the-deep-web.html accessed 21 November 2016

Pantazis, C and Pemberton, S. (2009) From the "old" to the "new" suspect community: examining the impacts of recent UK counter-terrorist legislation, *British Journal of Criminology*, 49(5), 646-666

Pantucci, R. (2010) A contest to democracy? How the UK has responded to the current terrorist threat, *Democratization* 17(2), 251-271

Pape, R. A. (2003) The Strategic Logic of Suicide Terrorism, *American Political Science Review*, 97:3 343-361

Parmer, A. (2011) Stop and Search in London: Counter-Terrorist or Counter-Productive? *Policing & Society* 21, no.4: 369–382

Patrice, J. (2016) Bombs used by ISIS in Brussels terror attacks are for sale online, NewsGrio, http://www.newsgrio.com/articles/world/uk/244032-bombs-used-by-isis-in-brussels-terror-attacks-are-for-sale-online.html accessed 5 December 2016

Peers, S. (2011) EU Justice and Home Affairs Law (3rd edition) Oxford: Oxford University Press

Perliger, A. (2012) How Democracies Respond to Terrorism: Regime Characteristics, Symbolic Power and Counterterrorism, *Security Studies*, 21:3, 490-528

Perry, M and Negrin H. (2008) *The Theory and Practice of Islamic Terrorism: An Anthology*, (Palgrave Macmillan)

Piazza, J. (2013) Regime Age and Terrorism: Are New Democracies Prone to Terrorism? *International Interactions: Empirical and Theoretical Research in International Relations*, 39:2, 246-263

Pollard, S. (2016) The case that shows why we must not stay in the European Arrest Warrant, The Spectator, 3 September 2016, available at http://www.spectator.co.uk/2016/09/the-case-that-shows-why-we-must-not-stay-in-the-european-arrest-warrant/ accessed 9 December 2016

Pollinger, Z. A. (2008) Counterfeit Goods and Their Potential Financing of International Terrorism, *The Michigan Journal of Business*, 85-102

Popham, P. (2014) Jean-Claude Juncker: The face of federalism, Independent, 6 June 2014, available at http://www.independent.co.uk/news/people/jean-claude-juncker-the-face-of-federalism-9504014.html accessed 24 November 2016

Prevent duty guidance: a consultation, HM Government, December 2014

Rankin, J. (2016) Europol chief says Brexit would harm UK crime-fighting, The Guardian, 22 June 2016, available at https://www.theguardian.com/politics/2016/jun/22/europol-chief-says-brexit-would-harm-uk-crime-fighting accessed 24 November 2016

Raplin, A-J. (2011) What is terrorism? *Behavioural Sciences of Terrorism and Political Aggression*, 3:3, 161-175

Rashid, A. (2010) *Taliban: The Power of Militant Islam in Afghanistan and Beyond*, (I. B. Tauris & Co Ltd)

Ratcliffe, J. (2008) *Intelligence-Led Policing*, (Willan)

Ratcliffe, J., Taniguchi, T. and Taylor, R. B. (2009) The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach, *Justice Quarterly*, 26:4

Ratcliffe, M. Rabenstein, C. and Staniforth, A. (2013) *Blackstone's Counter-Terrorism Handbook: Police National Legal Database* (3rd edition, Oxford University Press)

Rees, W. (2006) *Transatlantic Counter-Terrorism Cooperation: The New Imperative*, (Routledge)

Reid, A. S. and Ryder, N. (2010) For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000, *Information and Communications Technology Law*, 10:2, 179-201

Reiner, R. (2010) *The Politics of the Police* (4th edition, Oxford University Press)

Report on the Anti-Terrorism, Crime and Security Bill 2001 (2001-02 HC 351)

Reports on the Anti-Terrorism, Crime and Security Bill (2001-02 HL 37, HC 372)

Reports on the Anti-Terrorism, Crime and Security Bill (2001-02 HL 51, HC 420)

Report of the High Level Panel on Threats, Challenges and Change "A more secure world: Our shared responsibility" (2004), United Nations

Research and Evaluation on Radicalisation to Violent Extremism in the United States, US Department of Justice 2013, OMB: 1121-0329

Review of Counter-Terrorism and Security Powers, Review findings and Recommendations, January 2011, HM Government, Cm8004

Richards, A (2014) Conceptualizing Terrorism, *Studies in Conflict & Terrorism*, 37:3, 213-236

Richards, J (2016) *Needles in Haystacks: Law, Capability, Ethics, and Proportionality in Big Data Intelligence-Gathering*, in Bunnik, A., Cawley, A., Mulqueen, M., and Zwitter, A. *Big Data Challenges* (Palgrave Macmillan)

Rifkin, J. (2004) *The European Dream: How Europe's vision of the future is quietly eclipsing the American Dream*, (Cambridge: Polity Press)

Roberts, A. (2015) Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications, *The Modern Law Review*, 78(3) 522-548

Robins, R. S. and Post, J. M. (1997) *Political Paranoia: The Psychopolitics of Hatred* (New Haven, Yale University Press)

Rosendorff, P. and Sandler, T. (2010) Suicide Terrorism and The Backlash Effect, *Defence and Peace Economics*, 21:5-6, 443-457

Rudner, M. (2006) Using Financial Intelligence Against the Funding of Terrorism, *International Journal of Intelligence and CounterIntelligence*, 19:1, 32-58

Rudner, M. (2010) Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering, *Studies in Conflict & Terrorism*, 33:700-715)

Rusbridger, A. (2013) David Miranda, schedule 7 and the danger that all reporters now face The Guardian 19th August 2013 http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters accessed 21 November 2016

Ryder, N. (2007) A false sense of security? An analysis of legislative approaches towards the prevention of terrorist finance in the United States and the United Kingdom, *Journal of Business Law*, November 821-850

Sageman, M. (2008) *Leaderless Jihad: Terror networks in the Twenty-First Century*, (University of Philadelphia Press)

Saner, E. (2015) Brits abroad: is it against the law to fight ISIS? The Guardian, 25 February 2015, available at https://www.theguardian.com/world/shortcuts/2015/feb/25/brits-abroad-against-law-fight-isis accessed 5 December 2016

Sanchez-Cuenca, J. (2007) The Dynamics of National Terrorism: ETA and the IRA, *Terrorism and Political Violence*, 19:3, 289-306

Santora, M. Rashbaum, W. K. Baker, A. and Goldman, A. (2016) Ahmad Khan Rahami Is Arrested in Manhattan and New Jersey Bombings, The New York Times, 19 September 2016, available at http://www.nytimes.com/2016/09/20/nyregion/nyc-nj-explosions-ahmad-khan-rahami.html?_r=0 accessed 20 November 2016

Santora, M. and Goldman, A. (2016) Ahmad Khan Rahami Was Inspired by Bin Laden, Charges Say, The New York Times, 21 September 2016, available at http://www.nytimes.com/2016/09/21/nyregion/ahmad-khan-rahami-suspect.html accessed 20 November 2016

Sarma, K. (2005) Informers and the Battle Against Republican Terrorism: A Review of 30 Years of Conflict, *Police Practice and Research: An International Journal*, 6:2, 165-180)

Satana, N. S., Inman, M. and Birnir, J. K. (2013) Religion, Government Coalitions, and Terrorism, *Terrorism and Political Violence*, 25:1, 29-52

Saul, B. (2008) Defining 'Terrorism' to Protect Human Rights Sydney Law School, Legal Studies Research Paper No. 08-125

Saul, B. (2010) *Defining Terrorism in International Law*, (Oxford University Press)

Schmid, A. P. and Jongman, A. J. (1988) *Political Terrorism: A New Guide To Actors, Authors, Concepts, Data Bases, Theories, And Literature*, (Transaction Publishers)

Schmid, A. P. (2004) Frameworks for Conceptualising Terrorism, *Terrorism and Political Violence*, 16:2, 197-221

Schmid, A. P. (2011) *The Definition of Terrorism: The Routledge Handbook of Terrorism Research*, (Routledge)

Schmid, A. P. (2013) Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review, International Centre for Counter-Terrorism-The Hague (ICCT)

Schulhofer, S. J., Tyler T. R. and Huq A. Z. (2011) American Policing at a Crossroads: Unsustainable Policies and the Procedural Justice Alternative, *Journal of Criminal Law & Criminology*, Vol. 101, No. 2, 335-374

Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, HM Government, October 2010 Cm7948

Seib, P. (2012) Public Diplomacy versus terrorism, in Freedman, D. and Kishan Thussu, D. (editors) *Media & Terrorism* 14(3), 63-76

Semitsu, J. (2011) From Facebook to Mug Shot: How the Death of Social Networking Privacy Rights Revolutionized Online Government Surveillance, *Pace Law Review*, 31:1, 291-381

Sharma, S. and MacDonald, A. (2016) British volunteers in Syrian Kurd forces are 'terrorists', Turkey says. Middle East Eye, 1 September 2016, available at http://www.middleeasteye.net/news/turkey-british-ypg-terrorist-syria-874419624 accessed 5 December 2016

Sheptycki, J. (2007) High Policing in the Security Control Society, *Policing* 1(1), 25-37

Silber, M. D. and Bhatt, A. (2007) Radicalisation in the West: The homegrown threat, New York: Police Department, Intelligence Division

Silke, A. (2008) Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalisation, *European Journal of Criminology*, 5(1), 99-123

Simmons, H. C. and Mitch, J. R. (2001) Labelling Public Aggression: When Is It Terrorism? *The Journal of Social Psychology*, 125:2, 245-251

Smith, R. (1998) Criminal exploitation of new technologies, Australian Institute of Criminology, *Trends & Issues in Crime and Criminal Justice* No. 93,1

Sorell, T. (2011) Preventive Policing, Surveillance, and European Counter-Terrorism, *Criminal Justice Ethics*, 30:1, 1-22

Sottiaux, S.(2008) *Terrorism and the Limitation of Rights: The ECHR and the US Constitution* (Hart Publishing)

Sparago, M. (2007) Terrorist Recruitment: The Crucial Case of Al Qaeda's Global Jihad Terror Network, *Centre for Global Affairs, New York University*, Sping 2007,

Sparrow, A. Gabbat, A. and Quinn, B. (2013) Reactions to the detention of David Miranda at Heathrow Airport – as it happened, The Guardian, 20 August 2013 http://www.theguardian.com/politics/blog/2013/aug/19/glenn-greenwald-partner-detained-live-reaction accessed 10 December 2016

Spigelman, J. (2010) The forgotten freedom: freedom from fear, *International & Comparative Law Quarterly*, 543-570

Stone, J. (2016) ISIS Terrorists Used Disposable Burner Phones, Activated Just Hours Before, To Carry Out Paris Attacks, International Business Times, 21 March 2016, available http://www.ibtimes.com/isis-terrorists-used-disposable-burner-phones-activated-just-hours-carry-out-paris-2340265 accessed 5 December 2015

Syrett, K. (2011) *The Foundations of Public Law, Principles and Problems of Power in the British Constitution* (Palgrave Macmillan)

Taheri, A. (1987) *Holy Terror: The Inside Story of Islamic Terrorism*, (Sphere Books Ltd)

Taylor, R. W., Caeti, T. J. D., Loper, K., Fritsch, E. J., and Liederbach, J. (2006) *Digital Crime and Digital Terrorism*. (Pearson Education)

Taylor, J. (2010) Police smash Romanian 'child trafficking ring', The Independent, 12 October 2010, available at http://www.independent.co.uk/news/uk/crime/police-smash-romanian-child-trafficking-ring-2104694.html accessed 5 December 2016

The Data Retention (EC Directive) Regulations SI 2009/859

The Definition of Terrorism, A Report by Lord Carlile of Berriew Q.C. Independent Reviewer of Terrorism Legislation, Cm7052, March 2007

The European Parliament, (2005) The Hague Programme – Ten priorities for the next five years – a partnership for European renewal' Brussels COM (2005)

The Royal United Services Institute (RUSI) A Democratic Licence to Operate: Report of the Independent Surveillance Review Panel of the Independent Surveillance Review, Whitehall Reports, 13 July 2015

The RT Hon Lord Lloyd of Berwick (1996) Inquiry into Legislation Against Terrorism, Volume One, The Stationary Office Cm3420

The Rt. Hon. Dominic Grieve QC MP (2016) Intelligence and Security Committee of Parliament, Report on the draft Investigatory Powers Bill, 9 February, HC 795

The Rt. Hon. Sir Malcolm Rifkind MP, Intelligence and Security Committee, Access to communications data by the intelligence and security Agencies, February 2013, Cm8514

The Rt. Hon. Sir Malcolm Rifkind MP, Report on the intelligence relating to the murder of Fusilier Lee Rigby, Intelligence and Security Committee of Parliament, HC 795, 2014

The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. (November 2011)

Tomkins, A. (2010) National security and the role of the court: a changed landscape? Law Quarterly Review, 126, 543-567

Thomson, T. (2010) Crime Software may help police predict violent offences, The Guardian, 25 July 2010, available at http://www.guardian.co.uk/uk/2010/jul/25/police-software-crime-prediction accessed 15 December 2016

Thynne, K. (2009) Targeting the 'Terrorist Enemy': The Boundaries of an Armed Conflict Against Transnational Terrorists, *Australian International Law Journal*, 161-187

Tilley, N. (2008) *Modern Approaches to Policing: Community, Problem Orientated and Intelligence Led*, in Newburn, T. *Handbook of Policing* (Willan)

Titcomb, J (2016) World's internet traffic to surpass one zettabyte in 2016, The Telegraph, 4 February 2016, available at http://www.telegraph.co.uk/technology/2016/02/04/worlds-internet-traffic-to-surpass-one-zettabyte-in-2016/ accessed 5 December 2016

Travis, T. (2015) Snowden leak: governments' hostile reaction fuelled public distrust of spies, The Guardian, 15 June 2015, available at https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies accessed 15 December 2015

Travis, A. Asthana, A. and Chrisafis, A. (2016) UK and France restate commitment to border treaty after Calais talks, The Guardian, 30 August 2016, available at https://www.theguardian.com/world/2016/aug/30/uk-plays-down-calais-border-tensions-with-critical-ally-france accessed 20 December 2016

Trottier, D. (2012) *Social Media as Surveillance: Rethinking Visibility in a Converging World* (Ashgate Publishing).

Trottier, D. (2015) Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques, *European Journal of Cultural Studies*, 18:4-5

Tsukayama, H. Berman, M. and Markon, J (2016) Terror in Orlando: 50 killed in shooting rampage at gay club, gunman pledged allegiance to ISIS, The Washington Post, 13 June 2016, available at https://www.washingtonpost.com/news/post-nation/wp/2016/06/12/orlando-nightclub-shooting-about-20-dead-in-domestic-terror-incident-at-gay-club/?hpid=hp_hp-top-table-high_orlando-banner%3Ahomepage%2Fstory&utm_term=.8adec967a5ff accessed 30 December 2016

Tuman, J.S. (2010) *Communicating Terror: The Rhetorical Dimensions of Terrorism* (2nd edition, Sage)

Turner, I. (2011) The prevention of terrorism: in support of control orders, and beyond, *Northern Ireland Law Quarterly*, 62(3), 355-359

Tzanakopoulos, A. (2013) The Solange Argument as a Justification for Disobeying the Security Council in the Kadi Judgement, *Social Science Research Network*

United Nations General Assembly resolution 49/60 (1994) Declaration on Measures to Eliminate International Terrorism A/Res/60/49

United Nations General Assembly, Report of the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996, Sixth session (28 January-1 February 2002), Annex II, art. 2.1

United Nations General Assembly, Report of the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996, Sixth session (28 January-1 February 2002), Annex IV, art. 18.

United Nations General Assembly (2001) Resolution 55/25: United Nations Convention Against Transnational Organised Crime A/Res/55/2

United Nations Security Council Resolution 1566, (2004) Threats to international peace and security caused by terrorist acts S/RES/1566

United Nations General Assembly, Secretary General, Report of the Secretary-General In larger freedom: towards development, security and human rights for all, Chapter 3 (2005)

Vaughan-Nicols, S. (2013) Raytheon Riot: Defence Spying is Coming to Social Networks, ZDNet, 12 February, available at http://www.zdnet.com/raytheon-riot-defense-spying-is-coming-to-social-networks 7000011191/ accessed 23 August 2016

Vaughan, B. and Kilcommins, S. (2008) *Terrorism, Rights and the Rule of Law*, (Willan)

Vermeulen, F. (2014) Suspect Communities-Targeting Violent Extremism at the Local Level *Terrorism and Political Violence*, 26(2) 286-306

Vilasau, M. (2007) Traffic Data Retention v Data Protection: The New European Framework, *Computer and Telecommunications Law Review*, 52, 58

Wade, M. L. (2014) The European Union as a counter-terrorism actor: right path, wrong direction? *Crime Law Soc Change*, 62:355-383

Walen, A. (2011) Criminalising statements of terrorst intent: How to understand the law governing terrorist threats, and why it should be used instead of long term preventative detention, *The Journal of Criminal Law & Criminology*, 101:3, 803-854

Wang, Y. R. and Lumb, R. (2012) Integrating Eastern programme features in Western community policing: balancing individual freedom and collective wellbeing, *International Journal of Police Science and Management*, 14:4, 343-361

Walker, C. (2007) The Legal Definition of "Terrorism" in United Kingdom Law and Beyond, *Public Law*, [2007] 331-352

Walker, C (2008) Terrorism: Terrorism Act 2000 s.57-direction to jury on defence of possession of items for defensive purposes, Case Comment, *Criminal Law Review*, 72-80

Walker, C. (2008) Know Thine Enemy as Thyself: Discerning Friend from Foe under Anti-Terrorism Laws, *Melbourne University Law Review*, Vol. 32, 275-301

Walker, C. (2008) Terrorism: Terrorism Act 2000 ss. 1 and 58 – possession of terrorist documents, Case Comment, *Criminal Law Review* [2008] 160-165

Walker, C. (2009) Blackstone's Guide to The Anti-Terrorism Legislation, (2nd Edition, Oxford University Press)

Walker, C. (2010) Conscripting the public in terrorism policing: towards safer communities or a police state? *Criminal Law Review*, 441-456

Walker, C. (2011) The judicialisation of intelligence in legal process, Public Law, 235-237

Walker, C. (2012) The Terrorism Prevention and Investigation Measures Act 2011: one thing but not much the other? *Criminal Law Review* [2012] 6, 421-438

Walker, C. (2013) The Reshaping of Control Orders in the United Kingdom: Time for a Fairer Go, Australia, *Melbourne University Law Review*, 37(1)

Wardlow, G. (2002) *Political Terrorism*, (2nd Edition, Cambridge University Press)

Watt, N. (2013) PRISM Scandal: European Commission to Seek Privacy Guarantees from U.S., The Guardian, 10 June 2013, http://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees accessed 23 December 2016

Weenink, A. W. (2012) Situartional prevention of terrorism. Remarks from the field of counterterrorism in the Netherlands on Newman and Clarke's 'Policing Terrorism' *Trends Organ Crim*, 15:164-179

Welch, J. and Chakrabarti, S (2010) The War on Terror without the Human Rights Act – what difference has it made? European Human Rights Law Review, (6), 593-600

Whitman, J. Q. (2004) The Two Western Cultures of Privacy: Dignity Versus Liberty, *Yale Law Journal* 113: 1151–1179, available at http://digitalcommons.law.yale.edu/fss_papers/649/ accessed 20 December 2016

Whittaker, D. (2012) *The Terrorism Reader* (4th edition, Routledge)

Wilkinson, P. (2006) *Terrorism versus Democracy: The Liberal State Response* (2nd Edition, Routledge)

Williams, C. (2011) London Riots: BlackBerry Manufacturer offers to help police, The Telegraph, 8 August 2011, available at http://www.telegraph.co.uk/technology/blackberry/8689313/London-riots-BlackBerry-manufacturer-offers-to-help-police-in-any-way-we-can.html accessed 23 August 2016

Williamson, M. (2009) *Terrorism, war and international law: the legality of the use of force against Afghanistan in 2001*, (Ashgate Publishing)

Wintour, P. (2015) UK parents to get power to cancel children's passports over Isis fears, The Guardian, 20 July 2015, available at: https://www.theguardian.com/politics/2015/jul/20/uk-parents-power-cancel-childrens-passports-isis-fears accessed 24 November 2016

Wynn, K and Blyth, K. (2011) Predicting a riot: at what price privacy? Practical Law Company, available at http://uk.practicallaw.com/9-507-6354 accessed 23 August 2016

Xhelili, B. (2012) Privacy & Terrorism Review: Where have we come in 10 years? *Journal of International Commercial Law and Technology*, 7(2), 121-135

Young, D. (1999) *Origins of the Sacred: The Ecstasies of Love and War* (New York: St. Martin's Press)

Zedner, L. (2007) Pre-crime and post-criminology? *Theoretical Criminology*, 11:2

Zeidan, S. (2004) Desperately Seeking Definition: The International Community's Quest for Identifying the Specter of Terrorism, *Cornell International Law Journal*, Volume 36, Issue 3, Article 5, 491-496

Zhou, H-R. (2013) Revisiting the "manner and form" theory of parliamentary sovereignty, *The Law Quarterly Review*, 129, 610-638

Zimmerman, M. (2015) Darknet danger: Organs, murder, credit card info all for sale on Internet's underbelly, http://www.foxnews.com/tech/2015/04/23/darknet-danger-organs-murder-credit-card-info-all-for-sale-on-internet.html accessed 5 December 2016

Zwitter, A. (1998) The Anatomy of Ideology: An Analysis of the Structure of Ideology and the Mobilisation of Terrorist, HUMSEC Journal, Issue 1